b) soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578, e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato;

c) sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti ai clienti.

I dati relativi ai terzi possono essere trattati solo ove ciò sia strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

CAPO IV
IMPRESE BANCARIE ED ASSICURATIVE ED ALTRI TRATTAMENTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta:

a) ad imprese autorizzate o che intendono essere autorizzate all'esercizio dell'attività bancaria e creditizia, assicurativa o dei fondi pensione, anche se in stato di liquidazione coatta amministrativa, ai fini:

1) dell'accertamento, nei casi previsti dalle leggi e dai regolamenti, del requisito di onorabilità nei confronti di soci e titolari di cariche direttive o elettive;

2) dell'accertamento, nei soli casi espressamente previsti dalla legge, di requisiti soggettivi e di presupposti interdittivi 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, lettera a), della legge n. 675/1996, il titolare deve inviare al Garante una dettagliata relazione sulle modalità del trattamento;

b) a soggetti titolari di un trattamento di dati svolto nell'ambito di un'attività di richiesta, acquisizione e consegna di atti e documenti presso i competenti uffici pubblici, effettuata su incarico degli interessati;

c) alle società di intermediazione mobiliare, alle società di investimento a capitale variabile, e alle società di gestione del risparmio e dei fondi pensione, ai fini dell'accertamento dei requisiti di onorabilità in applicazione 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) 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;

b) a chiunque, per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

c) a persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n.

773, e successive modificazioni e integrazioni). Il trattamento deve essere necessario:

1) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero di un diritto della personalità o di un altro diritto fondamentale ed inviolabile;

2) su incarico di un difensore 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);

d) a chiunque, per adempiere ad obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale, contenute anche nella legge 19 marzo 1990, n. 55, e successive modificazioni ed integrazioni, o per poter produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto;

e) ai soggetti pubblici, ai fini dell'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare 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

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati per finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali.

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, lettera 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, lettere 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 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.2 PROVVEDIMENTI DEL GARANTE

6.2.1. PROVVEDIMENTO 30 dicembre 1999-13 gennaio 2000 - n. 1/P/2000 (in G.U. 2 febbraio 2000, n. 26, p. 31)

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 princìpi 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;

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 rispet-

to 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

6.2.2 PROVVEDIMENTO 10 febbraio 2000 (in G.U. 25 febbraio 2000, n. 46, p. 35)

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;

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 even-

tuali 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 31.03.2000 al seguente indirizzo: Garante per la protezione dei dati personali, Largo del Teatro Valle, 6 - 00186 Roma / fax 06.6818649 / 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

6.2.3. DELIBERAZIONE 29 febbraio 2000 n. 8 (in G.U. 18 marzo 2000, n. 65, p. 17)

Applicazione delle misure minime di sicurezza di cui al decreto del Presidente della Repubblica 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, lì 29 febbraio 2000

ALLEGATO

Nel riquadro d) (descrizione generale delle misure adottate per la sicurezza dei dati) è inserita la seguente avvertenza:

I soggetti che hanno notificato il trattamento dei dati personali prima del 29 marzo 2000 non devono effettuare una nuova notificazione per modificare il presente riquadro, qualora abbiano adottato le misure minime previste 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"*).

6.3 GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

6.3.1. Raccomandazione 4/99 sulla Carta europea dei diritti fondamentali

5143/99/IT/def.
WP 26

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

Raccomandazione 4/99 concernente l'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali

Adottata il 7 settembre 1999

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]
visto l'articolo 29 e l'articolo 30, paragrafo 3 della direttiva,
visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO LA SEGUENTE RACCOMANDAZIONE:

Il Consiglio europeo, riunito a Colonia il 4 giugno 1999, ha deciso l'elaborazione di una Carta dei diritti fondamentali dell'Unione europea. Nella sua decisione, il Consiglio afferma: "Allo stato attuale dello sviluppo dell'Unione è necessario elaborare una Carta di tali diritti al fine di sancirne in modo visibile l'importanza capitale e la portata per i cittadini dell'Unione."

Il Gruppo, composto da rappresentanti delle autorità responsabili della protezione dei dati personali negli Stati membri dell'Unione europea, appoggia pienamente l'iniziativa del Consiglio europeo mirante ad elaborare una Carta dei diritti fondamentali dell'Unione europea. Esso rileva che alcuni paesi europei hanno incluso nella loro costituzione un diritto fondamentale alla protezione dei dati personali. In alcuni altri paesi la giurisprudenza riconosce a tale diritto il carattere di diritto fondamentale.

Nella loro prassi, la Commissione europea e la Corte europea dei diritti dell'uomo hanno definito e concretizzato un diritto fondamentale sulla base delle implicazioni che vari diritti dell'uomo hanno in materia di protezione dei dati personali.

