Documentazione

Provvedimenti normativi

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

IL PRESIDENTE DELLA REPUBBLICA

[*omissis*]

Emana

il seguente decreto legislativo:

[*omissis*]

Art. 184. Norme abrogate
1. Sono abrogate le seguenti disposizioni:
[*omissis*]
- decreto legislativo 30 giugno 2003, n. 196, limitatamente all'articolo 179, comma 4;

[*omissis*]

(*) *G.U.* 24 febbraio 2004, n. 45.

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

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1

1. Il decreto-legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

ALLEGATO

Modificazioni apportate in sede di conversione al d.l. 24 dicembre 2003, n. 354

[*omissis*]

All'articolo 3:

- al comma 1, capoverso "Art. 132", comma 1, le parole "i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi" sono sostituite dalle seguenti "i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi";

- al comma 1, capoverso "Art. 132", comma 2, dopo le parole "i dati" sono inserite le seguenti: "relativi al traffico telefonico" e le parole: "trenta mesi per esclusive finalità di accertamento e repressione dei delitti" sono sostituite dalle seguenti: "ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti";

- al comma 1, capoverso "Art. 132", comma 3, le parole: "dell'autorità giudiziaria, d'ufficio o su istanza" sono sostituite dalle seguenti: "del giudice su istanza del pubblico ministero o" e sono aggiunte, in fine, le parole: "ferme restando le condizioni di cui all'articolo 8, comma 2, lettera *f*) , per il traffico entrante";

- al comma 1, capoverso "Art. 132", il comma 4 è sostituito dal seguente:

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

- al comma 1, capoverso "Art. 132", comma 5, l'alinea è sostituito dal seguente: "5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti anche a:";

- al comma 1, capoverso "Art. 132", comma 5, alla lettera *c*) le parole: "di accesso ai" sono sostituite dalle seguenti: "di trattamento dei" e le parole: "l'accesso sia consentito" sono sostituite dalle seguenti: "l'utilizzazione dei dati sia consentita";

- al comma 1, capoverso "Art. 132", il comma 6 è soppresso.

(*) *G.U.* 27 febbraio 2004, n. 48.

All'articolo 4:

- al comma 1, le parole: "Fino alla data del 31 dicembre 2005 per la conservazione del traffico si osserva il termine della prescrizione di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171" sono sostituite dalle seguenti: "Fino alla data in cui divengono efficaci le misure e gli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, per la conservazione del traffico telefonico si osserva il termine di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171".

[*omissis*]

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

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1.

1. Il decreto-legge 29 marzo 2004, n. 81, recante interventi urgenti per fronteggiare situazioni di pericolo per la salute pubblica, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Roma, 26 maggio 2004

ALLEGATO

Modificazioni apportate in sede di conversione al decreto-legge 29 marzo 2004, n. 81

[*omissis*]

Art. 2-*quinquies*.

1. Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 37, dopo il comma 1, è inserito il seguente:

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

b) all'articolo 83, dopo il comma 2, è aggiunto il seguente:

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

c) all'articolo 89, dopo il comma 2, è aggiunto il seguente:

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

d) all'articolo 181, la lettera *e*) del comma 1 è abrogata.

(*) *G.U.* 29 maggio 2004, n 125.

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

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1.

1. Il decreto-legge 24 giugno 2004, n. 158, concernente permanenza in carica degli attuali consigli degli ordini professionali e proroga di termini in materia di difesa d'ufficio e procedimenti civili davanti al tribunale per i minorenni, nonché di protezione dei dati personali, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

Roma, 27 luglio 2004

ALLEGATO

Modificazioni apportate in sede di conversione al decreto-legge 24 giugno 2004, n. 158

[omissis]

All'articolo 1, dopo il comma 1, è aggiunto il seguente:

"1-*bis*. Il regolamento previsto dall'articolo 4, comma 3, del regolamento di cui al decreto del Presidente della Repubblica 5 giugno 2001, n. 328, è emanato entro il 31 dicembre 2004. Entro la medesima data devono essere indette, ove il mandato non abbia più lunga durata, le elezioni per il rinnovo dei consigli degli ordini e collegi interessati".

(*) *G.U.* 30 luglio 2004, n. 177.

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

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1.

1. Il decreto-legge 9 novembre 2004, n. 266, recante proroga o differimento di termini previsti da disposizioni legislative, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

[omissis]

Roma, 27 dicembre 2004

DECRETO-LEGGE 9 NOVEMBRE 2004, N. 266

[omissis]

Art. 6. Trattamento di dati personali

1. All'articolo 180 del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modifiche:

a) al comma 1, le parole: "31 dicembre 2004" sono sostituite dalle seguenti: "30 giugno 2005";

b) al comma 3, le parole: "31 marzo 2005" sono sostituite dalle seguenti: "30 settembre 2005".

(*) *G.U.* 27 dicembre 2004, n. 302.

Provvedimenti del Garante

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. d), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del Codice;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 111 del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi volti a ridurre al

(*) *G.U.* 14 agosto 2004, n. 190.

minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato nell'ambito dei rapporti di lavoro;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Stefano Rodotà;

Autorizza:

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, finalizzato alla gestione dei rapporti di lavoro, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata:

a) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e agli organismi che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lett. b) e c);
b) ad organismi paritetici o che gestiscono osservatori in materia di lavoro, previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi anche aziendali;

l'autorizzazione riguarda anche l'attività svolta:

c) dal medico competente in materia di igiene e di sicurezza del lavoro, in qualità di libero professionista o di dipendente dei soggetti di cui alla lettera a) o di strutture convenzionate;
d) da associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro, al solo fine di perseguire le finalità di cui al punto 3), lett. h).

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) a lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione e lavoro, ovvero ad associati anche in compartecipazione e, se necessario in base ai punti 3) e 4), ai relativi familiari e conviventi;

b) a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatari;
c) a soggetti che effettuano prestazioni coordinate e continuative o ad altri lavoratori autonomi in rapporto di collaborazione con i soggetti di cui al punto 1);
d) a candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti;
e) a persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto 1);
f) a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui alle precedenti lettere.

3) Finalità del trattamento.
Il trattamento dei dati sensibili deve essere indispensabile:
a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi anche aziendali, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica;
b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;
d) per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
e) per esercitare il diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;
f) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
g) per garantire le pari opportunità;
h) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

4) Categorie di dati
Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e in particolare:
a) nell'ambito dei dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, i dati concernenti la fruizione di permessi e festività religiose o di servizi di mensa, nonché la manifestazione, nei casi previsti dalla legge, dell'obiezione di coscienza;
b) nell'ambito dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale, i dati concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali (sempre che il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pub-

bliche iniziative, nonché i dati inerenti alle trattenute per il versamento delle quote di servizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;

c) nell'ambito dei dati idonei a rivelare lo stato di salute, i dati raccolti e ulteriormente trattati in riferimento a invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psicofisica a svolgere determinate mansioni, all'appartenenza a determinate categorie protette, nonché i dati contenuti nella certificazione sanitaria attestante lo stato di malattia, anche professionale dell'interessato, o comunque relativi anche all'indicazione della malattia come specifica causa di assenza del lavoratore.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Restano inoltre fermi gli obblighi di informare l'interessato e, ove necessario, di acquisirne il consenso scritto, in conformità a quanto previsto dagli articoli 13, 23 e 26 del Codice.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e), del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto 3), ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e, ove necessario diffusi, nei limiti strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), a soggetti pubblici o privati, ivi compresi organismi sanitari, casse e fondi di previdenza ed assistenza sanitaria integrativa anche aziendale, istituti di patronato e di assistenza sociale, centri di assistenza fiscale, agenzie per il lavoro, associazioni ed organizzazioni sindacali di datori di lavoro e di prestatori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

Ai sensi dell'art. 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qua-

lora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità dalle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute:

a) nell'art. 8 della legge 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;
b) nell'art. 6 della legge 5 giugno 1990, n. 135, che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività;
c) nelle norme in materia di pari opportunità o volte a prevenire discriminazioni;
d) fermo restando quanto disposto dall'art. 8 della legge 20 maggio 1970, n. 300, nell'art. 10 del d.lg. 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute e ad eventuali controversie con i precedenti datori di lavoro, nonché di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 1/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

Il Presidente
Rodotà

Il Relatore
Rodotà

Il Segretario generale
Buttarelli

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto l'art. 76 del Codice, secondo cui gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85 del medesimo Codice, possono trattare i dati personali idonei a rivelare lo stato di salute anche senza il consenso dell'interessato, previa autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica di un terzo o della collettività;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice, princìpi valutati anche sulla base delle raccomandazioni adottate in materia di dati sanitari dal Consiglio d'Europa ed in particolare dalla Raccomandazione N.R (97) 5, in base alla quale i dati sanitari devono essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza e di efficacia pari a quelle previste in tale ambito;

(*) *G.U.* 14 agosto 2004, n. 190.

Considerato che un elevato numero di trattamenti idonei a rivelare lo stato di salute e la vita sessuale è effettuato per finalità di prevenzione o di cura, per la gestione di servizi socio-sanitari, per ricerche scientifiche o per la fornitura all'interessato di prestazioni, beni o servizi;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Stefano Rodotà;

Autorizza:

a) gli esercenti le professioni sanitarie a trattare i dati idonei a rivelare lo stato di salute, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica o la salute di un terzo o della collettività, e il consenso non sia prestato o non possa essere prestato per effettiva irreperibilità;
b) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare con il consenso i dati idonei a rivelare lo stato di salute e la vita sessuale;
c) gli organismi sanitari pubblici, istituiti anche presso università, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute, qualora ricorrano contemporaneamente le seguenti condizioni:
    1. il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;
    2. manchi il consenso (articolo 76, comma 1, lett. b), del Codice), in quanto non sia prestato o non possa essere prestato per effettiva irreperibilità;
    3. non si tratti di attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione ai sensi dell'art. 85, commi 1 e 2, del Codice;
d) anche soggetti diversi da quelli di cui alle lettere a), b) e c) a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora il trattamento sia necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato.

Per l'informativa e, ove previsto, il consenso si osservano anche le disposizioni di cui agli articoli 13, 23, 26 e da 75 a 82 del Codice.

1) Ambito di applicazione e finalità del trattamento

1.1. L'autorizzazione è rilasciata:
a) ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;
b) al personale sanitario infermieristico, tecnico e della riabilitazione che esercita

l'attività in regime di libera professione;

c) alle istituzioni e agli organismi sanitari privati, anche quando non operino in rapporto con il servizio sanitario nazionale.

In tali casi, l'autorizzazione è rilasciata anche per consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, dalla normativa comunitaria o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni, di diagnosi e cura, ivi compresi i trapianti di organi e tessuti, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di profilassi delle malattie infettive e diffusive, di tutela della salute mentale, di assistenza farmaceutica e di assistenza sanitaria alle attività sportive o di accertamento, in conformità alla legge, degli illeciti previsti dall'ordinamento sportivo. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario, ovvero di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini appena indicati.

Qualora il perseguimento di tali fini richieda l'espletamento di compiti di organizzazione o di gestione amministrativa, i destinatari della presente autorizzazione devono esigere che i responsabili e gli incaricati del trattamento preposti a tali compiti osservino le stesse regole di segretezza alle quali sono sottoposti i medesimi destinatari della presente autorizzazione, nel rispetto di quanto previsto anche dall'art. 83, comma 1, del Codice.

1.2. L'autorizzazione è rilasciata, altresì, ai seguenti soggetti:

a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle relazioni tra i fattori di rischio e la salute umana, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. In tali casi occorre acquisire il consenso (in conformità a quanto previsto dagli articoli 106, 107 e 110 del Codice), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima. Resta fermo quanto previsto dall'art. 98 del Codice;

b) alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;

c) alle comunità di recupero e di accoglienza, alle case di cura e di riposo, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;

d) agli enti, alle associazioni e alle organizzazioni religiose riconosciute, relativamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi nei limiti di quanto stabilito dall'art. 26, comma 4, lett. a), del Codice, fermo restando quanto previsto per le confessioni religiose dagli articoli 26, comma 3, lett. a), e 181, comma 6, del Codice e dell'autorizzazione n. 3/2004;

e) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati, ove necessario attinenti anche alla vita sessuale, e alle operazioni indispensabili per adempiere agli obblighi, anche precontrattuali, derivanti da un rapporto di fornitura all'interessato di beni, di prestazioni o di servizi.

Se il rapporto intercorre con istituti di credito, imprese assicurative o riguarda valori mobiliari, devono considerarsi indispensabili i soli dati ed operazioni necessari per fornire specifici prodotti o servizi richiesti dall'interessato. Il rapporto può riguardare anche la fornitura di strumenti di ausilio per la vista, per l'udito o per la deambulazione;

f) alle persone fisiche e giuridiche, agli enti, alle associazioni e agli altri organismi che gestiscono impianti o strutture sportive, limitatamente ai dati e alle operazioni indispensabili per accertare l'idoneità fisica alla partecipazione ad attività sportive o agonistiche;

g) alle persone fisiche e giuridiche e ad altri organismi, limitatamente ai dati dei beneficiari e dei donatori e alle operazioni indispensabili per effettuare trapianti di organi e tessuti, nonché donazioni di sangue.

1.3. La presente autorizzazione è rilasciata, altresì, quando il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale sia necessario per:

a) lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che il diritto sia di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile, e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario per il loro perseguimento;
b) adempiere o esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi per la gestione del rapporto di lavoro, nonché della normativa in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione, nei limiti previsti dalla autorizzazione generale del Garante n. 1/2004 e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111 del Codice.

1.4. Fino alla data in cui sarà efficace l'apposita autorizzazione per il trattamento dei dati genetici prevista dall'art. 90 del Codice, restano autorizzati i trattamenti di dati genetici nei soli limiti e alle condizioni individuate al punto 2, lett. b), dell'autorizzazione n. 2/2002.

2) Categorie di dati oggetto di trattamento

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e può comprendere le informazioni relative a stati di salute pregressi.

Devono essere considerate sottoposte all'ambito di applicazione della presente autorizzazione anche le informazioni relative ai nascituri, che devono essere trattate alla stregua dei dati personali in conformità a quanto previsto dalla citata raccomandazione N.R (97) 5 del Consiglio d'Europa.

3) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

32

Per le informazioni relative ai nascituri, il consenso è prestato dalla gestante. Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario (art. 82, comma 4, del Codice).

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e) del Codice, i dati possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti sopra indicati, ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

5) Comunicazione e diffusione dei dati

I dati idonei a rivelare lo stato di salute, esclusi i dati genetici, possono essere comunicati, nei limiti strettamente pertinenti agli obblighi, ai compiti e alle finalità di cui al punto 1), a soggetti pubblici e privati, ivi compresi i fondi e le casse di assistenza sanitaria integrativa, le aziende che svolgono attività strettamente correlate all'esercizio di professioni sanitarie o alla fornitura all'interessato di beni, di prestazioni o di servizi, gli istituti di credito e le imprese assicurative, le associazioni od organizzazioni di volontariato e i familiari dell'interessato.

Ai sensi degli artt. 22, comma 8, e 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

I dati idonei a rivelare la vita sessuale non possono essere diffusi, salvo il caso in cui la diffusione riguardi dati resi manifestamente pubblici dall'interessato e per i quali l'interessato stesso non abbia manifestato successivamente la sua opposizione per motivi legittimi.

6) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione, relative, ad esempio, al caso in cui la raccolta del consenso comporti un impiego di mezzi manifestamente sproporzionato in ragione, in particolare, del numero di persone interessate.

7) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dall'art. 5, comma 2, della legge 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, secondo cui la rilevazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona;

b) dall'art. 11 della legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare al medico provinciale competente per territorio una dichiarazione che non faccia menzione dell'identità della donna;
c) dall'art. 734-*bis* del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal Codice di deontologia medica adottato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati e di includerli, in particolare, nelle pubblicazioni a contenuto scientifico o finalizzate all'educazione, alla prevenzione o all'informazione di carattere sanitario.

8) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 2/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

Il Presidente
Rodotà

Il Relatore
Rodotà

Il Segretario generale
Buttarelli

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto altresì il comma 4, lett. a), del citato art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, "quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13";

Visto il comma 3, lettere a) e b), del predetto art. 26, il quale stabilisce che la disciplina di cui al relativo comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni; b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria;

Rilevato che le confessioni di cui alla lettera a) devono determinare, ai sensi del medesimo art. 26, comma 3, lett. a), idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

Visto l'art. 181, comma 6, del Codice secondo cui le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui al predetto art. 26, comma 3, lett. a), possono proseguire l'attività di trattamento nel rispetto delle medesime;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40, del Codice);

(*) *G.U.* 14 agosto 2004, n. 190.

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da enti ed organizzazioni di tipo associativo e da fondazioni, per la realizzazione di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

Autorizza:

il trattamento dei dati sensibili di cui art. 4, comma 1, lett. d), del Codice da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) AMBITO DI APPLICAZIONE

La presente autorizzazione è rilasciata:

a) alle associazioni anche non riconosciute, ai partiti e i movimenti politici, alle associazioni e alle organizzazioni sindacali, ai patronati e alle associazioni di categoria, alle casse di previdenza, alle organizzazioni assistenziali o di volontariato,

nonché le federazioni e confederazioni nelle quali tali soggetti sono riuniti in conformità, ove esistenti, allo statuto, all'atto costitutivo o ad un contratto collettivo;

b) alle fondazioni, ai comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, ivi comprese le organizzazioni non lucrative di utilità sociale (Onlus);

c) alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818.

L'autorizzazione è rilasciata altresì agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per l'applicazione dell'articolo 310 del decreto legislativo 16 aprile 1994, n. 297.

Resta fermo l'obbligo per le confessioni religiose di determinare, ai sensi dell'art. 26, comma 3, lett. a) del Codice, idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati con la presente autorizzazione.

Ai sensi dell'art. 181, comma 6, del Codice, le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'art. 26, comma 3, lett. a), del Codice possono proseguire l'attività di trattamento effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, nel rispetto delle medesime.

2) Finalità del trattamento

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi. La presente autorizzazione è rilasciata inoltre per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.

Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro o di liberi professionisti per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi, persone giuridiche o liberi professionisti.

I soggetti di cui alle lettere a), b) e c) possono comunicare alle persone giuridiche e agli organismi con scopo di lucro titolari di un autonomo trattamento, i soli dati sensibili strettamente indispensabili per le attività di effettivo ausilio alle predette finalità, con particolare riferimento alle generalità degli interessati e ad indirizzari, sulla base di un atto scritto che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo, le particolari misure di sicurezza, nonché, ove previsto, le idonee garanzie determinate. La dichiarazione scritta di consenso degli interessati deve porre tale circostanza in particolare evidenza e deve recare la precisa menzione dei titolari del trattamento e delle finalità da essi perseguite. Le persone giuridiche e gli organismi con scopo di lucro, oltre a quanto previsto

nei punti 4) e 6) in tema di pertinenza, non eccedenza e indispensabilità dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

3) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;
b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l'associazione, la fondazione o il diverso organismo;
c) ai soggetti che ricoprono cariche sociali o onorifiche;
d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall'associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all'atto costitutivo, ove esistenti;
e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;
f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

4) Categorie di dati oggetto di trattamento

L'autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l'autorizzazione generale n. 2/2004.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 4, comma 1, lettera d) del Codice, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, che non possano essere perseguite o adempiuti, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto ai predetti obblighi e finalità, in particolare per quanto riguarda i dati che rivelano le opinioni e le intime convinzioni, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, dagli articoli 31 e seguenti del Codice e dall'allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità, agli scopi e agli obblighi di cui al punto 2).

I dati sono raccolti, di regola, presso l'interessato.

Fermo restando quanto previsto ai punti 2) e 7) della presente autorizzazione, se è indispensabile, in conformità al medesimo punto 7) comunicare o diffondere dati all'esterno

33

dell'associazione, della fondazione, del comitato o del diverso organismo, il consenso scritto è acquisito previa idonea informativa resa agli interessati ai sensi dell'art. 13 del Codice, la quale deve precisare le specifiche modalità di utilizzo dei dati tenuto conto delle idonee garanzie adottate relativamente ai trattamenti effettuati.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e) del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità e gli scopi di cui al punto 2), ovvero per adempiere agli obblighi ivi menzionati.

Le verifiche di cui al punto 4) devono riguardare anche la pertinenza, non eccedenza e indispensabilità dei dati rispetto all'attività svolta dall'interessato o al rapporto che intercorre tra l'interessato e i soggetti di cui al punto 1), tenendo presente il genere di prestazione, di beneficio o di servizio offerto all'interessato e la posizione di quest'ultimo rispetto ai soggetti stessi.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati a soggetti pubblici o privati, e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi di cui al punto 2) e tenendo presenti le altre prescrizioni sopraindicate.

I dati sensibili possono essere comunicati alle autorità competenti se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti dalla normativa comunitaria, da norme di legge o di regolamento che stabiliscono divieti o limiti in materia di trattamento di dati personali.

Restano inoltre ferme le norme volte a prevenire discriminazioni, e in particolare le disposizioni contenute nel decreto-legge 26 aprile 1993, n. 122, convertito, con modificazioni, dalla legge 25 giugno 1993, n. 205, in materia di discriminazione per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia

già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 3/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. c), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario ai fini dello svolgimento delle investigazioni difensive ai sensi della legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, e che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale il diritto sia di rango pari a quello dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 135 del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

(*) *G.U.* 14 agosto 2004, n. 190.

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da liberi professionisti iscritti in albi o elenchi professionali per l'espletamento delle rispettive attività professionali;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Giuseppe Santaniello;

Autorizza:

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 4, comma 1, lettera d), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta, ai liberi professionisti tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96, o alle norme di attuazione dell'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza.

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

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, ai praticanti e ai tirocinanti presso il libero professionista, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

Il presente provvedimento non si applica al trattamento dei dati sensibili effettuato:

a) dagli esercenti la professione sanitaria e dagli psicologi, dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/2004;
b) per la gestione delle prestazioni di lavoro o di collaborazione di cui si avvale il libero professionista o taluno dei soggetti sopra indicati, alla quale si riferisce l'autorizzazione generale n. 1/2004;
c) da soggetti privati che svolgono attività investigative, dai giornalisti, dai pubblicisti e dai praticanti giornalisti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69.

2) Interessati ai quali i dati si riferiscono e categorie di dati
Il trattamento può riguardare i dati sensibili relativi ai clienti.

I dati sensibili relativi ai terzi possono essere trattati ove ciò sia strettamente indispensabile per l'esecuzione di specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

In ogni caso, i dati devono essere strettamente pertinenti e non eccedenti rispetto ad incarichi conferiti che non possano essere svolti mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato anche nel rispetto della citata autorizzazione generale n. 2/2004.

3) Finalità del trattamento
Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che il libero professionista può eseguire in base al proprio ordinamento professionale, e in particolare:

a) per curare gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro;
b) ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, anche a mezzo di sostituti e di consulenti tecnici, o, comunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
c) per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia, salvo quanto previsto dall'art. 60 del Codice in relazione ai dati sullo stato di salute e sulla vita sessuale.

4) Modalità di trattamento
Il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto all'incarico conferito dal cliente.

Restano fermi gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice.

Restano inoltre fermi gli obblighi di informare l'interessato ai sensi dell'art. 13, commi 1, 4 e 5, del Codice, anche quando i dati sono raccolti presso terzi, e di acquisire, ove necessario, il consenso scritto.

Se i dati sono raccolti per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive (punto 3), lett. b)), l'informativa relativa ai dati raccolti presso terzi, e il consenso scritto, sono necessari solo se i dati sono trattati per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità, oppure per altre finalità con esse non incompatibili.

Le informative devono permettere all'interessato di comprendere agevolmente se il titolare del trattamento è un singolo professionista o un'associazione di professionisti, ovvero se ricorre un'ipotesi di contitolarità tra più liberi professionisti o di esercizio della professione in forma societaria ai sensi del decreto legislativo 2 febbraio 2001, n. 96.

Resta ferma la facoltà del libero professionista di designare quali responsabili o incaricati del trattamento i sostituti, gli ausiliari, i tirocinanti e i praticanti presso il libero professionista, i quali, in tal caso, possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Analoga cautela deve essere adottata in riferimento agli incaricati del trattamento preposti all'espletamento di compiti amministrativi.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e), del Codice, i dati sensibili possono essere conservati, per il periodo di tempo previsto dalla normativa comunitaria, da leggi, o da regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine, anche mediante controlli periodici, deve essere verificata la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto agli incarichi in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

I dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti, non eccedenti e indispensabili rispetto a successivi incarichi.

6) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e ove necessario diffusi, a soggetti pubblici o privati, nei limiti strettamente pertinenti all'espletamento dell'incarico conferito e nel rispetto, in ogni caso, del segreto professionale.

I dati idonei a rivelare lo stato di salute possono essere comunicati solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle leggi 20 maggio 1970, n. 300, e 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, nonché dalle norme volte a prevenire discriminazioni.

34

Restano fermi, altresì, gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici o di buona condotta relativi alle singole figure professionali.

9) Efficacia temporale e disciplina transitoria
La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 4/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

Il Presidente
Rodotà

Il Relatore
Santaniello

Il Segretario generale
Buttarelli

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d) del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata tenuto conto dei codici di deontologia e di buona condotta di cui agli articoli 106 e 140 del Codice;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione dei codici di deontologia e di buona condotta riguardanti alcuni specifici settori presi in considerazione dal presente provvedimento (articoli 111 e 140 del Codice);

Considerata la necessità di garantire il rispetto di alcuni princìpi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da parte di soggetti operanti in diversi settori di attività economiche di seguito individuate;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

(*) *G.U.* 14 agosto 2004, n. 190.

35

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Gaetano Rasi;

Autorizza:

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, fatta eccezione dei dati idonei a rivelare la vita sessuale, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

CAPO I - ATTIVITÀ BANCARIE, CREDITIZIE, ASSICURATIVE, DI GESTIONE DI FONDI, DEL SETTORE TURISTICO, DEL TRASPORTO

1) Soggetti ai quali è rilasciata l'autorizzazione:

a) imprese autorizzate all'esercizio dell'attività bancaria e creditizia o assicurativa ed organismi che le riuniscono, anche se in stato di liquidazione coatta amministrativa;
b) società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;
c) società ed altri organismi di intermediazione finanziaria, in particolare per la gestione o l'intermediazione di fondi comuni di investimento o di valori mobiliari;
d) società ed altri organismi che emettono carte di credito o altri mezzi di pagamento, o che ne gestiscono le relative operazioni;
e) imprese che svolgono autonome attività strettamente connesse e strumentali a quelle indicate nelle precedenti lettere, e relative alla rilevazione dei rischi, al recupero dei crediti, a lavorazioni massive di documenti, alla trasmissione dati, all'imbustamento o allo smistamento della corrispondenza, nonché alla gestione di esattorie o tesorerie;
f) imprese che operano nel settore turistico o alberghiero o del trasporto, agenzie di viaggio e operatori turistici.

2) Finalità del trattamento

La presente autorizzazione è rilasciata, anche senza richiesta, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti di cui al punto 1) assumono, nel proprio settore di attività, al fine di fornire specifici beni, prestazioni o servizi richiesti dall'interessato.

L'autorizzazione è rilasciata anche per adempiere o per esigere l'adempimento ad obblighi previsti, anche in materia fiscale e contabile, dalla normativa comunitaria, dalla legge, dai regolamenti, o dai contratti collettivi, o prescritti da autorità od organi di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.

Il trattamento avente tali finalità può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

3) Interessati ai quali i dati si riferiscono e categorie di dati trattati
Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che, ove necessario, abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

4) Comunicazione e diffusione dei dati
I dati sensibili possono essere comunicati, nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società controllate e collegate ai sensi dell'art. 2359 del codice civile, nonché, ove necessario, ai familiari dell'interessato.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lett. c), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

I dati sensibili non possono essere diffusi.

Capo II - Sondaggi e ricerche

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento
Imprese, società, istituti ed altri organismi o soggetti privati, ai soli fini del compimento di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il sondaggio o la ricerca devono essere effettuati per scopi puntualmente determinati e legittimi, noti all'interessato.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati
Il trattamento può riguardare i dati attinenti ai soggetti che abbiano manifestato il proprio consenso informato e che abbiano risposto a questionari o ad interviste effettuate nell'ambito di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il consenso deve essere manifestato in ogni caso per iscritto.

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

3) Conservazione dei dati
Il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente, mediante un riferimento ad una qualsiasi altra informazione.

I dati personali, individuali o aggregati, devono essere distrutti o resi anonimi subito dopo la raccolta, e comunque non oltre la fase contestuale alla registrazione dei campioni raccolti. La registrazione deve essere effettuata senza ritardo anche nel caso in cui i campioni siano stati raccolti in numero elevato.

Entro tale ambito temporale, resta ferma la possibilità per il titolare della raccolta, nonché per i suoi responsabili o incaricati, di utilizzare i dati personali al fine di verificare presso gli interessati la veridicità o l'esattezza dei campioni.

4) Comunicazione dei dati
I dati sensibili non possono essere né comunicati, né diffusi.

I campioni del sondaggio o della ricerca possono essere comunicati o diffusi in forma

individuale o aggregata, sempreché non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili.

Capo III - Attività di elaborazione di dati

1) Soggetti ai quali è rilasciata l'autorizzazione

Imprese, società, istituti ed altri organismi o soggetti privati, titolari autonomi di un'attività svolta nell'interesse di altri soggetti, e che presuppone l'elaborazione di dati ed altre operazioni di trattamento eseguite in materia di lavoro ovvero a fini contabili, retributivi, previdenziali, assistenziali e fiscali.

2) Prescrizioni applicabili

Il trattamento è regolato dalle autorizzazioni:

a) n. 1/2004, rilasciata il 30 giugno 2004, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione;
b) n. 4/2004, rilasciata il 30 giugno 2004, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati, qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Capo IV - Attività di selezione del personale

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

La presente autorizzazione è rilasciata, anche senza richiesta, alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di attività svolta anche di propria iniziativa nell'interesse di terzi, ai soli fini della ricerca o della selezione del personale.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la loro raccolta è giustificata da scopi determinati e legittimi ed è strettamente indispensabile per instaurare tale rapporto.

Il trattamento dei dati idonei a rivelare lo stato di salute dei familiari o dei conviventi dei candidati è consentito con il consenso scritto degli interessati e qualora sia finalizzato al riconoscimento di uno specifico beneficio in favore dei candidati, in particolare ai fini di un'assunzione obbligatoria o del riconoscimento di un titolo derivante da invalidità o infermità, da eventi bellici o da ragioni di servizio.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Il trattamento deve riguardare le sole informazioni strettamente pertinenti a tale finalità, sia in caso di risposta a questionari inviati anche per via telematica, sia nel caso in cui i candidati forniscano dati di propria iniziativa, in particolare attraverso l'invio di curricula.

Non è consentito il trattamento dei dati:

a) idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni a carattere religioso, filosofico, politico o sindacale, l'origine razziale ed etnica, e la vita sessuale;
b) inerenti a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;
c) in violazione delle norme in materia di pari opportunità o volte a prevenire discriminazioni.

3) Comunicazione e diffusione dei dati
I dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui ai punti 1) e 2), a soggetti pubblici o privati che siano specificamente menzionati nella dichiarazione di consenso dell'interessato.

I dati sensibili non possono essere diffusi.

4) Norme finali
Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti.

CAPO V - MEDIAZIONE A FINI MATRIMONIALI

1) Soggetti ai quali è rilasciata l'autorizzazione
La presente autorizzazione è rilasciata alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati che esercitano, anche attraverso agenzie autorizzate, un'attività di mediazione a fini matrimoniali o di instaurazione di un rapporto di convivenza.

2) Finalità del trattamento
L'autorizzazione è rilasciata ai soli fini dell'esecuzione dei singoli incarichi conferiti in conformità alle leggi e ai regolamenti.

3) Interessati ai quali i dati si riferiscono
Il trattamento può riguardare i soli dati sensibili attinenti alle persone direttamente interessate al matrimonio o alla convivenza.

Non è consentito il trattamento di dati relativo a persone minori di età in base all'ordinamento del Paese di appartenenza o, comunque, in base alla legge italiana.

4) Categorie di dati oggetto di trattamento
Il trattamento può riguardare i soli dati e le sole operazioni che risultino indispensabili in relazione allo specifico profilo o alla personalità descritto o richiesto dalle persone interessate al matrimonio o alla convivenza.

I dati devono essere forniti personalmente dai medesimi interessati.

L'informativa preliminare al consenso scritto deve porre in particolare evidenza le categorie di dati trattati e le modalità della loro comunicazione a terzi.

5) Comunicazione dei dati
I dati possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lett. c), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

L'eventuale diffusione anche per via telematica di taluni dati sensibili deve essere oggetto di apposita autorizzazione di questa Autorità.

6) Norme finali
Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti, in particolare nell'ambito della legge penale e della disciplina di pubblica sicurezza, nonché in materia di tutela dei minori.

35

CAPO VI - PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati idonei a rivelare lo stato di salute

Il trattamento dei dati idonei a rivelare lo stato di salute deve essere effettuato anche nel rispetto dell'autorizzazione n. 2/2004, rilasciata il 30 giugno 2004.

Il trattamento dei dati genetici non è consentito nei casi previsti dalla presente autorizzazione.

2) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, dagli articoli 31 e seguenti del Codice e dall'Allegato B) al Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità indicate nei capi che precedono.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Resta inoltre fermo l'obbligo di informare l'interessato, ai sensi dell'art. 13, commi 1, 4 e 5 del Codice, anche quando i dati sono raccolti presso terzi.

3) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e) del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità ovvero per adempiere agli obblighi o agli incarichi menzionati nei precedenti capi. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

Restano fermi i diversi termini di conservazione previsti dalle leggi o dai regolamenti.

Resta altresì fermo quanto previsto nel capo II in materia di sondaggi e di ricerche.

4) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

5) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento dalla normativa

comunitaria, che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dalla legge 20 maggio 1970, n. 300;
b) dalla legge 5 giugno 1990, n. 135;

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici, previsti anche dai codici deontologici e di buona condotta adottati in attuazione dell'art. 12 del Codice.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati.

6) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 5/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. c), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario per svolgere una investigazione difensiva ai sensi della legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, e che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato il diritto sia di rango pari a quello dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 135 del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

(*) *G.U.* 14 agosto 2004, n. 190.

Considerato che il Garante ha rilasciato un'autorizzazione di ordine generale relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale (n. 2/2004, rilasciata il 30 giugno 2004), anche in riferimento alle predette finalità di ordine giudiziario;

Considerato che numerosi trattamenti aventi tali finalità sono effettuati con l'ausilio di investigatori privati, e che è pertanto opportuno integrare anche le prescrizioni dell'autorizzazione n. 2/2004 mediante un ulteriore provvedimento di ordine generale che tenga conto dello specifico contesto dell'investigazione privata, anche al fine di armonizzare le prescrizioni da impartire alla categoria;

Considerato che ulteriori misure ed accorgimenti saranno prescritti dal Garante all'atto della sottoscrizione del citato codice di deontologia e di buona condotta in via di emanazione (art. 12 del Codice);

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visti gli articoli 42 e seguenti del Codice in materia di trasferimento di dati personali all'estero;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Gaetano Rasi;

Autorizza:

gli investigatori privati a trattare i dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata, anche senza richiesta, alle persone fisiche e giuridiche, agli istituti, agli enti, alle associazioni e agli organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

2) Finalità del trattamento

Il trattamento può essere effettuato unicamente per l'espletamento dell'incarico ricevuto dai soggetti di cui al punto 1) e in particolare:

a) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto, che, quando i dati siano idonei a rivelare lo

stato di salute e la vita sessuale dell'interessato, deve essere di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;

b) su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (art. 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397).

Restano ferme le altre autorizzazioni generali rilasciate ai fini dello svolgimento delle investigazioni in relazione ad un procedimento penale o per l'esercizio di un diritto in sede giudiziaria, in particolare:

a) nell'ambito dei rapporti di lavoro (autorizzazione n. 1/2004, rilasciata il 30 giugno 2004);
b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2004, rilasciata il 30 giugno 2004);
c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione n. 3/2004, rilasciata il 30 giugno 2004);
d) da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione n. 4/2004, rilasciata il 30 giugno 2004);
e) relativamente ai dati di carattere giudiziario (autorizzazione n. 7/2004, rilasciata il 30 giugno 2004).

3) Categorie di dati e interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili di cui all'art. 4, comma 1, lett. d) del Codice, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità di cui al punto 1), che non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

I dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti.

4) Modalità di trattamento

Gli investigatori privati non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di dati. Tali attività possono essere eseguite esclusivamente sulla base di un apposito incarico conferito per iscritto, anche da un difensore, per le esclusive finalità di cui al punto 2).

L'atto di incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa.

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità di cui al punto 2).

L'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'art. 13 del Codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati.

Nel caso in cui i dati sono raccolti presso terzi, è necessario informare l'interessato e acquisire il suo consenso scritto (art. 13, commi 1, 4 e 5 e art. 26, comma 4, del Codice), solo se i dati sono trattati per un periodo superiore a quello strettamente necessario per esercitare il diritto in sede giudiziaria o per svolgere le investigazioni difensive, oppure se i dati sono utilizzati per ulteriori finalità non incompatibili con quelle precedentemente perseguite.

Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

L'investigatore privato deve eseguire personalmente l'incarico ricevuto e non può avvalersi di altri investigatori non indicati nominativamente all'atto del conferimento dell'incarico.

Nel caso in cui si avvalga di collaboratori interni designati quali responsabili o incaricati del trattamento in conformità a quanto previsto dagli articoli 29 e 30 del Codice, l'investigatore privato deve vigilare con cadenza almeno settimanale sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Per quanto non previsto nella presente autorizzazione, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato nel rispetto delle ulteriori prescrizioni contenute nell'autorizzazione generale n. 2/2004 e, allorché rilasciata, in quella prevista dall'art. 90 del Codice, in particolare per ciò che riguarda le informazioni relative ai nascituri e ai dati genetici.

Il trattamento dei dati deve inoltre rispettare le prescrizioni del codice di deontologia e di buona condotta di cui all'articolo 135 del Codice in via di definizione.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e), del Codice i dati sensibili possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto.

A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico.

La mera pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

6) Comunicazione e diffusione dei dati

I dati possono essere comunicati unicamente al soggetto che ha conferito l'incarico.

I dati non possono essere comunicati ad un altro investigatore privato, salvo che questi sia stato indicato nominativamente nell'atto di incarico e la comunicazione sia necessaria per lo svolgimento dei compiti affidati.

I dati idonei a rivelare lo stato di salute possono essere comunicati alle autorità competenti solo se è necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

36

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti dalla normativa comunitaria, ovvero da norme di legge o di regolamento, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare:

a) dagli articoli 4 (impianti e apparecchiature per finalità di controllo a distanza dei lavoratori) e 8 (indagini sulle opinioni del lavoratore o su altri fatti non rilevanti ai fini della valutazione dell'attitudine professionale) della legge 20 maggio 1970, n. 300 e dall'art. 10 (indagini sulle opinioni del lavoratore e trattamenti discriminatori) del d.lg. 10 settembre 2003, n. 276;
b) dalla legge 5 giugno 1990, n. 135, in materia di sieropositività e di infezione da HIV;
c) dalle norme processuali o volte a prevenire discriminazioni;
d) dall'art. 734-*bis* del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano fermi, in particolare, gli obblighi previsti in tema di liceità e di correttezza nell'uso di strumenti o apparecchiature che permettono la raccolta di informazioni anche sonore o visive, ovvero in tema di accesso a banche dati o di cognizione del contenuto della corrispondenza e di comunicazioni o conversazioni telefoniche, telematiche o tra soggetti presenti.

Resta ferma la facoltà per le persone fisiche di trattare direttamente dati per l'esclusivo fine della tutela di un proprio diritto in sede giudiziaria, anche nell'ambito delle investigazioni relative ad un procedimento penale. In tali casi, il Codice non si applica anche se i dati sono comunicati occasionalmente ad una autorità giudiziaria o a terzi, sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione (art. 5, comma 3, del Codice).

9) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 6/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

Il Presidente
Rodotà

Il Relatore
Rasi

Il Segretario generale
Buttarelli

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

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto l'art. 4, comma 1, lett. e), del Codice, il quale individua i dati giudiziari;

Visti, in particolare, gli articoli 21, comma 1, e 27 del Codice, che consentono il trattamento di dati giudiziari, rispettivamente, da parte di soggetti pubblici e di privati o di enti pubblici economici, soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni eseguibili;

Visti gli articoli 20, commi 2 e 4, e le disposizioni relative a specifici settori di cui alla Parte II, del Codice e, in particolare, i Capi III e IV del Titolo IV, nel quale sono indicate finalità di rilevante interesse pubblico che rendono ammissibile il trattamento di dati giudiziari da parte di soggetti pubblici;

Visto l'art. 22 del Codice, il quale prevede i principi applicabili al trattamento di dati sensibili e giudiziari da parte di soggetti pubblici;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Visti gli articoli 51 e 52 del Codice in materia di informatica giuridica e ritenuta la necessità di favorire la prosecuzione dell'attività di documentazione, studio e ricerca in campo giuridico, in particolare per quanto riguarda la diffusione di dati relativi a precedenti giurisprudenziali, in ragione anche dell'affinità che tali attività presentano con quelle di manifestazione del pensiero già disciplinate dall'art. 137 del Codice;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice;

(*) *G.U.* 14 agosto 2004, n. 190.

37

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Giuseppe Santaniello;

Autorizza:

i trattamenti di dati giudiziari per le finalità di rilevante interesse pubblico di seguito specificate ai sensi degli articoli 21 e 27 del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

CAPO I - RAPPORTI DI LAVORO

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, a persone fisiche e giuridiche, enti, associazioni ed organismi che:

a) sono parte di un rapporto di lavoro;
b) utilizzano prestazioni lavorative anche atipiche, parziali o temporanee;
c) conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

Il trattamento deve essere indispensabile per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario.

L'autorizzazione è altresì rilasciata a soggetti che in relazione ad un'attività di composizione di controversie esercitata in conformità alla legge svolgono un trattamento indispensabile al medesimo fine.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti a soggetti che hanno assunto o intendono assumere la qualità di:

a) lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione lavoro, ovvero di associati anche in compartecipazione o di titolari di borse di lavoro e di rapporti analoghi;

b) amministratori o membri di organi esecutivi o di controllo;
c) consulenti e liberi professionisti, agenti, rappresentanti e mandatari.

CAPO II - ORGANISMI DI TIPO ASSOCIATIVO E FONDAZIONI

1) Ambito di applicazione e finalità del trattamento
L'autorizzazione è rilasciata anche senza richiesta:
a) ad associazioni anche non riconosciute, ivi compresi partiti e movimenti politici, associazioni ed organizzazioni sindacali, patronati, associazioni a scopo assistenziale o di volontariato, a fondazioni, comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché a cooperative sociali e società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818;
b) ad enti ed associazioni anche non riconosciute che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi.

Il trattamento deve essere indispensabile per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo.

2) Interessati ai quali i dati si riferiscono
Il trattamento può riguardare dati attinenti:
a) ad associati, soci e aderenti, nonché, nei casi in cui l'utilizzazione dei dati sia prevista dall'atto costitutivo o dallo statuto, a soggetti che presentano richiesta di ammissione o di adesione;
b) a beneficiari, assistiti e fruitori delle attività o dei servizi prestati dall'associazione, dall'ente o dal diverso organismo.

CAPO III - LIBERI PROFESSIONISTI

1) Ambito di applicazione e finalità del trattamento
L'autorizzazione è rilasciata anche senza richiesta ai:
a) liberi professionisti, anche associati, tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96 o alle norme di attuazione dell'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza;
b) soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'art. 34 del regio decreto legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato;
c) sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

2) Interessati ai quali i dati si riferiscono
Il trattamento può riguardare dati attinenti ai clienti.