Infine, il nuovo articolo 286 del trattato che istituisce la Comunità europea dispone che, a decorrere dal 1° gennaio 1999, gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali si applicano alle istituzioni e agli organismi europei.

Includere la protezione dei dati personali nel quadro dei diritti fondamentali europei significherebbe rendere tale protezione giuridicamente vincolante in tutta l'Unione e tener conto della crescente importanza della protezione dei dati nella società dell'informazione.

---

[1] GU L 281 del 23.11.1995, p. 31; il testo della direttiva è disponibile al seguente indirizzo: http://europa.eu.int/comm/dg15/de/media/dataprot/index.htm

Il Gruppo raccomanda pertanto alla Commissione europea, al Parlamento Europeo e al Consiglio dell'Unione europea di includere il diritto fondamentale alla protezione dei dati personali nella Carta dei diritti fondamentali. Il Gruppo è disposto a collaborare all'elaborazione della Carta.

Fatto a Bruxelles, il 7 settembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

6.3.2. Negoziato Europa-Usa sul trasferimento dati

Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti

5092/98/IT/finale
WP 15

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

Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti

Adottato il 26 gennaio 1999

Il Gruppo di lavoro è a conoscenza delle discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti al fine di garantire il duplice obiettivo di un livello elevato di tutela dei dati personali e la libera circolazione di tali dati attraverso l'Atlantico. Il Gruppo di lavoro ritiene che queste discussioni siano importanti e spera che esse potranno conseguire risultati positivi in tempi brevi. Alla luce di tali discussioni, il 4 novembre 1998 l'Ambasciatore Aaron ha inviato una lettera con allegati, contenente una serie di proposte da discutere negli Stati Uniti tra rappresentanti di società USA e il Ministero federale del Commercio. A questo proposito, il Gruppo di lavoro invita le parti e i governi degli Stati membri dell'UE rappresentati nel Comitato istituito dall'articolo 31 della Direttiva 95/46/EC[1] a tener conto dei punti che seguono:

Le norme sulla tutela dei dati non sono fatte solo per proteggere gli utenti delle nuove tecnologie (in particolare, informatica e Internet) al fine di garantirne la fiducia e aiutare così lo sviluppo di tali tecnologie e lo scambio internazionale di dati. Esse esprimono anche l'adesione ad alcuni principi e diritti fondamentali basati su una cultura comune di rispetto della sfera privata e di altri valori intrinsechi all'essere umano e condivisi tanto dagli Stati membri dell'UE che dagli Stati Uniti.

1. Negli USA, la tutela della sfera privata e dei dati si affida a un complesso tessuto di norme settoriali, a livello federale e statale, e di autoregolamentazione dell'industria. In tempi recenti, c'è stato uno sforzo per migliorare credibilità e applicabilità degli strumenti autoregolamentari dell'industria, soprattutto in relazione ad Internet e al commercio elettronico. Il Gruppo di lavoro ritiene però che non si possa contare su questo mosaico di leggi settoriali, il cui ambito di applicazione è limitato, e di autoregolamentazione volontaria per tutelare adeguatamente tutti i casi di dati personali trasferiti dall'UE.

2. Data la complessità del sistema USA di tutela della sfera privata e dei dati, la definizione di un "punto di riferimento" convenuto della tutela in forma di "principi per un approdo sicuro", offerto a tutti gli operatori economici USA, è un buon approccio che, in casi specifici, potrebbe essere completato da soluzioni contrattuali. Tuttavia, per garantire la libera circolazione dei dati verso gli Stati Uniti in base a tali principi, sono necessari miglioramenti ulteriori. Inoltre, potrebbe rivelarsi necessario trovare metodi che chiariscano quali società

[1] Direttiva 95/46/EC 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 23.11.1995, p. 31.
Disponibile presso:http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm.

saranno coperte dai "principi per un approdo sicuro".

3. Si noti che la decisione di aderire a tali principi riguarda solo le singole società, e, in mancanza di una legislazione globale, resta quindi il problema delle società che non vogliono applicarli.

4. In generale, va chiarito lo statuto di tali principi. Se, in prima istanza, l'adesione ai principi può essere volontaria, una volta che una società aderisce, reclamando perciò i vantaggi di un "approdo sicuro", il rispetto dei principi deve essere obbligatorio.

5. La credibilità del sistema è seriamente compromessa dalla mancanza di controlli di conformità indipendenti e dall'affidarsi alla sola autocertificazione della società. La verifica indipendente va fatta in modo serio ma al tempo stesso praticabile anche per le piccole imprese. I modelli attualmente sviluppati negli USA dal *Better Business Bureau OnLine and TrustE* stanno andando nella giusta direzione.