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

CAPO IV - IMPRESE BANCARIE ED ASSICURATIVE ED ALTRI TRATTAMENTI

1) Ambito di applicazione e finalità del trattamento
L'autorizzazione è rilasciata, anche senza richiesta:
a) ad imprese autorizzate o che intendono essere autorizzate all'esercizio dell'attività

bancaria e creditizia, assicurativa o dei fondi pensione, anche se in stato di liquidazione coatta amministrativa, ai fini:

1. dell'accertamento, nei casi previsti dalle leggi e dai regolamenti, del requisito di onorabilità nei confronti di soci e titolari di cariche direttive o elettive;
2. dell'accertamento, nei soli casi espressamente previsti dalla legge, di requisiti soggettivi e di presupposti interdittivi;
3. dell'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana;
4. dell'accertamento di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, in relazione ad illeciti direttamente connessi con la medesima attività. Per questi ultimi casi, limitatamente ai trattamenti di dati registrati in una specifica banca di dati ai sensi dell'art. 4, comma 1, lett. p), del Codice, il titolare deve inviare al Garante una dettagliata relazione sulle modalità del trattamento;

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

c) alle società di intermediazione mobiliare, alle società di investimento a capitale variabile, e alle società di gestione del risparmio e dei fondi pensione, ai fini dell'accertamento dei requisiti di onorabilità in applicazione della normativa in materia di intermediazione finanziaria e di previdenza o di forme pensionistiche complementari, e di eventuali altre norme di legge o di regolamento.

2) Ulteriori trattamenti

L'autorizzazione è rilasciata altresì:

a) a chiunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato e i dati siano trattati esclusivamente per tale finalità e per il periodo strettamente necessario per il suo perseguimento;

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

c) a persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

Il trattamento deve essere necessario:

1. per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero di un diritto della personalità o di un altro diritto fondamentale ed inviolabile;
2. su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (articolo 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397);

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

e) a chiunque, ai fini dell'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalla normativa in materia di appalti.

Capo V - Documentazione giuridica

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati per

finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali, nel rispetto di quanto previsto dagli articoli 51 e 52 del Codice.

CAPO VI - PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati trattati
Possono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2) Modalità di trattamento
Il trattamento dei dati deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto agli obblighi, ai compiti o alle finalità precedentemente indicati. Fuori dei casi previsti dai Capi IV, punto 2 e V, o nei quali la notizia è acquisita da fonti accessibili a chiunque, i dati devono essere forniti dagli interessati nel rispetto della disciplina prevista dal d.P.R. 14 novembre 2002, n. 313.

3) Conservazione dei dati
Con riferimento all'obbligo previsto dall'art. 11, comma 1, lett. e) del Codice, i dati possono essere conservati per il periodo di tempo previsto da leggi o regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per le finalità perseguite.

Ai sensi dell'art. 11, comma 1, lett. c), d) ed e) del Codice, i soggetti autorizzati verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi. Al fine di assicurare che i dati siano strettamente pertinenti, non eccedenti e indispensabili rispetto alle finalità medesime, i soggetti autorizzati valutano specificamente il rapporto tra i dati e i singoli obblighi, compiti e prestazioni. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente gli obblighi, i compiti e le prestazioni.

4) Comunicazione e diffusione
I dati possono essere comunicati e, ove previsto dalla legge, diffusi, a soggetti pubblici o privati, nei limiti strettamente indispensabili per le finalità perseguite e nel rispetto, in ogni caso, del segreto professionale e delle altre prescrizioni sopraindicate.

5) Richieste di autorizzazione
I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione al Garante, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante si riserva l'adozione di ogni altro provvedimento per i trattamenti non considerati nella presente autorizzazione.

Per quanto riguarda invece i trattamenti disciplinati nel presente provvedimento, il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle relative prescrizioni, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali

37

non considerate nella presente autorizzazione.

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute nell'art. 8 della legge 20 maggio 1970, n. 300, fatto salvo dall'art. 113 del Codice, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore e dall'art. 10 del d.lg. 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare determinate indagini o comunque trattamenti di dati ovvero di preselezione di lavoratori.

6) Efficacia temporale e disciplina transitoria
La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 7/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

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

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

38 Disposizioni in materia di comunicazione e di propaganda politica (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORI il prof. Giuseppe Santaniello e il dott. Mauro Paissan;

Premesso:

1. Finalità del provvedimento

Le iniziative di propaganda elettorale intraprese da partiti, organismi politici, comitati promotori, sostenitori e singoli candidati costituiscono un momento particolarmente significativo della partecipazione alla vita democratica (art. 49 Cost.) che deve però rispettare i diritti e le libertà fondamentali delle persone cui si riferiscono le informazioni utilizzate.

Con l'approssimarsi di una tornata di consultazioni elettorali, l'Autorità ritiene necessario richiamare l'attenzione sulle garanzie vigenti dopo l'entrata in vigore del Codice in materia di protezione dei dati personali che ha sostituito la legge n. 675/1996 (d.lg. 30 giugno 2003, n. 196), e fornire in particolare indicazioni sull'informativa alle persone interessate.

A tal fine, verranno segnalati in questo provvedimento i casi in cui si possono utilizzare dati personali a fini di propaganda informando gli interessati, ma senza richiedere il loro consenso, e i casi in cui al contrario il consenso è necessario. Saranno poi evidenziati i diritti degli interessati di conoscere le modalità di utilizzazione dei dati che li riguardano e di far interrompere l'attività di propaganda nei propri confronti.

2. Dati tratti da registri o elenchi pubblici

a) Quando si può prescindere dal consenso

È possibile utilizzare dati personali senza il consenso degli interessati per la propaganda elettorale solo se i dati sono estratti da fonti "pubbliche" nel senso proprio del termine, ovvero conoscibili da chiunque senza limitazioni.

Questa ipotesi ricorre quando si utilizzano registri, elenchi, atti o documenti che sono detenuti da un soggetto pubblico, e al tempo stesso sono liberamente accessibili –senza discriminazioni– in base ad un'espressa disposizione di legge o di regolamento.

Se non ricorre questa condizione, l'amministrazione o l'ente pubblico che detiene i dati non può permetterne l'utilizzo a partiti, forze politiche o candidati, dovendo utilizzarli solo per svolgere funzioni istituzionali e osservando i presupposti e i limiti stabiliti, caso per caso, da norme generali o speciali contenute anche nel Codice (art. 18, commi 2 e 3, d.lg. cit.), che a volte rendono i dati "pubblici" solo per permetterne l'uso per alcune finalità.

Possono essere ad esempio utilizzate per la propaganda elettorale:

a) le c.d. liste elettorali (ovvero, le liste degli aventi diritto al voto detenute presso i

(*) Provvedimento 12 febbraio 2004, in *G.U.* 24 febbraio 2004, n. 45.

comuni), le quali "possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo … o per il perseguimento di un interesse collettivo o diffuso" (art. 51 d.P.R. 20 marzo 1967 n. 223, come modificato dall'art. 177, comma 5, del d.lg. n. 196/2003);

b) gli elenchi di iscritti ad albi e collegi professionali (art. 61, comma 2, d.lg. n. 196/2003), e i dati contenuti in taluni registri detenuti dalle camere di commercio;

c) altri elenchi e registri in materia di elettorato attivo e passivo. Sebbene sia opportuno al riguardo un chiarimento normativo, risultano utilizzabili a fini di propaganda le seguenti fonti:
   - l'elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo (formato sulla base dei dati contenuti nelle liste elettorali e trasmesso agli uffici consolari: art. 4, commi 1 e 5, d.l. 24 giugno 1994, n. 408, convertito con l. 3 agosto 1994, n. 483);
   - le c.d. liste aggiunte dei cittadini elettori di uno Stato membro dell'Unione europea (istituite a livello comunale anche in riferimento ai dieci Paesi che vi faranno parte dal 1° maggio 2004), residenti in Italia e che intendano ivi esercitare il diritto di voto alle elezioni del Parlamento europeo (d.lg. n. 197/1996; circolare Min. interno 30 dicembre 2003, n. 134, in Gazzetta Ufficiale 8 gennaio 2004, n. 5; v. anche Com. della Commissione europea COM (2003) 174 def. dell'8 aprile 2003);
   - l'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle liste elettorali, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (AIRE) e degli schedari consolari (art. 5 l. 27 dicembre 2001, n. 459);
   - l'elenco dei cittadini italiani residenti all'estero aventi diritto al voto per l'elezione del Comitato degli italiani all'estero (Comites), reso pubblico con modalità definite con un regolamento (artt. 13 e 26 l. 23 ottobre 2003, n. 286; art. 5, comma 1, l. 27 dicembre 2001, n. 459; art. 5, comma 1, d.P.R. 2 aprile 2003, n. 104).

Va comunque segnalato a chi utilizza fonti "pubbliche" la necessità di porre attenzione:
- alle modalità prescritte in alcuni casi per accedere ai dati (ad esempio, per identificare il soggetto che ne ottiene copia);
- alla circostanza che i dati siano accessibili al pubblico solo per finalità specifiche. Non possono ad esempio ritenersi utilizzabili a fini di propaganda le informazioni sugli studenti ricavabili dalla pubblicazione degli esiti di attività scolastiche, oppure gli elenchi di immigrati o affetti da determinate malattie o di beneficiari di provvidenze economiche concesse da amministrazioni comunali a portatori di handicap, invalidi e indigenti, le graduatorie per il ricovero in istituti di sostegno o in case di cura, le liste di assegnazione degli alloggi di edilizia residenziale pubblica, gli elenchi dei beneficiari di parcheggi riservati a persone con ridotta capacità motoria;
- alle condizioni e ai limiti eventualmente posti per stabilire come utilizzare i dati dopo averne ottenuta copia. Tale utilizzazione deve poi avvenire sempre in termini compatibili con gli scopi per i quali i dati sono stati raccolti e registrati (art. 11, comma 1, lett. b), d.lg. n. 196/2003), e che in alcuni casi è possibile solo se si indica la data della loro estrazione e l'origine.

Non sono invece utilizzabili per la propaganda elettorale altre fonti della pubblica amministrazione, quali, ad esempio:

1) atti anagrafici e dello stato civile

I dati degli iscritti nelle anagrafi comunali della popolazione non possono essere forniti in alcun modo a privati per scopi di propaganda elettorale (tantomeno in forma elaborata di elenchi di intestatari di nuclei familiari), anche se il richiedente è un amministratore locale o il titolare di una carica elettiva.

Possono rivolgere una motivata richiesta di rilascio di elenchi solo le amministrazioni pubbliche per esclusivo uso di pubblica utilità (art. 34 d.P.R. n. 223/1989). Questa garan-

zia opera anche nei confronti del comune, il quale può utilizzare anch'esso i dati anagrafici che detiene solo per usi di pubblica utilità, anche in caso di comunicazione istituzionale (art. 177 d.lg. n. 196/2003), sicché tali dati non possono essere utilizzati per la propaganda elettorale o per pubbliche relazioni di carattere personale.

Anche gli atti dello stato civile sono soggetti ad un regime ben diverso da quello delle liste elettorali (art. 450 cod. civ.; d.P.R. n. 396/2000) e non possono quindi ritenersi "pubblici" nel senso proprio del termine sopra indicato;

2) dati tratti dalle liste elettorali di sezione già utilizzate nei seggi

Le liste elettorali di sezione già utilizzate nei singoli seggi e sulle quali sono stati annotati dati relativi alle persone che hanno votato non possono essere utilizzate a fini di propaganda. Tali liste contengono dati particolari a volte sensibili (idonei a rivelare l'effettiva partecipazione dei cittadini alle votazioni o, in tutto o in parte, a particolari consultazioni), e sono verificabili da ogni cittadino entro quindici giorni dal deposito in cancelleria, solo per il controllo sulla regolarità delle operazioni elettorali (art. 62 d.P.R. 16 maggio 1960 n. 570, recante il t.u. delle leggi per la composizione e l'elezione degli organi delle amministrazioni comunali, applicabile anche alle elezioni regionali ex art. 1, comma 6, l. 17 febbraio 1968, n. 108). A tali liste non è applicabile né la disciplina di cui al citato art. 51 del d.P.R. n. 223/1967, né il diritto di accesso riconosciuto ai titolari di cariche elettive ai fini dell'espletamento del relativo mandato;

3) dati annotati da scrutatori e rappresentanti di lista

Scrutatori e rappresentanti di lista, nell'esercitare funzioni affidate o consentite dalla legge e connesse al regolare svolgimento delle operazioni di voto, possono venire a conoscenza di dati anche sensibili (quali quelli relativi a coloro che hanno votato o meno presso una determinata sezione), da trattare con ogni opportuna cautela anche a garanzia della libertà e segretezza del voto, soprattutto nei casi in cui (come i referendum abrogativi o le votazioni di ballottaggio) la partecipazione al voto o l'astensione può evidenziare di per sé una particolare opzione politica. In particolare, tali soggetti non possono compilare elenchi di persone astenutesi dal voto, specie al fine di invitarle a votare in successivi appuntamenti elettorali;

4) schedari istituiti presso gli uffici consolari

Ai dati anagrafici dei cittadini iscritti negli schedari istituiti presso gli uffici consolari ai sensi dell'art. 67 del d.P.R. n. 200/1967, possono ritenersi applicabili le disposizioni sul rilascio degli atti anagrafici, che prevedono la possibilità di rilasciare elenchi degli iscritti nell'anagrafe della popolazione residente unicamente alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità.

3. Casi equiparati ai registri pubblici: elenchi telefonici

La disciplina degli elenchi telefonici, cartacei ed elettronici, è stata oggetto di recenti modifiche che hanno mutato in radice la loro natura in attuazione di norme comunitarie.

Il nuovo regime sarà attuato prevedibilmente nella seconda metà del 2004 e la propaganda sarà possibile in futuro solo nei confronti di chi vi acconsenta.

Nel frattempo, gli elenchi della telefonia fissa (e non anche quelli della telefonia mobile) restano utilizzabili per la propaganda elettorale solo mediante invio di posta ordinaria o chiamate telefoniche effettuate da un operatore, a meno che gli interessati si siano opposti (cfr. art. 55 e 75 d.lg. 1 agosto 2003, n. 259).

4. Propaganda lecita con il consenso

Fuori dei predetti casi, benché la propaganda elettorale abbia una sua specificità rispetto alla comunicazione commerciale e di *marketing*, non è possibile effettuarla senza un consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente l'utilizzo dei dati a tale fine (e sia espresso in forma scritta se, come si vedrà, i dati hanno natura sensibile), in particolare quando si ricorre ai seguenti mezzi:

a) invio di fax;

b) invio di messaggi *Sms* e *Mms*;
c) chiamate telefoniche senza l'intervento di un operatore.
Ci si riferisce all'utilizzo di sistemi automatizzati che effettuano chiamate vocali preregistrate senza l'intervento, caso per caso, di un operatore;
d) chiamate di ogni tipo a terminali di telefonia mobile.

Il regime transitorio menzionato per la telefonia fissa non riguarda la telefonia mobile.

Senza il consenso preventivo e informato dell'abbonato, o del reale ed unico utilizzatore della scheda di traffico prepagato, non è lecito effettuare chiamate vocali di propaganda a terminali mobili, automatizzate e non, o inviare -anche in questo caso- messaggi *Sms* o *Mms* anche tramite siti *web*.

La volontà dell'interessato deve essere manifestata prima della chiamata o del messaggio e non può essere elusa inviando senza consenso un primo messaggio con il quale si chieda di aderire all'invio di ulteriori messaggi di propaganda.

Il consenso deve essere espresso in forma chiara (specificando la finalità di propaganda specie quando è richiesto con una formula ampia, riferita anche a scopi commerciali e di *marketing*) e "positiva" (anziché con una modalità di silenzio-assenso);

e) indirizzi di posta elettronica.

Gli indirizzi di posta elettronica recano dati personali che non rientrano tra le fonti "pubbliche" liberamente accessibili da chiunque e sono utilizzabili solo sulla base di un libero consenso (artt. 24 e 130 d.lg. n. 196/2003; v. Provv. del Garante 29 maggio 2003 sul c.d. *spamming*, in *www.garanteprivacy.it*).

Il consenso è necessario anche quando gli indirizzi o altri dati personali:
- sono ricavati da pagine *web*;
- sono formati ed utilizzati automaticamente con un *software* senza l'intervento di un operatore, oppure in mancanza di una verifica della loro attuale attivazione o dell'identità del destinatario;
- quando gli indirizzi non sono registrati dopo l'invio dei messaggi.

La circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi di qualunque genere.

Il principio del consenso si applica anche per:
- i dati di utenti che prendono parte a forum o *newsgroup*, resi conoscibili in Internet per partecipare ad una determinata discussione e che non sono utilizzabili per fini diversi senza un consenso specifico (art. 11, comma 1, lettere a) e b), d.lg. n. 196/2003);
- gli indirizzi compresi nella lista "anagrafica" di abbonati ad un Internet provider, o pubblicati su siti *web* per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale od associativa;
- comunicazioni inviate a gestori anche privati di siti web utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio;

f) iscritti ad associazioni politiche o a partiti.

L'utilizzazione da parte di partiti o associazioni politiche di dati relativi a loro iscritti, a simpatizzanti o a partecipanti ad iniziative politiche in occasione delle quali si raccolgano informazioni sul loro conto (come pure di dati acquisiti sottoscrivendo petizioni, proposte di legge, richieste di referendum o raccolte di firme), comporta un trattamento di dati personali "sensibili".

In questi casi il consenso specifico deve essere manifestato per iscritto.

Quando il consenso è raccolto all'atto di adesione all'organizzazione, occorre un'idonea informativa collegata ad un chiaro contesto interno risultante dallo statuto o da altri atti dell'organizzazione noti agli interessati (v. comunicato stampa del Garante del 16 ottobre 1997, in *Bollettino* n. 2, p. 82). Particolare attenzione va prestata poi alla chiarezza dell'informativa e alla formula di consenso presenti su siti *web* che raccolgano dati sensibili di aderenti o simpatizzanti anche ai fini dell'invio di *newsletter* a contenuto politico.

Se i dati sono acquisiti nell'ambito di altri eventi politici, l'informativa deve evidenziare parimenti con chiarezza l'utilizzazione dei dati che si prevede in aggiunta alle finalità perseguite in via principale (ad esempio, nel caso in cui si intenda comunicare i dati a singoli candidati o a comitati elettorali delle medesime formazioni politiche).

Ogni eventuale comunicazione ad altri soggetti (organizzazioni di simpatizzanti, enti, associazioni, società e persone fisiche non direttamente connesse all'attività del titolare del trattamento), indipendente ed ulteriore rispetto alle finalità della raccolta dei dati, deve essere basata su un consenso distinto da quello previsto per il predetto trattamento "principale";

g) utenti o aderenti a organizzazioni non politiche.

Quando si presta un'attività (ad esempio, assicurativa) o un servizio (ad esempio, presso una casa di cura) o si svolge un'attività associativa no-profit a scopo diverso da quello politico, non è lecito utilizzare indirizzari o altri dati personali per propagandare candidati interni alla società, all'ente o all'associazione o da questi sostenuti (v. Provv. Garante del 5 ottobre 1999 e del 9 ottobre 2000, in Bollettino n. 14/15, p. 17 s.).

L'utilizzazione a fini di propaganda dei dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politica, è possibile solo quando ricorrono le seguenti condizioni:

- venga disposta legittimamente in base all'ordinamento interno;
- le modalità di utilizzo dei dati a fini di propaganda siano compatibili con gli scopi principali perseguiti dall'associazione o altro organismo;
- sia prevista specificamente nell'informativa resa agli iscritti al momento dell'adesione o del suo rinnovo.

5. Dati acquisiti nell'esercizio di un mandato

I titolari di alcune cariche elettive, nel corso del mandato e sulla base di specifiche disposizioni volte a favorire il suo pieno esercizio, possono venire lecitamente a conoscenza di dati personali (cfr., ad esempio, art. 37 d.lg. 18 agosto 2000, n. 267; cfr. anche parere del 20 maggio 1998, in Bollettino n. 4, pag. 7 s. e del 7 marzo 2001, in Bollettino n. 18, p. 24) da utilizzare, anche a fini di trasparenza e buon andamento, per scopi pertinenti all'esercizio del mandato che possono rendere legittimo anche un eventuale contatto con gli interessati.

È in questo quadro illegittima l'eventuale richiesta di ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per la propaganda anche dopo la scadenza dal mandato.

Possono al contrario essere utilizzati i dati personali raccolti direttamente dal titolare della carica elettiva, nel quadro delle relazioni interpersonali con cittadini ed elettori.

6. Uso di dati raccolti da terzi

Diversi interessati divengono consapevoli solo a seguito di una loro contestazione che il consenso espresso in precedenza in modo generico è stato utilizzato anche per attività di propaganda elettorale.

Il candidato o l'organismo politico, quando acquisisce i dati da un privato che li ha raccolti in base a formule di consenso vaghe, riferite a scopi di vario tipo non meglio precisati (spesso, prevalentemente di tipo commerciale), ha l'onere di verificare in modo adeguato –anche con modalità a campione e avvalendosi della figura del mandatario elettorale: cfr. art. 7 l. 10 dicem-

38

bre 1993, n. 515– che gli interessati siano stati informati in modo specifico e abbiano prestato un consenso idoneo, che è validamente espresso solo se è manifestato "specificamente in riferimento ad un trattamento chiaramente individuato … e se sono state rese all'interessato le informazioni di cui all'articolo 13" del Codice (art. 23, comma 3, d.lg. n. 196/2003).

Tale consenso deve essere manifestato liberamente, in forma differenziata rispetto alla prestazione di beni e servizi, in modo esplicito e documentato per iscritto: altrimenti, il trattamento è illecito e i dati sono inutilizzabili (art. 11, comma 2, d.lg. n. 196/2003).

Sull'organismo politico o candidato grava altresì l'onere di verificare –anche avvalendosi del predetto mandatario– che l'informativa sia fornita in caso di servizi di propaganda curati da terzi che inviino lettere o messaggi di propaganda utilizzando fonti conoscitive accessibili a chiunque.

7. Informativa agli interessati

Chi effettua attività di propaganda elettorale, anche se utilizza dati "pubblici" nel senso proprio del termine, deve fornire agli interessati la prevista informativa (art. 13 d.lg. n. 196/2003).

Si può adempiere a tale obbligo anche attraverso un'informazione sintetica, ma efficace, ed utilizzando, a titolo esemplificativo, una formula di tenore analogo al seguente:

"I dati che ci ha fornito liberamente (oppure: che sono stati estratti da …) sono utilizzati da … solo a fini di propaganda elettorale, anche con strumenti informatici, e non saranno comunicati a terzi (eventuale: salvo che all'organizzazione che cura le spedizioni). Può in ogni momento accedere ai dati, opporsi al loro trattamento o chiedere di integrarli, rettificarli o cancellarli, rivolgendosi a … (indicare almeno un responsabile del trattamento, se è stato designato)".

Questa informativa deve essere inserita nel materiale di propaganda caratterizzato da lettere o da messaggi di posta elettronica.

Analoghe formule sintetiche possono essere utilizzate in caso di chiamate a numeri estratti da elenchi telefonici, fornendo all'inizio della conversazione un'informativa che indichi subito chi effettua la propaganda, la finalità della chiamata e i diritti del ricevente.

Chi effettua propaganda, qualora non ritenga di inviare il predetto materiale potrebbe:
- estrarre i dati da pubblici registri, elenchi, atti o altri documenti conoscibili da chiunque senza contattare tutti gli interessati;
- oppure, potrebbe inviare materiale propagandistico di dimensioni ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non permetta di inserire efficacemente un'idonea informativa anche di tenore sintetico.

Limitatamente a questi ultimi due casi, il Garante ritiene proporzionato rispetto ai diritti degli interessati sollevare il soggetto che utilizza i dati per esclusivi fini di propaganda elettorale dall'obbligo di fornire l'informativa. Ciò solo per le consultazioni della primavera del 2004 conformemente a quanto già provveduto con il provvedimento del 7 febbraio 2001 (in Gazzetta Ufficiale n. 36 del 13 febbraio 2001, p. 65).

Questa misura evita anche che in un breve arco di tempo un alto numero di interessati riceva un elevato numero di informative analoghe da parte di più soggetti impegnati nella campagna elettorale e che utilizzano le medesime fonti conoscitive, in particolare le liste elettorali comunali.

La disciplina applicabile (art. 13, commi 4 e 5, lett. c), d.lg. n. 196/2003) affida al Garante il compito di verificare se l'informativa comporti un impiego di mezzi sproporzionato rispetto al diritto tutelato, considerata la possibilità di prescrivere altre misure appropriate. La manifesta sproporzione può ravvisarsi caso per caso o in relazione a settori generali o tipi di trattamento.

Nel caso dell'attività di propaganda elettorale oggetto del presente provvedimento, l'integrale adempimento agli obblighi di informativa agli interessati può essere considerato sproporzionato rispetto al diritto tutelato, quando la persona cui si riferiscono i dati estratti da fonti pubbliche accessibili a chiunque non è contattata da chi utilizza i dati, oppure riceve materiale di propaganda che non permette un agevole inserimento dell'informativa.

Nel caso in cui, invece, l'interessato è contattato mediante l'invio di lettere, oppure di messaggi per posta elettronica, l'informativa – secondo la predetta formula – può essere inserita nella lettera o nel messaggio, anziché essere inviata all'atto della registrazione "interna" dei dati.

Resta fermo l'obbligo di informativa nel caso in cui i dati siano acquisiti direttamente presso l'interessato, anziché da fonti pubbliche conoscibili da chiunque.

8. MISURE DI SICUREZZA ED ALTRI ADEMPIMENTI

Ciascun partito, movimento o comitato elettorale, nonostante non debba notificare al Garante il trattamento dei dati (cfr. artt. 37 e 38 d.lg. n. 196/2003), è tenuto, oltre che agli adempimenti di cui agli artt. 29 e 30 del Codice in ordine all'individuazione e alla designazione degli incaricati del trattamento e degli eventuali responsabili, ad adottare idonee misure di sicurezza per i trattamenti di dati cartacei e automatizzati e, comunque, quelle "minime" (artt. 31, 33, 34, 35 e allegato B) d.lg. n. 196/2003).

Restano ferme le specifiche prescrizioni che limitano la propaganda elettorale per talune consultazioni dopo la chiusura della campagna elettorale (v., ad esempio, art. 2 l. n. 515/1993).

9. GARANZIE PER GLI INTERESSATI

La possibilità che l'interessato non debba acconsentire all'uso dei dati per finalità di propaganda elettorale, o possa non ricevere alle condizioni sopra indicate un'apposita informativa, non lo priva delle garanzie previste dal Codice come quella di chiedere al titolare del trattamento se vi sono dati che lo riguardano, di conoscerne il contenuto in modo intelligibile, l'origine, ecc.

L'interessato può opporsi in ogni momento al trattamento dei dati e, in particolare, alla propaganda, anche quando abbia manifestato un consenso.

Tali richieste obbligano i titolari del trattamento a darvi riscontro e, in caso di opposizione, a non recapitare più all'opponente ulteriori messaggi anche in occasione di successive campagne.

Qualora il titolare di trattamento non fornisca un riscontro idoneo ad una richiesta di esercizio dei diritti di cui al predetto art. 7, l'interessato può rivolgersi all'autorità giudiziaria o presentare un reclamo o un ricorso al Garante con le modalità previste dagli artt. 142 s. del d.lg. n. 196/2003.

10. USO DEI DATI DECORSO IL PERIODO DI ESONERO

Decorsa la data del 30 giugno 2004, partiti, movimenti politici, comitati promotori, sostenitori e candidati potranno continuare a trattare (anche mediante mera conservazione) i dati estratti da fonti pubbliche accessibili a chiunque per finalità di propaganda elettorale o di connessa comunicazione politica, solo se informeranno gli interessati entro il 30 settembre 2004 nei modi previsti dall'art. 13 del Codice. Diversamente, i dati dovranno essere cancellati o distrutti non oltre la medesima data. Tali considerazioni non riguardano dati per i quali gli interessati siano stati invece informati nei termini sopra indicati.

TUTTO CIÒ PREMESSO IL GARANTE:

a) segnalaai titolari di trattamento interessati, ai sensi dell'art. 154, comma 1, lett. c), del d.lg. n. 196/2003, la necessità di conformare il trattamento ai principi richiamati nel presente provvedimento;
b) ai sensi dell'art. 13, comma 5, del d.lg. n. 196/2003, dispone che partiti e movimenti politici, comitati promotori, sostenitori e candidati i quali trattino dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per esclusive finalità di propaganda elettorale e di connessa comunicazione politica in occasione delle consultazioni elettorali del primo semestre del 2004, possano astenersi dall'informare gli interessati alle condizioni indicate in motivazione;
c) dispone che il presente provvedimento sia pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 12 febbraio 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello
Paissan

IL SEGRETARIO GENERALE
Buttarelli

39 Casi da sottrarre all'obbligo di notificazione al Garante (*)

Registro delle Deliberazioni
n. 1 del 31 marzo 2004

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTO l'art. 37, commi 1 e 2, del d.lg. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

RILEVATO che tale Codice indica i trattamenti di dati da notificare al Garante e demanda a questa Autorità il compito di individuare, tra essi, quelli sottratti all'obbligo di notificazione purché non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle modalità di trattamento o della natura dei dati (art. 37, comma 1);

RILEVATO che il medesimo Codice demanda altresì al Garante il compito di individuare ulteriori trattamenti in aggiunta a quelli elencati nella predetta disposizione;

VISTA la documentazione in atti;

RILEVATO in sede di prima applicazione del Codice che taluni trattamenti sono effettuati con modalità che permettono, allo stato, di sottrarli all'obbligo di notificazione, ferma restando l'osservanza degli ulteriori principi ed obblighi previsti dal Codice in materia di protezione dei dati personali;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Stefano Rodotà;

DELIBERA:

A) di sottrarre all'obbligo di notificazione al Garante, tra i casi previsti dall'art. 37, comma 1, del d.lg. 30 giugno 2003, n. 196:

1) con riferimento ai casi di cui al comma 1, lett. a) di tale disposizione:

a) i trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica. Ciò limitatamente ai dati e alle operazioni, compresa la comunicazione, indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;

b) i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla legge n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria. Ciò sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

c) i trattamenti di dati che indicano la posizione geografica di mezzi di tra-

(*) *G.U.* 6 aprile 2004, n. 81.

sporto aereo, navale e terrestre, effettuati esclusivamente a fini di sicurezza del trasporto;

2) con riferimento ai casi di cui al comma 1, lett. b) della medesima disposizione, i trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti:
   a) a fini di procreazione assistita, di trapianto di organi e tessuti, indagine epidemiologica, rilevazione di malattie mentali, infettive, diffusive o di sieropositività. Ciò sempre che i trattamenti siano effettuati non sistematicamente, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica e limitatamente ai dati e alle operazioni indispensabili per la tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;
   b) ad esclusivi fini di monitoraggio della spesa sanitaria o di adempimento di obblighi normativi in materia di igiene e sicurezza del lavoro e della popolazione;
3) con riferimento ai casi di cui al comma 1, lett. c), i trattamenti di dati idonei a rivelare la sfera psichica di lavoratori:
   a) effettuati da associazioni, enti od organismi a carattere sindacale per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di rapporto di lavoro o di previdenza, anche in tema di diritto al lavoro dei disabili;
   b) effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico o religioso riguardo a dati di propri dipendenti o collaboratori, per adempiere esclusivamente a specifici obblighi previsti dalla normativa in materia di rapporto di lavoro o di previdenza;
4) con riferimento ai casi di cui al comma 1, lett. d), i trattamenti di dati personali:
   a) che non siano fondati unicamente su un trattamento automatizzato volto a definire profili professionali, effettuati per esclusive finalità di occupazione o di gestione del rapporto di lavoro, fuori dei casi di cui alla lettera e) del medesimo art. 37, comma 1;
   b) che non siano fondati unicamente su un trattamento automatizzato volto a definire il profilo di un investitore, effettuati esclusivamente per adempiere a specifici obblighi previsti dalla normativa in materia di intermediazione finanziaria;
   c) relativi all'utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet;
5) con riferimento ai casi di cui al comma 1, lett. e), i trattamenti di dati sensibili effettuati:
   a) al solo fine di selezione di personale per conto esclusivamente di soggetti appartenenti al medesimo gruppo bancario o societario;
   b) da soggetti pubblici per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di occupazione e mercato del lavoro;
   c) da associazioni o organizzazioni di categoria al solo fine di svolgere ricerche campionarie relativamente a dati riguardanti l'adesione alla medesima associazione o organizzazione;
6) con riferimento ai casi di cui al comma 1, lett. f), i trattamenti di dati personali:
   a) effettuati da soggetti pubblici per la tenuta di pubblici registri o elenchi conoscibili da chiunque;
   b) registrati in banche di dati utilizzate in rapporti con l'interessato di fornitura di beni, prestazioni o servizi, o per adempimenti contabili o fiscali, anche in caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato;
   c) registrati in banche di dati utilizzate da soggetti pubblici o privati per adempiere esclusivamente ad obblighi normativi in materia di rapporto di

lavoro, previdenza o assistenza;

d) registrati in banche di dati utilizzate da soggetti pubblici al solo fine della tenuta ed esecuzione di atti, provvedimenti e documenti, in tema di riscossione di tributi, applicazione di sanzioni amministrative, o rilascio di licenze, concessioni o autorizzazioni;

e) relativi a immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio;

f) trattati, in base alla legge, dai soggetti autorizzati in relazione alle operazioni e ai dati necessari all'esclusivo fine di prestare l'attività di garanzia collettiva dei fidi e i servizi a essa connessi o strumentali ("confidi");

B) di inviare copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 marzo 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

40 Sistemi di informazioni creditizie e bilanciamento di interessi (*)

Registro delle Deliberazioni
n. 9 del 16 novembre 2004

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTO il provvedimento adottato in data odierna da questa Autorità con il quale il Garante ha verificato la conformità alle leggi e ai regolamenti ed ha disposto la pubblicazione sulla Gazzetta ufficiale del codice di deontologia e di buona condotta sottoscritto in tema di sistemi informativi di cui sono titolari soggetti privati, utilizzati per la concessione di credito al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti (art. 20, comma 2, lett. e), d.lg. n. 467/2001; art. 117 del Codice in materia di protezione dei dati personali);

VISTI i precedenti provvedimenti adottati al riguardo dal Garante il 10 aprile 2002 (in Gazzetta ufficiale 8 maggio 2002, n. 106) e il 31 luglio 2002 (in Bollettino del Garante n. 30/2002, p. 47) e ritenuta la necessità che questa Autorità, anche in relazione agli elementi acquisiti durante i lavori propedeutici alla sottoscrizione del predetto codice di deontologia e di buona condotta, indichi in materia modalità di attuazione idonee ed efficaci delle disposizioni del Codice sui presupposti di liceità del trattamento;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Gaetano Rasi;

PREMESSO:

1. Sistemi di informazioni creditizie

I sistemi informativi gestiti da soggetti privati ai fini della concessione di crediti al consumo o della valutazione dell'affidabilità dei richiedenti e della puntualità nei pagamenti non sono attualmente oggetto di specifica normativa, a differenza di quanto avviene per:

- servizi o sistemi centralizzati di rilevazione dei rischi creditizi, prevalentemente di rilevante importo, istituiti in base al testo unico delle leggi in materia bancaria e creditizia con deliberazioni del Cicr, regolati da istruzioni della Banca d'Italia e sottoposti alla relativa vigilanza;
- altri registri, banche di dati e archivi pubblici conoscibili da chiunque, utilizzati anche ai fini della concessione di crediti e disciplinati con specifiche normative (es.: registro informatico dei protesti, conservatorie dei registri immobiliari, ecc.).

In Italia, i sistemi informativi gestiti da privati si sono sviluppati prima dell'introduzione della normativa sulla protezione dei dati personali, in assenza di regole e di criteri comuni ed in forme diverse. Ciò, è avvenuto nell'ambito di associazioni o consorzi di operatori finanziari o di attività o servizi a pagamento svolti su iniziativa di società specializzate, in genere sulla base di accordi o contratti tra i gestori dei sistemi e i privati che vi partecipano.

Tali sistemi sono utilizzati da operatori del settore creditizio e finanziario -banche ed

(*) *G.U.* 23 dicembre 2004, n. 300.

intermediari finanziari come, ad esempio, le società finanziarie e di *leasing* finanziario- per condividere e scambiare informazioni su finanziamenti anche di contenuto importo e su pagamenti ratei. I fini perseguiti sono quelli di tutela del credito e di contenimento dei relativi rischi, in relazione anche alla necessità di accrescere la stabilità del sistema bancario e finanziario e all'esigenza rappresentata nel settore volta a sviluppare le attività produttive attraverso il sostegno della domanda di beni di consumo e di servizi (con particolare riferimento a contesti come quello del credito al consumo, presi in considerazione solo indirettamente o parzialmente nell'ambito delle "centrali rischi" di natura pubblica disciplinate, come detto, a livello normativo).

I sistemi privati in esame, già correntemente denominati come "centrali rischi" private, sono stati ora disciplinati dal previsto codice di deontologia e di buona condotta che li ha anche definiti come "sistemi di informazioni creditizie".

2. Consenso ed altri presupposti di liceità del trattamento

Con riferimento al trattamento dei dati personali, inclusi quelli relativi allo svolgimento "positivo" dei rapporti di credito, i soggetti privati che gestiscono i predetti sistemi informativi devono acquisire, per l'eventuale tramite degli organismi partecipanti, il consenso libero ed informato degli interessati, espresso specificamente in rapporto ai vari trattamenti, in conformità a quanto stabilito dal Codice (art. 23) e dal predetto codice di deontologia e buona condotta.

Nel quadro di un elevato livello di garanzie per gli interessati (art. 2 del Codice), va garantito agli stessi il diritto di decidere consapevolmente se i propri dati possano essere registrati nei predetti sistemi informativi (allo scopo, ad esempio, di rendere più agevole il rilascio di futuri finanziamenti), senza condizionamenti anche di fatto o timori che tale determinazione si ripercuota negativamente sui propri rapporti, attuali o futuri, con gli operatori finanziari.

In alternativa al consenso, il titolare del trattamento di dati effettuato ai fini della concessione di credito al consumo, della valutazione dell'affidabilità dei richiedenti e della puntualità nei pagamenti, può già ora avvalersi, in alcuni casi, di altri presupposti di liceità previsti dal Codice. Ciò, quando il medesimo trattamento:

a) è necessario per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato (ad esempio, per istruire una richiesta di finanziamento rivolta alla banca o alla società finanziaria: art. 24, comma 1, lett. b), del Codice);
b) riguarda dati relativi allo svolgimento di attività economiche da parte di società, imprenditori individuali e liberi professionisti, rispettando i limiti richiamati dal Codice (art. 24, comma 1, lett. d);
c) è necessario per finalità di difesa giudiziaria e per il tempo a ciò strettamente necessario, nonché in relazione a richieste degli interessati o di competenti autorità pubbliche, nei casi previsti dalla legge (art. 24, comma 1, lettere a) e f);
d) riguarda dati anonimi trattati per finalità statistiche, per i quali il Codice non è applicabile.

Tali presupposti sono utilizzabili dagli operatori entro i predetti ambiti limitati. Risulta quindi necessario verificare se, in vista della prossima applicazione del codice di deontologia e di buona condotta, il trattamento di determinati dati personali relativi a ritardati o mancati pagamenti effettuati nell'ambito dei predetti sistemi informativi privati possa essere basato su un ulteriore presupposto di liceità, utilizzabile anch'esso dagli operatori in alternativa al consenso libero, espresso e documentato degli interessati (art. 23 del Codice).

Un'idonea alternativa al consenso va ravvisata nell'istituto del bilanciamento di interessi, che il Codice ha confermato nel nostro ordinamento apportandovi un'opportuna integrazione sulla base dell'esperienza (art. 24, comma 1, lett. *g*).

Il presente provvedimento intende dare attuazione a tale istituto, individuando, sulla base dei principi stabiliti dall'art. 11 del Codice, i casi in cui il trattamento di alcuni dati personali relativi ai predetti rapporti di credito potrà avvenire, nell'ambito dei già menzio-

nati sistemi informativi, anche senza il consenso degli interessati, al solo fine di perseguire i legittimi interessi del titolare o dei terzi destinatari dei dati e con le modalità stabilite dal presente provvedimento e dal predetto codice di deontologia e di buona condotta.

3. Diritti delle persone e legittimi interessi del settore creditizio e finanziario

Nel procedere a tale attuazione, va rilevato che i complessi trattamenti di dati personali effettuati negli ambiti sopra descritti presentano alcuni rischi per i diritti e le libertà fondamentali degli interessati, potendo spiegare effetti negativi per la vita privata, per il legittimo accesso all'acquisto di beni e alla fruizione di servizi, nonché, più in generale, per la dignità e la reputazione, per le loro relazioni sociali o professionali e per l'iniziativa privata.

Considerato il rilevante impatto che i sistemi privati di informazioni creditizie spiega nei rapporti produttivi e commerciali attraverso le valutazioni effettuate per la concessione di crediti al consumo o nella valutazione dell'affidabilità dei richiedenti e della puntualità nei pagamenti, occorre evitare duplicazioni e sovrapposizioni di basi informative e la proliferazione di banche di dati plurisettoriali, centralizzate o interconnesse, con un eccesso di informazioni rivolte a vari scopi, che riguardano un numero elevato di persone e che possono risultare particolarmente invasive a causa dei diversi incroci di dati possibili.

Per altro verso, va constatato che l'acquisizione e lo scambio di informazioni significative relative a ritardati o mancati pagamenti di crediti al consumo, anche attraverso sistemi informativi gestiti da privati, possono risultare rilevanti per la corretta valutazione del merito creditizio e della situazione finanziaria dei richiedenti da parte di banche, società finanziarie e altri intermediari (tenuti ad assicurare una sana e prudente gestione dei finanziamenti) o per contenere eccessivi indebitamenti degli interessati e sovraesposizioni rispetto ai redditi dei debitori, nonché per prevenire artifizi e raggiri.

4. Bilanciamento degli interessi in caso di trattamento di dati relativi ad informazioni di tipo negativo

Una conoscenza più agevole delle informazioni appena indicate può risultare quindi particolarmente utile per le valutazioni che gli operatori del settore effettuano per concedere crediti o finanziamenti. Resta ferma la necessità che i dati siano trattati nei predetti sistemi solo per i periodi specificati nel citato codice di deontologia e di buona condotta, tenendo conto di vari fattori (evoluzione del settore; funzioni dei menzionati sistemi informativi; corrispondenti tempi di conservazione previsti per altre rilevazioni di rischi creditizi disciplinate e sottoposte alla vigilanza della Banca d'Italia; termini attualmente previsti per conservare i dati riferiti a comportamenti debitori, registrati presso diversi archivi pubblici per finalità diverse da quelle proprie del rischio creditizio, termini di cui è prevista a breve l'armonizzazione in attuazione dell'art. 119 del Codice).

In base ai richiamati principi di pertinenza, completezza e non eccedenza dei dati, e tenuto conto del nuovo quadro di regole e garanzie introdotto dal codice di deontologia e buona condotta, il Garante ritiene di poter individuare come necessari per perseguire i legittimi interessi dei titolari del trattamento effettuato nell'ambito dei menzionati sistemi informativi, i trattamenti di dati personali relativi a:

a) ritardi nel pagamento di un credito, dati che possono essere conservati nei predetti sistemi, in caso di ritardi pari a due rate o mesi, per dodici mesi dalla data di registrazione dei dati relativi alla loro regolarizzazione e, in caso di ritardi di entità superiore, per ventiquattro mesi dalla data medesima;
b) rapporti di credito per i quali si sono verificati ritardi o inadempimenti non successivamente regolarizzati, dati che possono essere conservati nei predetti sistemi per non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto oppure, in caso di altre vicende rilevanti in relazione al pagamento, dalla data in cui è risultato necessario il loro ultimo aggiornamento, o comunque dalla data di cessazione del rapporto. In quest'ultimo caso, tenendo conto del requisito della completezza dei dati in rapporto alle finalità perseguite (art. 11, comma 1, lett. d), del Codice), possono essere conservati ulteriormente anche i dati personali relativi ad informazioni creditizie di tipo positivo eventualmente presenti nel

sistema informativo, anche se riferiti ad altri rapporti di credito riguardanti il medesimo interessato.