6. Deve essere possibile che i reclami di singoli, i cui dati sono stati trasferiti dall'UE, siano trattati in un modo pratico ed efficace e che in ultima istanza siano giudicati da un'entità indipendente. In proposito è importante individuare uno o più enti pubblici od organizzazioni indipendenti negli USA disposti a fungere da punto di contatto per le autorità di tutela dei dati dell'UE e a indagare sui reclami. Occorre anche accertarsi che esistano accordi pratici per tutti i corrispondenti settori USA. Enti normativi già esistenti (*Federal Trade Commission; Office of the Comptroller of the Currency*) possono assumere tale ruolo nei settori di loro competenza.

7. Sui contenuti, i principi del tipo "approdo sicuro" devono comprendere, per essere accettabili, almeno tutti i principi precisati nelle direttive OCSE del 1980 sulla tutela della sfera privata, sottoscritti anche dagli Stati Uniti e recentemente riaffermati alla Conferenza OCSE di Ottawa sul commercio elettronico. Tali principi sono anche applicati dalla Direttiva 95/46/EC e dalla legislazione nazionale degli Stati membri dell'UE. In proposito, l'elenco di principi sopra ricordato, pubblicato il 4.11.1998 dal Ministero del commercio USA suscita le seguenti preoccupazioni:

   a) il diritto di accesso delle persone è limitato a quanto è "ragionevole". Le direttive OCSE sulla tutela della sfera privata non limitano il diritto in quanto tale, affermano solo che esso va esercitato "in modo ragionevole";

   b) manca il requisito dell'indicazione di uno scopo, presente nelle direttive OCSE, solo in parte sostituito da un possibilità di "scelta" che permette di usare per uno scopo dati raccolti per un altro, a meno che le persone non possano decidere di negarla;

   c) i dati "proprietari" e quelli elaborati manualmente sono esclusi dall'ambito di applicazione dei principi USA; il principio della "scelta" non garantisce alcuna tutela ai dati raccolti da terzi e quello di "accesso" esclude le informazioni provenienti da pubblici registri;

   d) secondo il terzo paragrafo dell'introduzione, "l'adesione ai principi è soggetta" a numerose eccezioni e limiti come la "gestione di rischio" e la "sicurezza delle informazioni". Per il Gruppo di lavoro si tratta di nozioni troppo vaghe e incerte: esso raccomanda che siano chiarite o cancellate.

Fatto a Bruxelles, il 26 gennaio 1999

Per il Gruppo
Il Vicepresidente
Stefano RODOTÀ

Parere 2/99 riguardante l'adeguatezza dei "principi internazionali per un approdo sicuro" stabiliti dal Ministero del commercio USA il 19 aprile 1999

5047/99/EN/final
WP 19

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

Parere 2/99 riguardante l'adeguatezza dei "principi internazionali per un approdo sicuro" stabiliti dal Ministero del commercio USA il 19 aprile 1999

Adottato il 3 maggio 1999

Le discussioni fra la Commissione delle Comunità europee e il Governo degli Stati Uniti sono proseguite dopo che il Gruppo di lavoro ha pubblicato, nel gennaio 1999[3], il suo parere sul livello di protezione dei dati negli Stati Uniti. Recentemente, la Commissione ha presentato al Gruppo di lavoro una versione riveduta dei principi del Ministero federale del commercio per avere un suo parere sul livello di tutela dei dati che essi offrono.

La Commissione ha anche comunicato al Gruppo di lavoro che prevede l'adozione di una decisione, basata sull'articolo 25.6 della direttiva[4], concernente questi principi, se risultano assicurare un livello adeguato di protezione per il trasferimento di dati da società europee a società statunitensi aderenti ai principi per un "approdo sicuro".

L'attuale versione dei principi non può comunque essere considerata definitiva poiché contiene varie note che indicano i campi in cui non è ancora stato raggiunto un accordo soddisfacente con gli Stati Uniti. Il Gruppo di lavoro considera quindi questo parere provvisorio e parziale. Esso è provvisorio perché i documenti non sono ancora definitivi e lo status delle FAQ (frequently asked questions - domande poste frequentemente) stabilito dal Ministero federale del commercio non è ancora stato indicato chiaramente al Gruppo di lavoro (il loro contenuto non viene quindi preso in considerazione nel presente parere). Inoltre, si tratta di un parere parziale perché il Gruppo di lavoro non dispone ancora di tutti i documenti necessari per un esame globale della situazione negli Stati Uniti, e in particolare di un quadro delle modalità d'applicazione dei principi e di un'analisi della tutela offerta dalle leggi settoriali statunitensi.

Il Gruppo di lavoro ribadisce la sua opinione che il complesso tessuto di leggi settoriali con un limitato ambito d'applicazione e di norme di autoregolamentazione attualmente esistente negli Stati Uniti non è sufficiente a fornire in tutti i casi una tutela adeguata dei dati personali trasferiti dall'Unione europea. Ritiene perciò utile l'approccio "approdo sicuro" ed incoraggia la Commissione a continuare il suo lavoro volto alla ricerca di una serie di principi che saranno adottati dal Ministero federale del commercio in modo da fornire un punto di riferimento alle società statunitensi che desiderano assicurarsi di soddisfare i requisiti di tutela adeguata stabiliti dalla direttiva.

---

[3] Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le attuali discussioni fra la Commissione europea e il Governo degli Stati Uniti, adottato dal Gruppo di lavoro il 26 gennaio 1999.
[4] Un progetto di decisione della Commissione è stato consegnato al Gruppo di lavoro il 30 marzo 1999.

Il Gruppo di lavoro ritiene utile esaminare le implicazioni pratiche di quest'accordo per il lavoro delle autorità di controllo nazionali.

Implicazioni pratiche dell'"approdo sicuro" per il lavoro delle autorità di controllo nazionali

Il Gruppo di lavoro ritiene molto importante che le società con sede negli Stati Uniti aderenti ai principi per un "approdo sicuro" siano individuate in modo inequivocabile e quindi considera molto opportuna la raccomandazione del Ministero federale del commercio alle società americane di notificare al Ministero la loro intenzione di aderire al programma. Il Gruppo di lavoro ritiene che tale notifica debba essere per quanto possibile completa, essere resa pubblica ed indicare in particolare una persona di contatto nella società in grado di trattare le richieste dei singoli individui e l'organo di controllo responsabile dell'applicazione dei principi.

Per poter partecipare al programma "approdo sicuro", le organizzazioni statunitensi possono" partecipare a un programma sulla tutela della vita privata sviluppato dal settore privato ..." o farlo in base alle leggi statunitensi che proteggono efficacemente la vita privata nella misura in cui le sue attività siano disciplinate da tali leggi. Il Gruppo di lavoro chiede ulteriori chiarimenti su questi programmi e sui loro criteri operativi. Per quanto riguarda le leggi settoriali statunitensi, il Gruppo di lavoro chiede chiarimenti sul loro esatto contenuto riguardo alla tutela della vita privata.

Il Gruppo di lavoro sottolinea anche che i principi per un "approdo sicuro" si riferiscono solo alla legittimità degli aspetti internazionali del trasferimento dei dati derivanti dagli articoli 25 e 26 della direttiva. Gli esportatori di dati con sede in Europa (affiliati o meno a una società con sede negli Stati Uniti aderente all'"approdo sicuro") sono soggetti all'applicazione delle altre disposizioni della direttiva, per esempio quelle relative alla notifica del trattamento dei dati alle autorità di controllo nazionali.

Il compito delle autorità di controllo sarebbe inoltre facilitato da una descrizione precisa dei poteri delle autorità di regolamentazione. Il Gruppo di lavoro è stato informato che le autorità statunitensi stanno preparando questo documento.

Considerando il ruolo delle autorità di controllo nazionali nel rilascio delle autorizzazioni di trasferimenti internazionali basati su contratti, il Gruppo di lavoro chiede chiarimenti sul significato dell'ultima frase del paragrafo 4 dell'introduzione, che dice *"Le organizzazioni possono applicare le salvaguardie ritenute necessarie dall'UE anche per i trasferimenti di dati personali dall'UE agli USA incorporando i principi per un 'approdo sicuro' pertinenti negli accordi conclusi con parti che trasferiscono dati personali dall'UE"*.

Infine, per quanto riguarda la possibilità per le organizzazioni aderenti ai principi del Ministero federale del commercio di affidarsi alle autorità di controllo nazionali per l'applicazione dei principi, il Gruppo di lavoro sottolinea che le autorità di controllo nazionali non hanno giurisdizione nei paesi terzi e di conseguenza non dispongono dei poteri necessari per controllare efficacemente l'applicazione dei principi da parte delle organizzazioni statunitensi.

- Per quanto riguarda il contenuto dei principi stessi, il Gruppo di lavoro riconosce che rispetto alla versione del 4 novembre, sebbene i principi siano stati indeboliti sotto alcuni aspetti, sono stati compiuti progressi in vari campi, in particolare:
- La definizione dei dati personali si riferisce ora a una persona fisica identificata o identificabile;
- Le eccezioni ai principi appaiono più coerenti e riflettono in parte quelle previste nella direttiva. È il caso, in particolare, della soppressione di espressioni come "gestione del rischio", "sicurezza delle informazioni" e "dati proprietari".
- Nell' "avviso" la persona fisica va informata su un cambiamento di finalità;
- I dati "sensibili" sono ora descritti con precisione nell'articolo 2 "Scelta";
- Nei trasferimenti successivi si differenzia ora tra trasferimenti tra organizzazioni aderenti ai principi e trasferimenti verso Paesi terzi non partecipanti al programma per un "approdo sicuro".