Nei casi individuati nel presente punto 4, il trattamento dei dati personali appena indicati è pertanto lecito per le finalità menzionate anche in assenza del consenso degli interessati, ai sensi dell'art. 24, comma 1, lett. g), del Codice, con effetto dal 1° gennaio 2005, data in cui il predetto codice di deontologia e buona condotta entrerà in vigore.

La presente decisione riguarda solo i soggetti definiti come "gestore" o "partecipante" nell'art. 1 del predetto codice di deontologia e buona condotta.

PER QUESTI MOTIVI, IL GARANTE:

1) individua nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. g), del Codice, i casi nei quali il trattamento dei dati personali nell'ambito dei sistemi informativi oggetto del codice di deontologia e di buona condotta di cui in motivazione, può essere effettuato dai gestori e dai partecipanti a tali sistemi nei limiti e alle condizioni sopra indicate, al solo fine di perseguire i predetti legittimi interessi e senza richiedere il consenso degli interessati;
2) dispone infine che il presente provvedimento sia pubblicato sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 16 novembre 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

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

Registro delle Deliberazioni
n. 14 del 23 dicembre 2004

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTO l'art. 12, lett. *a*), della direttiva europea n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui l'esercizio del diritto di accesso dell'interessato ai dati personali che lo riguardano e a talune informazioni sul loro trattamento deve essere garantito liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi;

VISTO l'art. 8 della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98;

VISTI gli articoli da 7 a 10 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) in tema di esercizio dei diritti dell'interessato e, in particolare, di esercizio del diritto di accesso;

RILEVATO che il principio introdotto dalla previgente disciplina (art. 13, comma 2, legge n. 675/1996; art. 17, commi 7 e 8, d.P.R. 31 marzo 1998, n. 501) e confermato dal Codice è quello della tendenziale gratuità dell'esercizio del diritto di accesso, trattandosi appunto di un diritto e non di richiesta di prestazione dietro corrispettivo;

VISTO l'art. 10, commi 7 e 8, del Codice in riferimento all'articolo 7, commi 1 e 2, lettere *a*), *b*) e *c*), secondo cui si può eventualmente chiedere all'interessato un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata in ciascun caso specifico, anziché la copertura di tutti gli eventuali costi derivanti dall'esercizio del diritto, solo a seguito di alcune richieste (richiesta di conferma dell'esistenza o meno di dati personali che riguardano l'interessato, oppure dell'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento o della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici);

CONSIDERATO che il predetto contributo spese può essere chiesto quando non risulta confermata l'esistenza di dati che riguardano l'interessato e che il medesimo contributo, oltre a non poter eccedere i costi effettivamente sopportati per la ricerca effettuata nel caso specifico, non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale; rilevato che il Garante può individuare l'importo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente;

RILEVATO che l'esistenza di dati che riguardano l'interessato deve intendersi confermata, agli effetti dell'applicazione del presente provvedimento, anche quando i dati cancellati o non più reperibili risultino, comunque, essere stati trattati in precedenza;

CONSIDERATO che, se risulta confermata l'esistenza di dati, può essere chiesto un contributo spese quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione;

RITENUTA la necessità di determinare in termini generali la predetta misura del contributo spese relativamente ai menzionati casi di esercizio del diritto di accesso ai dati personali o a talune informazioni;

CONSIDERATO ALTRESÌ:

1. Casi considerati di esercizio dei diritti

Il presente provvedimento riguarda le seguenti istanze rivolte a qualunque titolare del trattamento pubblico o privato, in conformità al Codice (artt. 7, commi 1 e 2, lettere *a*), *b*) e *c*), 8 e 9):

- richiesta di ottenere conferma dell'esistenza di dati personali;
- richiesta di ottenere la comunicazione dei dati in forma intelligibile;
- richiesta di ottenere l'indicazione dell'origine dei dati;
- richiesta di conoscere le finalità del trattamento;
- richiesta di conoscere le modalità del trattamento;
- richiesta di conoscere la logica applicata al trattamento effettuato con l'ausilio di strumenti elettronici.

Il contributo spese in esame non si riferisce, quindi, all'esercizio di diritti dell'interessato diversi da quelli sopra specificamente indicati (ad esempio, non è ipotizzabile un contributo in caso di richiesta di rettificazione o di opposizione al trattamento).

Gli importi massimi del contributo spese qui previsti in base al Codice sono determinati tenendo conto della normativa comunitaria e internazionale, della corrispondente misura prevista anteriormente al Codice e della necessità di non rendere oneroso l'esercizio dei diritti dell'interessato.

Il principio generale resta, infatti, quello secondo cui l'esercizio del diritto di accesso ai dati che riguardano l'interessato è gratuito.

2. Casi in cui non risulta confermata l'esistenza di dati

In riferimento ai casi in cui non può ritenersi confermata l'esistenza dei dati, va nuovamente rilevato che il contributo spese non è integralmente compensativo di tutti gli eventuali costi di un riscontro.

Tale contributo, per disposizione di legge, non può in ogni caso eccedere i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

Ciò premesso, l'importo massimo che può essere richiesto è determinato dal Garante nella misura di euro dieci, in termini sostanzialmente corrispondenti all'importo già previsto direttamente dalla normativa previgente (L. 20.000; art. 17, comma 7, d.P.R. n. 501/1998).

Con riferimento al medesimo caso in cui non risulti confermata l'esistenza dei dati, lo stesso contributo è individuato forfettariamente in misura pari a euro 2,50, in relazione al caso in cui i dati siano trattati con strumenti elettronici e la risposta (negativa) sia fornita oralmente.

Il contributo spese di cui al presente punto 2 non può essere chiesto quando i dati, cancellati o comunque non reperibili, risultano essere stati comunque trattati in precedenza.

3. Casi in cui risulta confermata l'esistenza di dati

Negli altri casi in cui, a seguito di una richiesta dell'interessato, risulta invece confermata

41

l'esistenza di dati che lo riguardano, l'esercizio del diritto è gratuito, ma può essere chiesto un contributo spese in presenza di una richiesta di riprodurre uno speciale supporto su cui i dati personali figurano.

L'interessato può infatti richiedere specificamente la riproduzione di uno speciale supporto sul quale sono presenti già i dati personali (art. 10, comma 8).

Tale caso riguarda solo le richieste di comunicare i dati in forma intelligibile e non attiene, inoltre, alle richieste di trasporre i dati su supporti di uso più comune, come ordinari *floppy disk* o *cd-rom*, concernendo solo richieste attinenti a determinati supporti di maggior costo quali audiovisivi, lastre, nastri o altri specifici supporti magnetici.

In riferimento a questi casi, si deve ritenere legittima la richiesta, rivolta all'interessato, di contribuire alla particolare spesa necessaria per comunicare i dati, sempre che l'interessato medesimo abbia chiesto specificamente di ottenere in tale forma la comunicazione dei dati che lo riguardano.

Sulla base di una valutazione ponderata delle principali situazioni verificabili, e della circostanza che si tratta anche in questo caso di un contributo, va ritenuto congruo l'importo di euro 20,00.

Si tratta di un importo massimo in quanto, anche in questo caso, il contributo non può comunque eccedere i costi effettivamente sostenuti e documentabili nel caso specifico;

VISTI gli altri atti d'ufficio;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Giuseppe Santaniello;

TUTTO CIÒ PREMESSO IL GARANTE:

determina gli importi relativi al contributo spese in caso di esercizio dei diritti dell'interessato nei termini di cui in motivazione e prescrive ai titolari del trattamento, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice in materia di protezione dei dati personali di adottare le misure necessarie indicate nel presente provvedimento per rendere il trattamento conforme alle disposizioni vigenti.

Roma, 23 dicembre 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

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

DECISIONE DELLA COMMISSIONE

del 28 aprile 2004

sulla adeguata protezione dei dati personali nell'Isola di Man

[*notificata con il numero C(2004) 1556*]

(Testo rilevante ai fini del SEE)

(2004/411/CE)

(*) G.U.C.E. 30 aprile 2004, L 151/50.

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

Notificata con il numero C(2004) 1914
Testo rilevante ai fini del SEE
2004/535/CE

LA COMMISSIONE DELLE COMUNITÀ EUROPEE

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[1], in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) In virtù della direttiva 95/46/CE gli Stati membri dispongono che la trasmissione di dati personali ad un paese terzo possa aver luogo soltanto se il paese terzo di cui si tratta garantisce un livello di protezione adeguato e se le leggi nazionali di attuazione delle altre disposizioni della direttiva sono rispettate prima della trasmissione.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Sulla base di tale constatazione, dati personali possono essere trasmessi dagli Stati membri senza che sia necessaria alcuna garanzia supplementare.

(3) In virtù della direttiva 95/46/CE il livello di protezione dei dati è valutato con riguardo a tutte le circostanze relative ad una trasmissione o a una categoria di trasmissioni di dati e tenendo conto, in particolare, delle condizioni elencate all'articolo 25, paragrafo 2.

(4) Nell'ambito dei trasporti aerei, la scheda nominativa del passeggero (*Passenger Name Record*, nel prosieguo «PNR») è una scheda comprendente le informazioni relative al viaggio di ciascun passeggero. Essa contiene tutte le informazioni necessarie per consentire il trattamento e il controllo delle prenotazioni da parte delle compagnie aeree della prenotazione e delle compagnie aeree partecipanti. Ai fini della presente decisione i termini «passeggero» e «passeggeri» comprendono i membri dell'equipaggio. Per «compagnia aerea della prenotazione» s'intende la compagnia aerea presso la quale il passeggero ha fatto la sua prenotazione originale, o presso la quale delle prenotazioni addizionali sono state fatte dopo l'inizio del viaggio. Per «compagnie aeree partecipanti» s'intende qualsiasi compagnia aerea alla quale la compagnia aerea della prenotazione ha chiesto un posto per un passeggero su uno o vari voli.

(5) L'ufficio statunitense delle dogane e della protezione delle frontiere (United States

(*) *G.U.C.E.* 6 luglio 2004, L 235/11.
(1) *G.U.C.E.* 23 novembre 1995, L 281/ 31. Direttiva modificata da ultimo dal regolamento (CE) n. 1882/2003 (*G.U.C.E.* 31 ottobre 2003, L 284, p.1).

Bureau of Customs and Border Protection, nel prosieguo «CBP») del ministero della Sicurezza interna (Department of Homeland Security) richiede a ciascuna compagnia aerea che garantisce un servizio internazionale di trasporto di passeggeri con destinazione o in partenza dagli Stati Uniti di fornirgli un accesso elettronico ai dati PNR, nella misura in cui tali dati siano stati raccolti e memorizzati nei sistemi informatici di prenotazione della compagnia aerea.

(6) L'obbligo di trasmissione dei dati personali contenuti nei PNR dei passeggeri aerei al CBP si basa su una legge adottata dagli Stati Uniti nel novembre 2001[1], e su regolamenti di attuazione adottati dal CBP in base a tale legge[2].

(7) La legislazione statunitense in questione riguarda il rafforzamento della sicurezza, nonché le condizioni di ingresso negli Stati Uniti e di uscita dal paese. Si tratta di questioni su cui gli Stati Uniti hanno un potere di decisione nell'ambito della propria sovranità. Del resto tali esigenze non sono incompatibili con gli impegni internazionali che il paese ha contratto. Gli Stati Uniti sono un paese democratico, governato dal principio dello stato di diritto e dotato di una solida tradizione in materia di libertà civili. La legittimità del suo procedimento legislativo e la forza e l'indipendenza del suo apparato giudiziario non sono in discussione. La libertà di stampa costituisce un'ulteriore solida garanzia contro le violazioni delle libertà civili.

(8) La Comunità sostiene pienamente gli Stati Uniti nella loro lotta contro il terrorismo nei limiti imposti dal diritto comunitario. La legislazione comunitaria provvede a trovare l'equilibrio necessario tra le esigenze della sicurezza e il rispetto della vita privata. Ad esempio, l'articolo 13 della direttiva 95/46/CE consente agli Stati membri di adottare le misure legislative intese a limitare la portata degli obblighi e dei diritti previsti da tale direttiva, qualora tale restrizione sia giustificata dalla necessità di salvaguardare la sicurezza dello Stato, la difesa, la pubblica sicurezza, nonché la prevenzione, le indagini, l'accertamento e la punizione di reati.

(9) Le trasmissioni di dati riguardano dei responsabili specifici del trattamento, vale a dire le compagnie aeree che garantiscono i collegamenti tra la Comunità e gli Stati Uniti, e un solo destinatario negli Stati Uniti, vale a dire il CBP.

(10) Qualunque accordo volto a stabilire una disciplina normativa per le trasmissioni di PNR agli Stati Uniti, in particolare attraverso la presente decisione, deve essere limitato nel tempo. È stato concordato un periodo di tre anni e mezzo. Nel corso di tale lasso di tempo, il contesto può cambiare in modo radicale e la Comunità e gli Stati Uniti convengono che è necessaria una futura revisione degli accordi.

(11) Il trattamento da parte del CBP dei dati personali contenuti nei PNR dei passeggeri aerei che gli sono inviati è disciplinato dalle disposizioni che figurano nella «Dichiarazione d'impegno del ministero della Sicurezza interna (Department for Homeland Security) — Ufficio delle dogane e della protezione delle frontiere (CBP) dell'11 maggio 2004» (nel prosieguo «la dichiarazione d'impegno») e dalla legislazione americana, alle condizioni previste dalla dichiarazione d'impegno.

(12) Per quanto riguarda la legislazione americana, la legge sulla libertà d'informazione (Freedom of Information Act) è rilevante nel contesto attuale nella misura in cui disciplina le condizioni alle quali il CBP può opporsi alle domande di trasmissioni di dati e trattare in tale modo i dati dei PNR in modo confidenziale. Detta legge disciplina inoltre la trasmissione dei PNR alle persone interessate, elemento che è strettamente collegato al diritto di accesso di cui esse dispongono. La legge sulla libertà d'informazione si applica senza distinzione ai cittadini americani e stranieri.

(13) Per quanto riguarda la dichiarazione d'impegno, e conformemente a quanto previsto al paragrafo 44, le disposizioni della dichiarazione sono state o saranno recepite da leggi, direttive o altri atti normativi negli Stati Uniti e hanno, pertanto, diversi gradi di efficacia giuridica. La dichiarazione d'impegno è pubblicata integralmente nel registro federale sotto la responsabilità del ministero della Sicurezza interna. Essa rappresenta indubbiamente un

(1) Titolo 49, United States Code, sezione 44909, lettera c), paragrafo 3.
(2) Titolo 19, Code of Federal Regulations, sezione 122.49, lettera b).

impegno politico serio e maturo da parte del ministero della Sicurezza interna e il suo rispetto è controllato congiuntamente dagli Stati Uniti e dalla Comunità. L'inadempimento può essere eventualmente fatto valere attraverso mezzi giuridici, amministrativi e politici e, se persistente, comporta la sospensione degli effetti della presente decisione.

(14) I criteri in virtù dei quali il CBP tratta i dati PNR dei passeggeri sulla base della legislazione americana e della dichiarazione d'impegno comprendono i principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche.

(15) Per quanto riguarda la limitazione delle trasmissioni di dati ad una finalità specifica, i dati personali dei passeggeri aerei contenuti nei PNR che sono trasmessi al CBP sono trattati per uno scopo specifico e sono utilizzati o comunicati ulteriormente soltanto nella misura in cui ciò non sia incompatibile con la finalità della trasmissione. In particolare, i dati dei PNR devono essere utilizzati al solo scopo di prevenire e di combattere il terrorismo e i reati collegati al terrorismo, altri reati gravi, compresa la criminalità organizzata transnazionale, la fuga in caso di mandato d'arresto emesso o di pena detentiva comminata per quei reati.

(16) Per quanto riguarda la qualità dei dati e il principio di proporzionalità, che devono essere considerati in rapporto agli importanti motivi d'interesse pubblico che giustificano la trasmissione dei dati dei PNR, i dati dei PNR non devono essere ulteriormente modificati dal CBP. Un massimo di trentaquattro categorie di dati PNR sono trasmesse e le autorità americane sono tenute a consultare la Commissione prima di aggiungere nuovi elementi. Ulteriori informazioni personali ricercate sulla base di quanto è stato direttamente ricavato dai dati PNR sono ottenute da fonti diverse da quelle governative soltanto mediante ricorso a mezzi legittimi. In linea generale, i PNR sono cancellati dopo un periodo massimo di tre anni e sei mesi, ad eccezione dei dati consultati nell'ambito di inchieste specifiche ovvero manualmente.

(17) Per quanto riguarda il principio di trasparenza, il CBP fornisce informazioni ai viaggiatori in merito alla finalità della trasmissione e del trattamento, nonché all'identità del responsabile del trattamento nel paese terzo, ed altre informazioni.

(18) Per quanto riguarda il principio di sicurezza, il CBP adotta le misure di sicurezza tecniche e organizzative adeguate al rischio presentato dal trattamento.

(19) Il diritto di accesso e di rettifica sono riconosciuti, in quanto le persone interessate possono chiedere una copia dei loro dati PNR, nonché una rettifica dei dati inesatti. Le eccezioni previste sono in linea di massima paragonabili alle restrizioni che possono essere imposte da uno Stato membro in forza dell'articolo 13 della direttiva 95/46/CE.

(20) Le trasmissioni successive di dati vengono effettuate, caso per caso, ad altre autorità governative, anche di altri paesi, incaricate della lotta contro il terrorismo o dell'applicazione della legge, per finalità corrispondenti a quelle stabilite nella dichiarazione di limitazione ad una finalità specifica. Le trasmissioni possono anche essere effettuate ai fini della protezione degli interessi vitali della persona interessata o di altre persone, in particolare nei casi di importanti rischi sanitari o nell'ambito di un procedimento penale o negli altri casi previsti dalla legge. Le autorità che ricevono i dati devono, in virtù delle condizioni esplicite di diffusione, impiegare i dati unicamente ai fini previsti e non possono procedere ad una trasmissione successiva senza l'accordo delle CBP. Nessun'altra autorità straniera, federale, statale o locale dispone di un accesso elettronico diretto ai dati del PNR attraverso le basi di dati del CBP. Il CBP si oppone alla divulgazione pubblica dei PNR sulla base delle deroghe previste dalle relative disposizioni della legge sulla libertà di informazione.

(21) Il CBP non utilizza i dati sensibili di cui all'articolo 8 della direttiva 95/46/CE e, in attesa della creazione di un sistema di selezione che consenta di escludere tali dati dai PNR trasferiti, si impegna ad introdurre gli strumenti per la loro cancellazione e nel frattempo a non utilizzarli.

(22) Per quanto riguarda i meccanismi di attuazione volti a garantire il rispetto di questi principi da parte del CBP, è previsto un sistema di formazione e d'informazione del per-

sonale del CBP, nonché di sanzioni per i membri del personale. Il rispetto da parte del CBP della vita privata in generale sarà controllato dal responsabile della Protezione della vita privata (Chief Privacy Officer) presso il ministero della Sicurezza interna, il quale, pur essendo un funzionario di tale ministero, dispone di un'ampia autonomia organizzativa e deve rendere conto ogni anno al Congresso. Le persone i cui dati PNR sono stati trasmessi possono inviare i loro reclami al CBP o, in caso di mancata risoluzione, al responsabile della Protezione della vita privata, direttamente o tramite le autorità incaricate della protezione dei dati negli Stati membri. L'ufficio responsabile della Protezione della vita privata del ministero della Sicurezza interna esamina con procedura d'urgenza i reclami che gli sono trasmessi dalle autorità incaricate della protezione dei dati negli Stati membri a nome dei residenti della Comunità, se questi ultimi ritengono che i loro reclami non siano stati trattati in modo soddisfacente dal CBP o dall'ufficio responsabile della protezione della vita privata del ministero della Sicurezza interna. Il rispetto della dichiarazione d'impegno è oggetto di un esame annuale congiunto, effettuato dal CBP in collaborazione con il ministero della Sicurezza interna e da un gruppo diretto dalla Commissione.

(23) Al fine di contribuire alla trasparenza e di assicurare la capacità delle autorità competenti negli Stati membri di garantire la protezione degli individui per quanto riguarda il trattamento dei loro dati personali, è opportuno precisare le circostanze eccezionali nelle quali la sospensione di specifici flussi di dati possa essere giustificata, indipendentemente dalla constatazione del livello di protezione adeguato.

(24) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, ha espresso numerosi pareri sul livello di protezione garantito dalle autorità americane per quanto riguarda i dati PNR, i quali hanno guidato la Commissione nel corso del negoziato con il ministero della Sicurezza interna. La Commissione ha preso atto di questi pareri nell'elaborazione di questa decisione[1].

(25) Le misure di cui alla presente decisone sono conformi al parere del comitato istituito dall'articolo 31, paragrafo 1, della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, l'Ufficio statunitense delle dogane e della protezione delle frontiere (CBP) è considerato in grado di garantire un livello di protezione adeguato dei dati delle schede nominative dei passeggeri (PNR) trasmessi dalla Comunità per quanto riguarda i voli con destinazione o partenza dagli Stati Uniti, conformemente alla dichiarazione d'impegno che figura nell'allegato.

Articolo 2

La presente decisione riguarda il livello di protezione adeguato garantito dal CBP al fine di rispondere ai requisiti posti dall'articolo 25, paragrafo 1, della direttiva 95/46/CE e non incide sulle condizioni o restrizioni imposte in attuazione di altre disposizioni della direttiva e che si applicano al trattamento di dati personali negli Stati membri.

Articolo 3

1. Fatti salvi i poteri che consentono loro di adottare misure volte a garantire il rispetto delle disposizioni nazionali adottate conformemente alle disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono esercitare i poteri di cui dispongono attualmente per sospendere la trasmissione di dati al CBP al fine di proteggere le persone fisiche per quanto riguarda il trattamento dei loro dati personali in uno dei casi seguenti:

a) quando un'autorità degli Stati Uniti competente ha accertato che il CBP non rispetta le norme in materia di protezione;

b) quando è probabile che le norme di protezione stabilite nell'allegato I non siano rispettate; quando vi sono motivi ragionevoli di credere che il CBP non adotta o non adotterà, in tempi opportuni, le misure che s'impongono per regolare il caso in questione; quando il proseguimento della trasmissione di dati comporterebbe un rischio

(1) Parere 6/2002 sulla trasmissione da parte delle compagnie aeree d'informazioni relative ai passeggeri e ai membri dell'equipaggio e di altri dati agli Stati Uniti, adottato dal gruppo di lavoro il 24 ottobre 2002, disponibile su: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf

Parere 4/2003 sul livello di protezione garantito negli Stati Uniti per la trasmissione di dati relativi ai passeggeri, adottato dal gruppo di lavoro il 13 giugno 2003, disponibile su: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf

Parere 2/2004 su «Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)», adottato dal gruppo di lavoro il 29 gennaio 2004, disponibile su: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

imminente di grave pregiudizio per le persone interessate e le autorità competenti dello Stato membro si sono ragionevolmente sforzate, in tali circostanze, di avvertire il CBP e di dargli la possibilità di rispondere.

2. La sospensione della trasmissione cessa dal momento in cui è garantita l'applicazione delle norme di protezione e l'autorità competente interessata negli Stati membri ne è avvertita.

Articolo 4

1. Gli Stati membri informano immediatamente la Commissione in merito alle misure adottate in forza dell'articolo 3.

2. Gli Stati membri e la Commissione si informano reciprocamente in merito a qualsiasi modificazione delle norme di protezione e ai casi nei quali le misure adottate dalle autorità incaricate di assicurare il rispetto da parte del CBP delle norme di protezione stabilite nell'allegato I non siano sufficienti a garantire tale rispetto.

3. Se le informazioni raccolte in virtù dell'articolo 3 e dei paragrafi 1 e 2 del presente articolo dimostrano che principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche non sono più rispettati, o che un qualunque organismo incaricato di assicurare il rispetto da parte del CBP delle norme di protezione stabilite nell'allegato non svolge efficacemente la sua missione, il CBP ne sarà informato e, se necessario, si applica la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di revocare o sospendere la presente decisione.

Articolo 5

L'applicazione della presente decisione è oggetto di un controllo sistematico e le constatazioni relative sono comunicate al comitato istituito dall'articolo 31 della direttiva 95/46/CE, con particolare riguardo ad elementi che possano incidere sulla valutazione di cui all'articolo 1 della presente decisione relativa all'adeguatezza del livello di protezione dei dati personali contenuti nei PNR dei passeggeri aerei trasmessi al CBP in forza dell'articolo 25 della direttiva 95/46/CE.

Articolo 6

Gli Stati membri adottano tutte le misure necessarie per conformarsi alla presente decisione entro quattro mesi a decorrere dalla notificazione della medesima.

Articolo 7

La presente decisione scade tre anni e sei mesi dopo la data della sua notificazione, a meno che la sua vigenza non sia prorogata secondo la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE.

Articolo 8

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 14 maggio 2004.

Per la Commissione
Frederik BOLKESTEIN
Membro della Commissione

ALLEGATO

DICHIARAZIONE D'IMPEGNO DELL'UFFICIO DELLE DOGANE E DELLA PROTEZIONE DELLE FRONTIERE DEL MINISTERO DELLA SICUREZZA INTERNA

A sostegno del progetto della Commissione europea per l'esercizio dei poteri che le sono conferiti dall'articolo 25, paragrafo 6, della direttiva 95/46/CE (in prosieguo la «direttiva») e l'adozione di una decisione che riconosca che l'Ufficio delle dogane e della protezione delle frontiere (Bureau of Customs and Border Protection, CBP) del ministero della Sicurezza interna (Department of Homeland Security) fornisce una protezione adeguata ai fini delle trasmissioni da parte dei vettori aerei dei dati delle schede nominative dei passeggeri (Passenger Name Record, PNR)[1], che possono rientrare nell'ambito d'applicazione della direttiva, il CBP assume i seguenti impegni:

Fondamento giuridico del diritto di ottenere il PNR

1. In virtù della legge [titolo 49, sezione 44909(c)(3), dell'USC - United States Code - Codice degli Stati Uniti] e dei regolamenti di attuazione (provvisori) (titolo 19, sezione 122.49b, del codice dei regolamenti federali), ciascun vettore aereo che assicura il trasporto aereo internazionale di passeggeri da e per gli Stati Uniti deve fornire al CBP un accesso elettronico ai dati del PNR nella misura in cui essi sono raccolti e conservati nei sistemi automatici di prenotazione/controllo delle partenze (nel prosieguo i «sistemi di prenotazione») dei vettori aerei.

Uso dei dati del PNR da parte del CBP

2. Il CBP può ottenere la maggior parte dei dati contenuti nel PNR tramite l'esame del biglietto aereo e di altri documenti di viaggio di un dato passeggero applicando i normali poteri di controllo alle frontiere. La possibilità di ottenere tali dati per via elettronica aumenterà significativamente la capacità del CBP di facilitare i viaggi bona fide e di svolgere con efficacia una valutazione anticipata dei rischi presentati dai passeggeri.

3. I dati del PNR sono utilizzati dal CBP al solo fine di prevenire e combattere: 1) il terrorismo e i crimini connessi; 2) altri reati gravi, compresa la criminalità organizzata transnazionale; e 3) la fuga dall'arresto o da pena detentiva per i suddetti crimini. L'uso dei dati del PNR a tali scopi consente al CBP di concentrare le proprie risorse su casi di elevato rischio, facilitando e salvaguardando i viaggi bona fide.

Requisiti relativi ai dati

4. I dati richiesti dal CBP sono elencati nell'allegato A. (I dati così identificati sono in appresso denominati «PNR» ai fini della presente dichiarazione d'impegno.) Il CBP, pur richiedendo l'accesso a ciascuno dei trentaquattro tipi di dati elencati nell'allegato «A», ritiene che raramente un singolo PNR conterrà l'intera serie dei dati identificati. Nei casi in cui il PNR non contenga l'intera serie dei dati, il CBP non cercherà di accedere direttamente ad altri dati del PNR non elencati nell'allegato «A» mediante il sistema di prenotazione dei vettori aerei.

5. Per quanto riguarda i dati classificati come «OSI» e «SSI/SSR», normalmente qualificati come note generali e campi aperti, il sistema automatizzato del CBP cercherà tali campi per ciascuno degli altri dati di cui all'allegato «A». Il personale del CBP non è autorizzato ad esaminare manualmente la totalità dei campi OSI e SSI/SSR, a meno che la persona oggetto di un PNR sia stata classificata dal CBP come persona ad alto rischio in relazione ad uno o più degli obiettivi di cui al punto 3.

6. Ulteriori informazioni personali ricercate direttamente dai dati del PNR possono essere ottenute da fonti estranee al governo soltanto mediante mezzi legali, compresi, se del caso, quelli di cooperazione giudiziaria, e soltanto ai fini di cui al punto 3. Ad esempio, se in un PNR figura un numero di carta di credito, le informazioni sulle transazioni legate a quel conto possono essere ricercate mediante mezzi legali quali un ordine di comparizione emesso da un gran giurì o da un giudice, o come altrimenti previsto dalla legge. Inoltre, l'accesso ai dati relativi agli indirizzi di posta elettronica ottenuti da un PNR deve rispettare le leggi degli

(1) Ai fini della presente dichiarazione d'impegno i termini "passeggero" e "passeggeri" comprendono i membri dell'equipaggio.

Stati Uniti sugli ordini di comparizione, i provvedimenti dei giudici, i mandati d'arresto e gli altri procedimenti autorizzati dalla legge, a seconda del tipo delle informazioni ricercate.

7. Il CBP consulta la Commissione in merito alla revisione dei dati del PNR richiesti, di cui all'allegato A, prima di effettuare tale revisione, se si rende conto di ulteriori campi del PNR che le compagnie aeree possano aggiungere ai propri sistemi e che potrebbero aumentare significativamente la capacità del CBP di valutare i rischi presentati dai passeggeri, o se le circostanze indicano che un campo del PNR precedentemente non richiesto sia necessario ai fini di cui al punto 3.

8. Il CBP può trasmettere i PNR in blocco all'Amministrazione per la sicurezza dei trasporti (Transportation Security Administration) affinché quest'ultima controlli il proprio sistema informatizzato di analisi preventiva dei passeggeri CAPPS II (Computer Assisted Passenger Prescreening System II). Tali trasmissioni non saranno effettuate fino a che non sarà stata autorizzato il controllo dei dati del PNR per i voli interni negli Stati Uniti. I dati del PNR trasmessi in virtù della presente disposizione non saranno conservati dall'Amministrazione per la sicurezza dei trasporti né da altre parti direttamente coinvolte nei controlli oltre il periodo necessario per i controlli stessi, e non saranno trasmessi a terzi [1]. L'obiettivo di tale trasmissione è strettamente limitato al controllo del sistema CAPPS II e relative interfaccia e, tranne in situazioni d'emergenza relative all'identificazione di un noto terrorista o individuo legato al terrorismo, non potrà avere conseguenze operative. In virtù del punto 10, che prevede un sistema automatizzato di selezione, il CBP selezionerà e cancellerà i dati «sensibili» prima di trasmettere qualunque PNR in blocco all'Amministrazione per la sicurezza dei trasporti a norma del presente punto.

Trattamento dei dati «sensibili»

9. Il CBP non userà i dati «sensibili» del PNR, vale a dire i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche e le convinzioni religiose o filosofiche, l'appartenenza a sindacati o i dati riguardanti la salute e la vita sessuale delle persone.

10. Il CBP attuerà al più presto un sistema automatizzato che selezioni e cancelli determinati codici e termini PNR «sensibili» individuati dal CBP stesso previa consultazione con la Commissione europea.

11. Fintantoché un sistema automatizzato di selezione non sarà realizzato, il CBP s'impegna a non utilizzare dati del PNR «sensibili» e a cancellare i dati «sensibili» da ogni divulgazione discrezionale di dati PNR a norma dei punti da 28 a 34[2].

Metodo di accesso ai dati del PNR

12. Per quanto riguarda i dati del PNR cui il CBP accede o che riceve direttamente dai sistemi di prenotazione dei vettori aerei per identificare le persone suscettibili di essere sottoposte ad un controllo alla frontiera, il personale del CBP potrà avere accesso o ricevere e usare unicamente i dati del PNR relativi alle persone il cui viaggio comprende un volo diretto o proveniente[3] dagli Stati Uniti.

13. Il CBP estrarrà informazioni sui passeggeri dai sistemi di prenotazione dei vettori aerei fino a quando questi ultimi saranno in grado di attuare un sistema per trasmettere i dati al CBP.

14. Il CBP estrarrà i dati del PNR associati a un volo particolare non prima di 72 ore precedenti la partenza di tale volo, e ricontrollerà i sistemi non più di tre volte tra l'estrazione iniziale, la partenza del volo dall'estero e l'arrivo del volo negli Stati Uniti, oppure tra l'estrazione iniziale e la partenza del volo dagli Stati Uniti, se del caso, per individuare eventuali cambiamenti delle informazioni. Qualora i vettori aerei siano in grado di trasmettere i dati del PNR, il CBP dovrà ricevere i dati 72 ore prima della partenza del volo, purché tutti i cambiamenti dei dati del PNR effettuati tra quel momento e l'ora d'arrivo del volo negli Stati Uniti o la partenza dagli stessi siano a loro volta trasmessi al CBP[4]. Nel raro caso in cui il CBP ottenga in anticipo informazioni, in base alle quali una o più persone particolarmente sospette potrebbero viaggiare in un volo diretto, proveniente o facente scalo negli Stati Uniti, il CBP può ottenere o richiedere di ottenere i dati del PNR prima delle 72 ore

(1) Ai fini di questa disposizione, il CBP non è considerato una parte direttamente coinvolta nei controlli di CAPPS II o una «parte terza».
(2) Fintantochè non sono attuati i sistemi automatizzati di selezione di cui al punto 10, il CBP adotterà, nel rispetto della legislazione degli Stati Uniti, ogni misura necessaria ad evitare la divulgazione di dati «sensibili» del PNR, qualora tali dati figurino in un PNR oggetto di una comunicazione non discrezionale da parte del CBP conformemente al punto 35.
(3) Comprese le persone che transitano attraverso gli Stati Uniti.
(4) Qualora i vettori aerei siano d'accordo a trasmettere i dati del PNR al CBP, quest'ultimo esaminerà coi vettori la possibilità di trasmettere i dati del PNR a intervalli regolari entro 72 ore prima della partenza dall'estero e l'arrivo del volo negli Stati Uniti, o entro 72 ore prima della partenza del volo dagli Stati Uniti, come del caso. Il CBP vuole utilizzare un metodo di trasmissione dei dati necessari del PNR che soddisfi le esigenze di un'efficace valutazione dei rischi, riducendo nel contempo il relativo impatto economico sui vettori aerei.

precedenti la partenza del volo, al fine di garantire un'azione adeguata essenziale per prevenire o combattere uno dei reati di cui al punto 3. Per quanto possibile nei casi in cui debba accedere ai dati del PNR prima delle 72 ore che precedono la partenza del volo, il CBP farà uso dei mezzi ordinari di applicazione delle leggi.

Conservazione dei dati del PNR

15. Previa approvazione dell'Amministrazione degli archivi nazionali (National Archives and Records Administration) (44 U.S.C. 2101, et seq.), il CBP limiterà l'accesso in linea ai dati del PNR agli utenti CBP autorizzati[1] per un periodo di sette giorni, dopodiché il numero dei funzionari autorizzati ad accedere ai dati del PNR sarà ancor più limitato per un periodo di tre anni e sei mesi a decorrere dalla data in cui si verifica l'accesso alle o il ricevimento delle informazioni del sistema di prenotazione del vettore aereo. Dopo tre anni e sei mesi, i dati del PNR cui non si sia avuto un accesso manuale nel periodo previsto saranno distrutti. I dati del PNR per i quali vi è stato un accesso manuale durante il periodo iniziale di tre anni e sei mesi saranno trasferiti dal CBP verso un file di dati cancellati[2], in cui rimarranno per un periodo di otto anni prima di essere distrutti. Tale calendario peraltro non si applicherebbe ai dati del PNR collegati ad un documento specifico contenente misure di applicazione. Tali dati resterebbero accessibili fino all'archiviazione del documento contenente misure di applicazione. Per quanto riguarda i PNR cui il CBP accede o che riceve direttamente dai sistemi di prenotazione dei vettori aerei durante il periodo di validità della presente dichiarazione d'impegno, il CBP rispetterà le regole di conservazione di cui al presente punto, indipendentemente dalla possibile scadenza del periodo di validità della presente dichiarazione a norma del punto 46.

Sicurezza del sistema informatico del CBP

16. Al personale autorizzato del CBP è consentito l'accesso al PNR attraverso il sistema chiuso di intranet del CBP completamente crittato e il cui collegamento è controllato dal Centro dati delle dogane (Customs Data Center). I dati del PNR immagazzinati nella banca dati CBP sono accessibili come file di «sola lettura» da parte del personale autorizzato, il che significa che i dati possono essere sistematicamente riformattati, ma che il loro contenuto non può essere in alcun modo modificato una volta ottenuti dal sistema di prenotazione del vettore aereo.

17. Nessun altro ente straniero, federale, statale o locale dispone di un accesso elettronico diretto ai dati del PNR tramite le banche dati del CBP, compreso il sistema integrato d'informazione doganale (Interagency Border Inspection System - IBIS).

18. I dati relativi all'accesso alle informazioni contenute nelle banche dati del CBP [come, per esempio: chi, dove, quando (data e ora) e ogni revisione dei dati] sono automaticamente registrati e verificati periodicamente dall'Ufficio per gli affari interni (Office of Internal Affairs) per evitare un uso non autorizzato del sistema.

19. Soltanto taluni dirigenti, dipendenti o subappaltatori per le tecnologie dell'informazione[3], sotto il controllo del CBP, che abbiano superato un'indagine relativa al loro passato, abbiano un titolo operativo di accesso protetto da password al sistema informatico del CBP, e siano formalmente incaricati della revisione dei dati del PNR, possono accedere a tali dati.

20. Ai dirigenti, dipendenti e subappaltatori del CBP si richiede di seguire un corso di formazione in materia di sicurezza e riservatezza dei dati, compreso il superamento di un esame ogni due anni. Per controllare e assicurare l'ottemperanza a tutte le norme relative alla protezione della vita privata e della sicurezza dei dati si usa il sistema di audit del CBP.

21. L'accesso senza autorizzazione del personale del CBP ai sistemi di prenotazione dei vettori aerei o al sistema informatico del CBP che raccoglie il PNR è punito con severe sanzioni disciplinari, che possono giungere fino al licenziamento e con la comminazione di pene, quali multe, detenzione fino ad un anno, o entrambe (cfr. titolo 18, sezione 1030, dell'USC).

22. Le direttive ed i regolamenti del CBP prevedono inoltre una severa azione disciplinare, in esito alla quale è previsto anche il licenziamento, nei confronti dei dipendenti del

(1) Tra gli utenti autorizzati del CBP rientrano i dipendenti addetti ai servizi di analisi degli uffici competenti, nonché i dipendenti addetti al National Targeting Center. Come precedentemente esposto le persone incaricate della conservazione, sviluppo e controllo delle banche dati del CBP potranno accedere a tali dati per le finalità indicate.

(2) Benché il documento del PNR non sia tecnicamente cancellato una volta trasferito nel file dei documenti cancellati, esso è archiviato come dato grezzo (non si tratta di una cartella immediatamente consultabile e, perciò, è inutile ai fini delle indagini «tradizionali») ed è a disposizione, per quanto necessario all'espletamento del compito, del solo personale autorizzato dell'Ufficio degli affari interni del CBP (e in alcuni casi dell'Ufficio dell'ispettore generale per le finalità di audit) e del personale incaricato della conservazione della banca dati dell'ufficio per l'informazione tecnologica del CBP.

(3) L'accesso da parte dei «subappaltatori» ai dati del PNR contenuti nel sistema informatizzato del CBP è limitato alle persone che hanno stipulato un contratto di appalto con il CBP per assisterlo nella gestione o nello sviluppo del suo sistema informatizzato.

CBP che rivelino dati contenuti nel sistema informatico del CBP senza autorizzazione (cfr. titolo 19, sezione 103.34, del codice dei regolamenti federali).

23. Le sanzioni penali, comprese le multe, la detenzione fino ad un anno o entrambe, possono essere comminate a tutti i dirigenti e dipendenti negli Stati Uniti per aver rivelato dati del PNR di cui siano giunti a conoscenza per motivi di lavoro, qualora non siano autorizzati a rivelarli dalla legge (cfr. titolo 18, sezioni 641, 1030, 1905, dell'USC).

Trattamento e tutela dei dati del PNR da parte del CBP

24. Il CBP tratta le informazioni del PNR, qualunque sia la nazionalità o il paese di residenza delle persone interessate, come dati sensibili in relazione all'applicazione della legge, come informazioni personali riservate relative al soggetto interessato, e come informazioni commerciali riservate del vettore aereo. Pertanto, esso non può rivelare tali dati al pubblico, salvo quando disposto dalla presente dichiarazione d'impegno o altrimenti previsto dalla legge.

25. La pubblicazione di dati del PNR è in generale disciplinata dalla legge sulla libertà di informazione (Freedom of Information Act) (titolo 5, sezione 552 dell'USC) che consente l'accesso di ogni persona, indipendentemente dalla nazionalità o dal paese di residenza, agli archivi di un ente federale statunitense, tranne quando tali archivi o una parte di essi siano sottratti alla divulgazione in forza di una deroga prevista da tale legge. Rientra tra tali deroghe anche quella che consente ad un ente di non divulgare un'informazione archiviata o una parte di essa quando si tratti di un'informazione commerciale riservata, quando la sua rivelazione rappresenterebbe una violazione chiaramente ingiustificata della vita privata dell'individuo, oppure quando l'informazione sia raccolta ai fini dell'applicazione della legge, nella misura in cui si può ragionevolmente ritenere che tale rivelazione rappresenti una violazione ingiustificata della vita privata dell'individuo [titolo 5, sezioni 552(b)(4), (6), (7)(C) dell'USC].

26. Le norme del CBP (titolo 19, sezione 103.12, del codice dei regolamenti federali), che regolano il trattamento delle richieste di informazioni, come quelle di dati del PNR, in attuazione della legge sulla libertà di informazione, dispongono che, salvo limitate eccezioni nel caso in cui la richiesta provenga dalla persona interessata, le regole in materia di divulgazione previste dalla legge sulla libertà di informazione non siano applicabili agli archivi del CBP per quanto riguarda le informazioni commerciali riservate, le informazioni che riguardano la vita privata dell'individuo quando la divulgazione costituirebbe una violazione manifestamente ingiustificata della vita privata dell'individuo e le informazioni raccolte in vista dell'applicazione della legge, qualora si possa ragionevolmente ritenere che la divulgazione costituisca una violazione ingiustificata della vita privata dell'individuo[1].

27. Nell'ambito di ogni ricorso amministrativo o giudiziario cui dia adito una richiesta, presentata in forza della legge sulla libertà di informazione, di dati del PNR raccolti dai vettori aerei, il CBP sosterrà che tali archivi non sono soggetti alla divulgazione prevista dalla legge sulla libertà di informazione.

Trasmissione dei dati del PNR ad altre amministrazioni pubbliche

28. Ad eccezione delle trasmissioni tra il CBP e l'Amministrazione per la sicurezza dei trasporti, a norma del punto 8, i servizi del ministero della Sicurezza interna saranno trattati come «enti terzi» soggetti alle stesse norme e condizioni di trasmissione dei dati del PNR valide per le altre autorità governative esterne a tale ministero.

29. Il CBP, nell'esercizio del suo potere discrezionale, trasmetterà i dati del PNR ad altre autorità governative, comprese le autorità degli altri paesi incaricate di far rispettare la legge o della lotta contro il terrorismo, previo esame del caso singolo, a fini di prevenzione e lotta contro i reati di cui al punto 3. Le autorità cui il CBP può trasmettere tali informazioni saranno in prosieguo denominate «autorità designate».

30. Il CBP esercita con prudenza il proprio potere discrezionale di trasmettere dati del PNR ai fini di cui al punto 3. Innanzitutto, esso determinerà se il motivo per la divulgazione dei dati a un'altra autorità designata sia conforme alle finalità indicate (cfr. punto 29). In caso affermativo, il CBP determinerà se tale autorità designata abbia il compito di prevenire la violazione di leggi o regolamenti connessi con tali finalità, di condurre indagini o esperire azioni

(1) Il CBP dovrebbe applicare tali deroghe in modo uniforme, indipendentemente dalla nazionalità o dal paese di residenza della persona oggetto dei dati.

giudiziarie a tal riguardo, o di attuare o far rispettare dette leggi o regolamenti, laddove il CBP venga a conoscenza di una violazione, concreta o potenziale, della legge. La fondatezza della divulgazione dovrà essere esaminata alla luce di tutte le circostanze presentate.

31. Per regolare la divulgazione dei dati PNR che possono essere trasmesse ad altre autorità designate, il CBP è considerato il «proprietario» dei dati, e le autorità designate sono soggette, in forza delle specifiche condizioni di trasmissione: 1) all'obbligo di usare i dati PNR soltanto ai fini di cui ai punti 29 o 34; 2) di garantire la cancellazione sistematica delle informazioni del PNR ricevute, in conformità con le procedure di conservazione dei dati applicate dall'autorità designata e 3) di richiedere l'autorizzazione esplicita del CBP per ogni trasmissione successiva dei dati. Il mancato rispetto delle condizioni per la trasmissione può dar luogo ad un'ispezione e ad una relazione del responsabile della Protezione della vita privata (Chief Privacy Officer) presso il ministero della Sicurezza interna a seguito della quale l'autorità designata può essere privata del diritto ad altre trasmissioni di dati del PNR da parte del CBP.

32. La divulgazione di dati del PNR da parte del CBP è soggetta alla condizione che l'ente destinatario tratti i dati in questione come informazioni riservate di carattere commerciale, come dati sensibili in relazione all'applicazione della legge o come dati riservati di carattere personale dei soggetti interessati, a norma dei punti 25 e 26, e come tali da ritenersi sottratti alla divulgazione in virtù della legge sulla libertà di informazione (titolo 5, sezione 552, dell'USC). Inoltre, l'ente destinatario è informato del fatto che ogni divulgazione successiva delle informazioni di cui trattasi è vietata senza previa autorizzazione espressa del CBP. Il CBP non autorizzerà alcuna trasmissione successiva di dati del PNR per finalità diverse da quelle indicate ai punti 29, 34 o 35.

33. I membri del personale di tali autorità designate che, senza autorizzazione, rivelano i dati del PNR sono passibili di sanzioni penali (titolo 18, sezioni 641, 1030, 1905, dell'USC).

34. Nessuna disposizione della presente dichiarazione d'impegno potrà impedire l'uso o la divulgazione dei dati del PNR alle autorità governative competenti qualora tale divulgazione sia essenziale per la tutela degli interessi vitali della persona interessata o di altre persone, in particolare in caso di gravi rischi per la salute. Le divulgazioni effettuate a tal fine sono soggette alle stesse condizioni applicabili alle trasmissioni descritte ai punti 31 e 32.

35. Nessuna disposizione della presente dichiarazione d'impegno può impedire l'uso o la divulgazione di dati del PNR nell'ambito di un procedimento penale o negli altri casi previsti dalla legge. Il CBP informerà la Commissione in ordine all'adozione, da parte delle autorità americane, delle leggi che incidono sulle dichiarazioni contenute nella presente dichiarazione d'impegno.

Informazione, accesso ai dati e mezzi di ricorso per le persone interessate dal PNR

36. Il CBP informerà i passeggeri dei requisiti del PNR e di tutti gli aspetti connessi al suo funzionamento, per esempio tramite la pubblicazione sul sito Internet del CBP, o negli opuscoli e altro materiale destinato ai passeggeri di informazioni di carattere generale relative all'autorità responsabile per la raccolta dei dati, alla finalità di tale raccolta, alla protezione dei dati, alla trasmissione degli stessi, all'identità del funzionario responsabile, ai mezzi di ricorso e agli sportelli cui rivolgersi per eventuali domande o problemi.

37. Le richieste delle persone interessate (note anche come «richiedenti principali»), volte a ottenere copia delle informazioni del PNR che li riguardano contenute nelle banche dati del CBP, sono trattate a norma della legge sulla libertà di informazione. Dette richieste possono essere inviate al seguente indirizzo: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, per posta. La richiesta può anche essere consegnata al Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C. Ulteriori informazioni riguardanti le procedure per presentare richieste a norma della legge sulla libertà di informazione si trovano alla sezione 103.5 del titolo 19 del codice dei regolamenti federali degli Stati Uniti. Al richiedente principale che presenti una tale domanda non potrà essere opposto, come motivo previsto dalla legge sulla libertà di informazione per non comunicare i dati del

PNR, il fatto che il CBP consideri di norma tali dati come informazioni riservate di carattere personale o informazioni commerciali segrete del vettore aereo.

38. In talune circostanze eccezionali il CBP può valersi della facoltà attribuitagli dalla legge sulla libertà di informazione di rifiutare o di rinviare la divulgazione di tutto o più probabilmente parte del fascicolo del PNR a un richiedente principale, a norma del titolo 5, sezione 552(b), dell'USC (ad esempio se si possa ragionevolmente ritenere che la divulgazione in virtù della legge sulla libertà di informazione sia tale da interferire con procedimenti penali o qualora essa sveli le tecniche e le procedure relative ad indagini, con il conseguente pericolo di elusione della legge). In virtù della legge sulla libertà di informazione ogni richiedente ha la possibilità di impugnare, per via amministrativa o giudiziaria, la decisione di rifiuto del CBP di comunicare le informazioni richieste [cfr. il titolo 5, sezione 552, lettera a), punto 4B, dell'USC, nonché il titolo 19, sezioni 103.7-103.9, del codice dei regolamenti federali - CFR].

39. Il CBP si impegna a rettificare[1] i dati su richiesta dei passeggeri o dei membri dell'equipaggio, dei vettori aerei o delle autorità incaricate della protezione dei dati negli Stati membri dell'Unione europea, nei limiti del mandato conferito dalla persona interessata, qualora il CBP accerti che tali dati figurano nella sua banca dati e ritenga che la rettifica sia giustificata e debitamente motivata. Il CBP informerà tutte le autorità designate che hanno ricevuto tali dati del PNR di tutte le rettifiche degli stessi.

40. Le richieste di rettifica dei dati del PNR contenute nella banca dati del CBP e i reclami dei singoli sul trattamento dei loro dati PNR da parte del CBP possono essere presentati, direttamente o tramite l'autorità incaricata della protezione dei dati competente, nei limiti del mandato conferito dalla persona interessata, all'indirizzo seguente: Assistano Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

41. Qualora l'oggetto di un reclamo non possa essere risolto dal CBP, esso può essere presentato per iscritto al Responsabile della protezione della vita privata, Chief Privacy Officer, Department of Homeland Security, Washington, D.C. 20528, che esaminerà il caso e cercherà di risolvere la controversia[2].

42. Inoltre, l'Ufficio responsabile per la protezione della vita privata del ministero della Sicurezza interna tratterà con procedura accelerata i reclami sottopostigli dalle autorità incaricate della protezione dei dati degli Stati membri dell'Unione europea per conto di un residente dell'Unione europea, qualora quest'ultimo abbia autorizzato l'autorità incaricata della protezione dei dati ad agire per suo conto e ritenga che il suo reclamo sulla protezione dei dati riguardante il PNR non sia stato trattato in modo soddisfacente dal CBP, conformemente ai punti da 37 a 41, o dall'Ufficio responsabile della protezione della vita privata del ministero della Sicurezza interna. L'Ufficio per la privacy comunicherà le proprie conclusioni e fornirà un parere alla o alle autorità incaricate della protezione dei dati riguardo alle eventuali azioni intraprese. Nella sua relazione al Congresso, il responsabile della Protezione della vita privata del ministero della Sicurezza interna farà riferimento al numero, al merito e alla soluzione data alle controversie relative al trattamento dei dati personali, quali i dati del PNR[3].

Rispetto delle regole

43. Il CBP, in collaborazione col ministero della Sicurezza interna, s'impegna a svolgere, una volta all'anno o più spesso se così deciso dalle parti, un'analisi congiunta con la Commissione, assistita se del caso da rappresentanti delle autorità europee preposte all'esercizio dell'azione penale e/o delle autorità degli Stati membri dell'Unione europea[4], sull'attuazione della presente dichiarazione d'impegno, al fine di contribuire all'effettivo funzionamento dei procedimenti descritti nella dichiarazione stessa.

44. Il CBP adotta regolamenti, direttive o altri documenti contenenti le presenti disposizioni per assicurare il rispetto della presente dichiarazione d'impegno da parte dei dirigenti, dei dipendenti e dei subappaltatori del CBP. Come indicato, i dirigenti, i dipendenti e i subappaltatori del CBP che non ottemperino alle direttive dell'ente contenute in tali documenti sono passibili di gravi sanzioni disciplinari ed eventualmente penali.

(1) Per quanto riguarda tale possibilità di «rettifica», il CBP vuole precisare di non avere la possibilità di modificare i dati contenuti nei documenti del PNR che raccoglie dai vettori aerei. Si creerà, invece, un fascicolo distinto collegato al documento PNR per indicare i dati errati e le relative correzioni. Più precisamente, il CBP apporterà nel documento di esame secondario (secondary examination record) del passeggero un'annotazione per segnalare che taluni dati del PNR sono (forse) errati.
(2) Il responsabile della Protezione della vita privata del ministero della Sicurezza interna è indipendente da qualunque direzione del ministero, e ha l'obbligo di garantire che le informazioni personali siano utilizzate in modo conforme alla legge (cfr. nota 13). Le decisioni del responsabile della Protezione della vita privata sono vincolanti per il ministero e non possono essere annullate per motivi politici.
(3) Ai sensi della sezione 222 della legge sulla sicurezza interna (Homeland Security Act) del 2002 (Public Law 107-296, del 25 novembre 2002), il responsabile della Protezione della vita privata del ministero della Sicurezza interna ha il compito di procedere a un esame dell'impatto sulla protezione della vita privata delle misure proposte dal ministero per quanto riguarda la riservatezza delle informazioni di carattere personale, compreso il tipo di informazioni raccolte e il numero di persone interessate. Inoltre, egli deve presentare annualmente al Congresso una relazione sulle attività del ministero che incidono sulla protezione della vita privata.
segue nota 3 e 4

Reciprocità

45. Qualora nell'Unione europea sia istituito un sistema di identificazione dei passeggeri aerei in forza del quale i vettori aerei siano tenuti a fornire alle autorità l'accesso ai dati del PNR delle persone, il cui itinerario di viaggio preveda un volo diretto verso o proveniente dall'Unione europea, il CBP solleciterà, in base al principio di reciprocità, la collaborazione delle compagnie aeree con sede negli Stati Uniti.

Revisione e durata di validità della dichiarazione d'impegno

46. La presente dichiarazione d'impegno si applica per un periodo di tre anni e sei mesi a decorrere dalla data di entrata in vigore di un accordo tra gli Stati Uniti e la Comunità europea che autorizzi il trattamento dei dati del PNR da parte dei vettori aerei ai fini del trasferimento di tali dati al CBP, in conformità con la direttiva. Scaduto il termine di due anni e sei mesi dall'entrata in vigore della presente dichiarazione d'impegno, il CBP, in collaborazione col ministero della Sicurezza interna, avvierà una trattativa con la Commissione al fine di estendere la dichiarazione stessa e gli eventuali accordi ad essa connessi a condizioni accettabili da entrambe le parti. Se un accordo accettabile da entrambe le parti non è raggiunto prima della data di scadenza della presente dichiarazione d'impegno, quest'ultima cessa di essere valida.

Non sono creati diritti privati o precedenti

47. La presente dichiarazione d'impegno non crea o conferisce alcun diritto o beneficio a persone fisiche o giuridiche, private o pubbliche.

48. Le disposizioni contenute nella presente dichiarazione d'impegno non costituiscono un precedente per le future trattative con la Commissione, l'Unione europea, gli enti collegati o uno Stato terzo per quanto riguarda il trasferimento di qualunque tipo di dati.

11 maggio 2004

ALLEGATO «A»

Dati del PNR richiesti dal CBP ai vettori aerei

1. Codice del documento PNR
2. Data di prenotazione
3. Data/e prevista/e di viaggio
4. Nome
5. Altri nomi che compaiono nel PNR
6. Indirizzo
7. Informazioni su tutte le modalità di pagamento
8. Indirizzo di fatturazione
9. Recapiti telefonici
10. Itinerario completo per lo specifico PNR
11. Informazioni sui viaggiatori abituali «Frequent flyer» (solo per le miglia percorse e indirizzo/i)
12. Agenzia viaggi
13. Agente di viaggio
14. Informazioni del PNR sul code share (scambio dei codici)
15. Fase di viaggio del passeggero
16. PNR scissi/divisi
17. Indirizzi di posta elettronica
18. Dati sull'emissione del biglietto
19. Osservazioni generali
20. Numero del biglietto
21. Numero del posto
22. Data di emissione del biglietto
23. Precedenti assenze all'imbarco
24. Numero di etichetta dei bagagli
25. Passeggero senza prenotazione

segue nota 3 e 4

La sezione 222, paragrafo 5, della legge inoltre prevede espressamente che il responsabile della Protezione della vita privata del ministero della Sicurezza interna riceva e riferisca al Congresso tutte le «denunce di violazioni della vita privata».

(4) La composizione dei gruppi delle due parti sarà comunicata in anticipo e può comprendere le autorità competenti per la protezione della vita privata/la protezione dei dati, per i controlli doganali e l'applicazione delle norme, per la sicurezza dei confini e/o dell'aviazione. Le autorità partecipanti dovranno ottenere tutte le autorizzazioni di sicurezza necessarie e rispettare la riservatezza delle discussioni e della documentazione cui potranno avere accesso. La riservatezza però non sarà un ostacolo a che entrambe le parti presentino una relazione sui risultati dell'analisi congiunta alle rispettive autorità competenti, compresi il Congresso degli Stati Uniti e il Parlamento europeo. Tuttavia, in nessun caso le autorità partecipanti potranno rivelare i dati personali di una persona, né qualunque informazione non pubblica derivante da documenti cui viene loro consentito di accedere, o informazioni operative o interne agli enti interessati che ottengono durante l'analisi congiunta. Le due parti determinano le modalità dettagliate per l'analisi congiunta.

43

26. Informazioni OSI
27. Informazioni SSI/SSR
28. Informazioni sulla fonte
29. Cronistoria dei cambiamenti fatti al PNR
30. Numero di viaggiatori nel PNR
31. Informazioni relative al posto
32. Biglietti di sola andata
33. Informazioni APIS eventualmente assunta
34. Campi ATFQ

44 Decisione del Consiglio del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (*Passenger Name Record*, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del Dipartimento per la sicurezza interna degli Stati Uniti (*)

(2004/496/CE)

IL CONSIGLIO DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 95 in combinato disposto con l'articolo 300, paragrafo 2, primo comma, prima frase, vista la proposta della Commissione, considerando quanto segue:

(1) Il 23 febbraio 2004 il Consiglio ha autorizzato la Commissione a negoziare, in nome della Comunità, un accordo con gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti.

(2) Il Parlamento europeo non ha espresso il suo parere nel termine fissato dal Consiglio, ai sensi dell'articolo 300, paragrafo 3, primo comma del trattato, dato l'urgente bisogno di porre rimedio alla situazione di incertezza in cui si trovano le compagnie aeree ed i passeggeri, nonché di proteggere gli interessi finanziari degli interessati.

(3) È opportuno approvare il presente accordo,

DECIDE:

Articolo 1

L'accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti è approvato in nome della Comunità.

Il testo dell'accordo è accluso alla presente decisione.

(*) *G.U.C.E.* 20 maggio 2004, L 183/83.

Articolo 2

Il Presidente del Consiglio è autorizzato a designare la (le) persona (persone) abilitata (abilitate) a firmare l'accordo in nome della Comunità europea.

Bruxelles, 17 maggio 2004

Per il Consiglio
Il Presidente
B. COWEN

ACCORDO

tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (passenger name record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti

LA COMUNITÀ EUROPEA E GLI STATI UNITI D'AMERICA

RICONOSCENDO l'importanza di rispettare i diritti e le libertà fondamentali, in particolare il diritto alla vita privata, e l'importanza di rispettare tali valori nella prevenzione e nella lotta contro il terrorismo e i reati ad esso connessi, nonché altri reati gravi di natura transnazionale, tra cui la criminalità organizzata;

VISTI le leggi e i regolamenti statunitensi che impongono a ciascun vettore aereo che assicura il trasporto di passeggeri da e per gli Stati Uniti nello spazio aereo estero di fornire all'ufficio doganale e di protezione dei confini (Bureau of Customs and Border Protection, in seguito denominato «CBP») del dipartimento per la sicurezza interna (Department of Homeland Security, in seguito denominato «DHS»), un accesso elettronico ai dati di identificazione delle pratiche (Passenger Name Record, in seguito denominato «PNR») nella misura in cui questi sono raccolti e conservati nei sistemi automatici di prenotazione/controllo dei vettori aerei;

VISTA la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 7, lettera c);

VISTE le dichiarazioni di impegno del CBP dell'11 maggio 2004, che saranno pubblicate nel registro federale (in seguito denominate «le dichiarazioni di impegno»);

VISTA la decisione C(2004) 1799 della Commissione adottata il 17 maggio 2004, ai sensi dell'articolo 25, paragrafo 6 della direttiva 95/46/CE, con cui si ritiene che il CBP, conformemente alle dichiarazioni di impegno allegate, assicuri un livello di protezione adeguato dei dati PNR trasferiti dalla Comunità europea (in seguito denominata «Comunità») in relazione ai voli da o per gli Stati Uniti (in seguito denominata «la decisione»);

CONSTATANDO che i vettori aerei dotati di sistemi di prenotazione/controllo situati nel territorio degli Stati membri della Comunità europea dovrebbero provvedere a trasmettere i dati PNR al CBP non appena ciò sia tecnicamente possibile, ma che, fino a quel momento, dovrebbe essere consentito alle autorità statunitensi di accedere direttamente a tali dati, ai sensi delle disposizioni del presente accordo;

AFFERMANDO che il presente accordo non costituisce un precedente per eventuali futuri discussioni o negoziati tra gli Stati Uniti e la Comunità europea, o tra una delle due parti e uno Stato terzo, in merito al trasferimento di una qualsiasi altra forma di dati;

VISTO l'impegno di entrambe le parti a collaborare per trovare senza indugio una solu-

zione appropriata e soddisfacente per entrambe in merito al trattamento dei dati relativi alle informazioni preventive sui passeggeri (Advance Passenger Information, API) trasferiti dalla Comunità agli Stati Uniti,

HANNO CONVENUTO QUANTO SEGUE:

1) Il CBP può accedere elettronicamente ai dati PNR provenienti dai sistemi di prenotazione/controllo («sistemi di prenotazione») dei vettori aerei situati nel territorio degli Stati membri della Comunità europea, in assoluta conformità della decisione, per tutto il periodo in cui la decisione è applicabile e solo finché non sia in vigore un sistema soddisfacente che permetta la trasmissione di tali dati da parte dei vettori aerei.

2) Ciascun vettore aereo che assicura il trasporto di passeggeri da o per gli Stati Uniti nello spazio aereo estero tratta i dati PNR contenuti nei suoi sistemi automatizzati di prenotazione come richiesto dal CBP ai sensi della normativa statunitense, in assoluta conformità della decisione e per tutto il periodo in cui la decisione è applicabile.

3) Il CBP prende nota della decisione e attesta che sta attuando le dichiarazioni di impegno allegate a detta decisione.

4) Il CBP tratta i dati PNR ricevuti e i titolari dei dati interessati da tale trattamento in conformità delle leggi e degli obblighi costituzionali statunitensi applicabili, senza discriminazioni illegittime, in particolare in base alla nazionalità e al paese di residenza.

5) Il CBP e la Commissione europea rivedono congiuntamente e su base periodica l'attuazione del presente accordo.

6) Qualora nell'Unione europea sia istituito un sistema di identificazione dei passeggeri aerei in forza del quale i vettori aerei siano tenuti a fornire alle autorità l'accesso ai dati PNR delle persone il cui itinerario di viaggio preveda un volo da o per l'Unione europea, il DHS, per quanto fattibile e unicamente su una base di reciprocità, promuove attivamente la cooperazione dei vettori aerei rientranti nella sua giurisdizione.

7) Il presente accordo entra in vigore all'atto della sua firma. Ciascuna parte può denunciare il presente accordo in qualsiasi momento, mediante notifica per via diplomatica. In tal caso, l'accordo cessa di essere in vigore novanta (90) giorni dopo la data di tale notifica. Il presente accordo può essere modificato in ogni momento mediante consenso scritto di entrambe le parti.

8) Il presente accordo non intende derogare o apportare modifiche alla normativa delle parti; esso non crea né conferisce alcun diritto o beneficio ad altre persone o enti, pubblici o privati.

Firmato, il 17 maggio 2004

Il presente accordo è redatto in duplice originale in lingua ceca, danese, estone, finlandese, francese, greca, inglese, italiana, lettone, lituana, maltese, olandese, polacca, portoghese, slovacca, slovena, spagnola, svedese, tedesca e ungherese, ciascun testo facente ugualmente fede. In caso di divergenze di interpretazione si considera determinante il testo inglese.

Per la Comunità europea

Per gli Stati Uniti d'America
Tom RIDGE
Segretario del Dipartimento
per la sicurezza interna degli Stati Uniti

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

AGREEMENT
BETWEEN THE EUROPEAN COMMUNITY AND
THE UNITED STATES OF AMERICA
ON THE PROCESSING AND TRASFER OF PRN DATA BY AIR CARRIES
TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY,
BEREAU OF CUSTOMS AND BORDER PROTECTION

CE/USA/EN1

(*) Firmato a Washington il 28 maggio 2004.

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

DECISIONE DELLA COMMISSIONE

del 27 dicembre 2004

che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a Paesi Terzi

[*notificata con il numero C(2004) 5271*]

(Testo rilevante ai fini del SEE)

(2004/915/CE)

(*) *G.U.C.E.* 29 dicembre 2004, L 385/74.

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

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20.10.2004
SEC (2004) 1323

COMMISSION STAFF WORKING DOCUMENT

The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce

(*) http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2004-1323_en.pdf

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

Safe Harbour Decision Implementation Study

prepared by

Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet
(Centre de Recherche Informatique et Droit,
University of Namur, Belgium)

with the assistance of

Prof. Dr. Joel R. Reidenberg
(Fordham University School of Law, New York, USA)

and Dr. Lee A. Bygrave
(Norwegian Research Centre for Computers and Law,
University of Oslo, Norway)

at the request of the
European Commission, Internal Market DG
Contract PRS/2003/A0-7002/E/27

Namur, 19 April 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/studies/safe-harbour-2004_en.pdf

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

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 66,

vista l'iniziativa del Regno di Spagna[1],

visto il parere del Parlamento europeo[2],

considerando quanto segue:

(1) Il sistema d'informazione Schengen, in seguito denominato "SIS", istituito a norma del titolo IV della convenzione del 1990 di applicazione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni[3], in seguito denominata "convenzione di Schengen del 1990", rappresenta uno strumento fondamentale per l'applicazione delle disposizioni dell'acquis di Schengen integrate nell'ambito dell'Unione europea.

(2) È stata riconosciuta la necessità di elaborare un nuovo SIS di seconda generazione, in seguito denominato "SIS II", in vista dell'allargamento dell'Unione europea e che consenta l'introduzione di nuove funzioni e si giovi nello stesso tempo degli ultimi sviluppi nel settore delle tecnologie dell'informazione. Sono stati compiuti i primi passi per lo sviluppo di questo nuovo sistema.

(3) Alcuni adattamenti di disposizioni vigenti e l'introduzione di talune nuove funzioni possono già essere realizzati rispetto alla versione attuale del SIS, in particolare per quanto riguarda la concessione dell'accesso ad alcuni tipi di dati inseriti nel SIS alle autorità che sarebbero agevolate nel corretto espletamento dei loro compiti dalla possibilità di consultare tali dati, compresi l'Europol e i membri nazionali dell'Eurojust, l'estensione delle categorie di oggetti smarriti per i quali possono essere inserite segnalazioni e la registrazione delle trasmissioni di dati a carattere personale. È dapprima necessario istituire in ciascuno Stato membro i dispositivi tecnici necessari a tal fine.

(4) Le conclusioni del Consiglio europeo di Laeken del 14 e 15 dicembre 2001 e, in particolare, il punto 17 (cooperazione tra i servizi speciali nella lotta contro il terrorismo) e 43 (Eurojust e cooperazione di polizia per quanto riguarda l'Europol) e il piano d'azione del 21 settembre 2001 contro il terrorismo si riferiscono alla necessità di rafforzare il SIS e migliorarne le capacità.

(5) È inoltre utile adottare disposizioni per quanto riguarda lo scambio di tutte le informazioni supplementari tramite le autorità all'uopo designate in tutti gli Stati membri (Informazioni supplementari richieste all'atto dell'ingresso nel territorio nazionale - SIRENE), fornendo a tali autorità una base giuridica comune nel quadro delle disposizioni della convenzione di Schengen del 1990 e stabilendo norme relative alla cancellazione dei dati da esse detenuti.

(6) Le modifiche da apportare a tal fine alle disposizioni dell'acquis di Schengen concer-

(*) *G.U.C.E.* 30 aprile 2004, L 162/29.
(1) *G.U.C.E.* 4 luglio 2002, C 160/ 5.
(2) G.U.C.E. 5 febbraio 2004, C 31/122.
(3) *G.U.C.E. 22 luglio 2000,* L 239/19.

nenti il SIS constano di due parti: il presente regolamento e una decisione del Consiglio basata sull'articolo 30, paragrafo 1, lettere a) e b), sull'articolo 31, lettere a) e b) e sull'articolo 34, paragrafo 2, lettera c) del trattato sull'Unione europea. Questo perché, come indicato nell'articolo 93 della convenzione di Schengen del 1990, scopo del SIS è quello di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza nazionale, nel territorio degli Stati membri e di applicare le disposizioni della summenzionata convenzione sulla circolazione delle persone in detti territori avvalendosi delle informazioni trasmesse tramite il SIS ai sensi delle disposizioni di detta convenzione. Poiché alcune delle disposizioni della convenzione di Schengen del 1990 devono essere applicate per entrambi gli scopi nello stesso tempo, è opportuno che esse siano modificate negli stessi termini tramite atti paralleli basati su ciascuno dei trattati.

(7) Il presente regolamento lascia impregiudicata la futura adozione della necessaria normativa che descriva nei dettagli l'impalcatura giuridica, gli obiettivi, il funzionamento e l'uso del SIS II, quali, ma non solo, le norme che definiscano ulteriormente le categorie di dati da inserire nel sistema, gli scopi per cui sono inserite e i criteri per l'inserimento, le norme riguardanti il contenuto delle registrazioni SIS, l'interconnessione delle segnalazioni, la compatibilità tra le stesse e ulteriori norme sull'accesso ai dati SIS e sulla protezione di dati a carattere personale e relativo controllo.

(8) Per quanto riguarda l'Islanda e la Norvegia, il presente regolamento costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen che rientrano nel settore di cui all'articolo 1, punto G, della decisione 1999/437/CE[1], relativa a talune modalità di applicazione di detto accordo.

(9) A norma degli articoli 1 e 2 del protocollo sulla posizione della Danimarca allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata e non è soggetta alla sua applicazione. Dato che il presente regolamento si basa sull'acquis di Schengen in applicazione delle disposizioni della parte terza, titolo IV, del trattato che istituisce la Comunità europea, la Danimarca decide, a norma dell'articolo 5 del succitato protocollo, entro un periodo di sei mesi dall'adozione del presente regolamento da parte del Consiglio, se intende recepirlo nel proprio diritto interno.

(10) Il presente regolamento rappresenta uno sviluppo del SIS ai fini della sua applicazione in relazione alle disposizioni dell'acquis di Schengen sulla circolazione delle persone. Il Regno Unito non ha chiesto di partecipare al SIS e non vi partecipa per questi fini, ai sensi della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[2]. Il Regno Unito non partecipa pertanto all'adozione del presente regolamento, non è da esso vincolato e non è soggetto alla sua applicazione.

(11) Il presente regolamento rappresenta uno sviluppo del SIS ai fini della sua applicazione in relazione alle disposizioni dell'acquis di Schengen sulla circolazione delle persone. L'Irlanda non ha chiesto di partecipare al SIS e non vi partecipa per questi fini, ai sensi della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen[3]. L'Irlanda non partecipa pertanto all'adozione del presente regolamento, non è da esso vincolata e non è soggetta alla sua applicazione.

(12) Il presente regolamento costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi dell'articolo 3, paragrafo 2, dell'atto di adesione,

(1) *G.U.C.E.* 10 luglio 1999, L 176/31.
(2) *G.U.C.E.* 1° giugno 2000, L 131/43.
(3) *G.U.C.E.* 7 marzo 2002, L 64/20.

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Le disposizioni della convenzione di Schengen del 1990 sono modificate come segue:

1) all'articolo 92 è aggiunto il paragrafo seguente:

"4. Gli Stati membri si scambiano, conformemente alla legislazione nazionale, tramite le autorità all'uopo designate (SIRENE) tutte le informazioni supplementari necessarie in relazione all'inserimento di segnalazioni e ai fini dell'adeguata azione da intraprendere nei casi in cui persone e oggetti, i cui dati sono stati inseriti nel sistema d'informazione Schengen, siano reperiti grazie alla consultazione di tale sistema. Tali informazioni possono essere usate solo per lo scopo per il quale sono state trasmesse."

2) all'articolo 94, paragrafo 3, primo comma, le lettere da a) a i) sono sostituite dalle seguenti:

"a) cognome e nomi, 'alias' eventualmente registrati separatamente;
b) segni fisici particolari, oggettivi ed inalterabili;
c) (...)
d) data e luogo di nascita;
e) sesso;
f) cittadinanza;
g) indicazione che le persone in questione sono armate, violente o sono evase;
h) motivo della segnalazione;
i) linea di condotta da seguire"

3) alla fine dell'articolo 101, paragrafo 1, è aggiunta la seguente frase:

"Tuttavia, l'accesso ai dati inseriti nel sistema d'informazione Schengen e il diritto di consultarli direttamente possono essere esercitati anche dalle autorità giudiziarie nazionali, tra cui quelle responsabili dell'avvio di investigazioni del pubblico ministero nelle azioni penali e indagini giudiziarie prima dell'atto di accusa, nell'assolvimento dei propri compiti, conformemente alla legislazione nazionale."

4) l'articolo 101, paragrafo 2, è sostituito dal seguente:

"2. Inoltre, l'accesso ai dati inseriti a norma dell'articolo 96 e i dati riguardanti documenti relativi a persone inseriti a norma dell'articolo 100, paragrafo 3, lettere d) e e), ed il diritto di consultarli direttamente possono essere esercitati dalle autorità competenti per il rilascio dei visti, dalle autorità centrali competenti per l'esame delle domande di visti e dalle autorità competenti per il rilascio dei documenti di soggiorno e per l'amministrazione degli stranieri nel quadro dell'applicazione delle disposizioni in materia di circolazione delle persone previste dalla presente convenzione. L'accesso ai dati da parte di tali autorità è disciplinato dal diritto nazionale di ciascuno Stato membro."

5) la seconda frase dell'articolo 102, paragrafo 4, è sostituita dalla seguente:

"In deroga a quanto precede, i dati inseriti a norma dell'articolo 96 e i dati relativi a documenti riguardanti persone inseriti a norma dell'articolo 100, paragrafo 3, lettere d) e e) possono essere utilizzati solo per gli scopi di cui all'articolo 101, paragrafo 2, conformemente alla legislazione nazionale di ciascuno Stato membro."

6) l'articolo 103 è sostituito dal seguente:

"Articolo 103
Ciascuno Stato membro provvede affinché ciascuna trasmissione di dati personali sia registrata nella sezione nazionale del sistema d'informazione Schengen dall'organo di gestione degli archivi di dati, ai fini del controllo dell'ammissibilità della ricerca. La registrazione può essere utilizzata soltanto a questo scopo e deve essere cancellata al più presto dopo un periodo di un anno e al più tardi un periodo di tre anni."

7) è inserito l'articolo seguente:

"Articolo 112 bis

1. I dati di carattere personale archiviati dalle autorità di cui all'articolo 92, paragrafo 4, in seguito allo scambio di informazioni a norma di detto paragrafo sono conservati soltanto per il tempo necessario a conseguire gli scopi per i quali sono stati forniti. Essi sono in ogni caso cancellati al più tardi un anno dopo che sono state cancellate dal sistema d'informazione Schengen le segnalazioni riguardanti la persona interessata o l'oggetto in questione.
2. Il paragrafo 1 non pregiudica il diritto di uno Stato membro di conservare negli archivi nazionali i dati relativi ad una determinata segnalazione effettuata da detto Stato membro o ad una segnalazione in collegamento con la quale è stata svolta un'azione nel suo territorio. Il periodo di tempo per cui tali dati possono essere conservati in tali archivi è regolato dalla legislazione nazionale."

8) è inserito l'articolo seguente:

"Articolo 113 bis

1. I dati diversi dai dati di carattere personale archiviati dalle autorità di cui all'articolo 92, paragrafo 4, in seguito allo scambio di informazioni a norma di detto paragrafo sono conservati soltanto per il tempo necessario a conseguire gli scopi per i quali sono stati forniti. Essi sono in ogni caso cancellati al più tardi un anno dopo che sono state cancellate dal sistema d'informazione Schengen le segnalazioni riguardanti la persona interessata o l'oggetto in questione.
2. Il paragrafo 1 non pregiudica il diritto di uno Stato membro di conservare negli archivi nazionali i dati relativi ad una determinata segnalazione effettuata da detto Stato membro o ad una segnalazione in collegamento con la quale è stata svolta un'azione nel suo territorio. Il periodo di tempo per cui tali dati possono essere conservati in tali archivi è regolato dalla legislazione nazionale."

Articolo 2

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale* dell'Unione europea.

2. Esso si applica a decorrere da una data che sarà fissata dal Consiglio che delibera all'unanimità, non appena adempiute le condizioni preliminari necessarie. Il Consiglio può decidere di fissare date differenti per l'applicazione di disposizioni differenti.

3. La decisione del Consiglio a norma del paragrafo 2 è pubblicata nella Gazzetta ufficiale dell'Unione europea.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Lussemburgo, 29 aprile 2004

Per il Consiglio
Il Presidente
M. McDowell

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

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 66,

vista la proposta della Commissione,

visto il parere del Parlamento europeo,

considerando quanto segue:

(1) Il Consiglio europeo di Siviglia del 21 e 22 giugno 2002 ha giudicato una priorità assoluta l'istituzione di un sistema comune d'identificazione dei dati dei visti e ne ha chiesto l'introduzione, al più presto, sulla scorta di uno studio di fattibilità e sulla base degli orientamenti adottati dal Consiglio il 13 giugno 2002 .

(2) Il 5 - 6 giugno 2003 il Consiglio ha accolto favorevolmente lo studio di fattibilità presentato dalla Commissione nel maggio 2003, ha confermato gli obiettivi stabiliti nei suoi orientamenti per il VIS ed ha invitato la Commissione a proseguire, di concerto con gli Stati membri, i lavori preparatori sullo sviluppo del VIS sulla base di un'architettura centralizzata, tenendo conto della possibilità di una piattaforma tecnica comune con il sistema d'informazione Schengen di seconda generazione (SIS II).

(3) Il Consiglio europeo riunitosi a Salonicco il 19 e 20 giugno 2003 ha ritenuto necessario che, a seguito dello studio di fattibilità, fossero elaborati quanto prima possibile orientamenti riguardanti la pianificazione dello sviluppo del VIS, la base giuridica appropriata che consentirà la sua istituzione e l'impegno delle risorse finanziarie necessarie.

(4) La presente decisione costituisce il fondamento giuridico necessario per l'iscrizione nel bilancio generale dell'Unione europea degli stanziamenti necessari allo sviluppo del VIS e l'esecuzione di tale parte del bilancio, comprese le misure preparatorie necessarie per gli elementi biometrici che devono essere inseriti in una fase successiva ai sensi delle conclusioni del Consiglio del 19 febbraio 2004 .

(5) Le misure per l'attuazione della presente decisione sono adottate secondo la decisione 1999/468/CE del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione[1]. Il comitato che assiste la Commissione dovrebbe, ove necessario, tenere riunioni in due diverse composizioni a seconda dell'ordine del giorno.

(6) Poiché lo scopo della presente decisione, vale a dire lo sviluppo di un VIS comune, non può essere realizzato in misura sufficiente dagli Stati membri e può dunque, a causa delle dimensioni e degli effetti dell'azione in questione, essere realizzato meglio a livello comunitario, la Comunità può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato. La presente decisione si limita a quanto è necessario per conseguire tale scopo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(7) La presente decisione rispetta i diritti fondamentali e osserva i principi riconosciuti, in particolare nella Carta dei diritti fondamentali dell'Unione europea.

(*) *G.U.C.E.* 15 giugno 2004, L 213/5.
(1) *G.U.C.E. 17 luglio 1999,* L 184/23.

(8) A norma degli articoli 1 e 2 del protocollo sulla posizione della Danimarca allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, la Danimarca non partecipa all'adozione della presente decisione, non è da essa vincolata e non è soggetta alla sua applicazione. Dato che la presente decisione si basa sull'acquis di Schengen in applicazione delle disposizioni della parte terza, titolo IV, del trattato che istituisce la Comunità europea, la Danimarca decide, a norma dell'articolo 5 del succitato protocollo, entro un periodo di sei mesi dall'adozione della presente decisione da parte del Consiglio, se intende recepirla nel proprio diritto interno.

(9) Per quanto riguarda l'Islanda e la Norvegia, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen[1], che rientrano nel settore di cui all'articolo 1, lettera B, della decisione 1999/437/CE del Consiglio[2], relativa a talune modalità di applicazione di detto accordo.

(10) È necessario concludere un accordo per permettere a rappresentanti dell'Islanda e della Norvegia di essere associati ai lavori dei comitati che assistono la Commissione nell'esercizio delle sue competenze d'esecuzione. Tale accordo è stato previsto nello scambio di lettere che ha avuto luogo tra la Comunità e l'Islanda e la Norvegia[3] e che è allegato all'accordo in questione.

(11) La presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen al quale il Regno Unito non partecipa, ai sensi della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[4]. Il Regno Unito non partecipa pertanto alla sua adozione, non è da essa vincolato e non è soggetto alla sua applicazione.

(12) La presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen al quale l'Irlanda non partecipa ai sensi della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen[5]. L'Irlanda non partecipa pertanto alla sua adozione, non è da essa vincolata e non è soggetta alla sua applicazione,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1.È istituito un sistema di scambio tra gli Stati membri di dati relativi ai visti, in seguito denominato «sistema d'informazione visti» (VIS), che permette alle autorità nazionali autorizzate di inserire e aggiornare dati relativi ai visti, nonché di consultare tali dati per via elettronica.

2.Il sistema d'informazione visti è basato su un'architettura centralizzata ed è costituito da un sistema d'informazione centrale, in seguito denominato «sistema centrale d'informazione visti» o «CS-VIS», con un'interfaccia in ciascuno Stato membro, in seguito denominata «interfaccia nazionale» o «NI-VIS», che assicura il collegamento con la competente autorità centrale nazionale del rispettivo Stato membro, e dall'infrastruttura di comunicazione tra il sistema centrale d'informazione visti e le interfacce nazionali.

Articolo 2

1.Il sistema centrale d'informazione visti, l'interfaccia nazionale in ciascuno Stato membro e l'infrastruttura di comunicazione tra il sistema centrale di informazione visti e le interfacce nazionali sono sviluppati dalla Commissione.

2.Le infrastrutture nazionali sono adeguate e/o sviluppate dagli Stati membri.

Articolo 3

Le misure necessarie allo sviluppo del sistema centrale d'informazione visti, dell'interfaccia nazionale in ciascuno Stato membro e dell'infrastruttura di comunicazione tra il

(1) *G.U.C.E.* 10 luglio 1999, L 176/36.
(2) *G.U.C.E.* 10 luglio 1999, L 176/31.
(3) *G.U.C.E.* 10 luglio 1999, L 176/53.
(4) *G.U.C.E.* 1 giugno 2000, L 131/43.
(5) *G.U.C.E.* 7 marzo 2002, L 64/20.

sistema centrale d'informazione visti e le interfacce nazionali sono adottate secondo la procedura di cui all'articolo 5, paragrafo 2, quando riguardano questioni diverse da quelle elencate nell'articolo 4.

Articolo 4

Le misure necessarie allo sviluppo del sistema centrale d'informazione visti, dell'interfaccia nazionale in ciascuno Stato membro e dell'infrastruttura di comunicazione tra il sistema centrale d'informazione visti e le interfacce nazionali sono adottate secondo la procedura di cui all'articolo 5, paragrafo 3, per quanto riguarda i seguenti aspetti:

a) la progettazione dell'architettura fisica del sistema, compresa la relativa rete di comunicazione;
b) gli aspetti tecnici che influiscono sulla protezione dei dati di carattere personale;
c) gli aspetti tecnici con importanti implicazioni finanziarie per i bilanci degli Stati membri o con implicazioni tecniche di rilievo per i sistemi nazionali degli Stati membri;
d) lo sviluppo dei requisiti di sicurezza, compresi gli aspetti biometrici.

Articolo 5

1.La Commissione è assistita dal comitato istituito dall'articolo 5, paragrafo 1, del regolamento (CE) n. 2424/2001 del Consiglio, del 6 dicembre 2001, sullo sviluppo del sistema d'informazione Schengen di seconda generazione (SIS II)[1].

2.Nei casi in cui è fatto riferimento al presente paragrafo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE.

Il periodo di cui all'articolo 4, paragrafo 3, della decisione 1999/468/CE è fissato a due mesi.

3.Nei casi in cui è fatto riferimento al presente paragrafo, si applicano gli articoli 5 e 7 della decisione 1999/468/CE.

Il periodo di cui all'articolo 5, paragrafo 6, della decisione 1999/468/CE è fissato a due mesi.

4.Il comitato adotta il proprio regolamento interno.

Articolo 6

La Commissione presenta una relazione annuale al Parlamento europeo e al Consiglio sulla situazione dello sviluppo del sistema centrale d'informazione visti, dell'interfaccia nazionale in ciascuno Stato membro e dell'infrastruttura di comunicazione tra il sistema centrale di informazione visti e le interfacce nazionali e la prima di tali relazioni è presentata entro la fine dell'anno in cui è firmato il contratto per lo sviluppo del VIS.

Articolo 7

La presente decisione si applica a decorrere dal ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea .

Articolo 8

Gli Stati membri sono destinatari della presente decisione conformemente al trattato che istituisce la Comunità europea.

Lussemburgo, 8 giugno 2004

Per il Consiglio
Il presidente
M. McDowell

(1) *G.U.C.E.* 13 dicembre 2001, L 328/4.

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

ARTICLE 29 - DATA PROTECTION WORKING PARTY

Brussels, 30 November 2004

Mr. Joseph BORREL FONTELLES
President of the European Parliament
European Parliament
Rue Wiertz
B - 1047 BRUSSELS

Subject: Proposal for a Council Regulation on standards for security features and biometrics in EU citizens's passports

(*) www.europa.eu.int/comm/internal_market/privacy/docs/news/art29-eupassports_en.pdf

52 Regolamento (CE) n. 2252/2004 del Consiglio del 13 dicembre 2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri (*)

REGOLAMENTO (CE) N. 2252/2004 DEL CONSIGLIO

del 13 dicembre 2004

relativo alle norme sulle caratteristiche di sicurezza
e sugli elementi biometrici dei passaporti e dei documenti di viaggio
rilasciati dagli Stati membri

(*) *G.U.C.E.* 29 dicembre 2004, L 385/1.

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

FUNDAMENTAL RIGHTS SERIES

E.U. NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS
(CFR-CDF)
RÉSEAU U.E. D'EXPERTS INDÉPENDANTS EN MATIÈRE DE DROITS FONDAMENTAUX

REPORT ON THE SITUATION OF FUNDAMENTAL RIGHTS IN THE EUROPEAN UNION IN 2003

January 2004

Reference : CFR-CDF.repEU.2003

The E.U. Network of Independent Experts on Fundamental Rights has been set up by the European Commission upon request of the European Parliament. It monitors the situation of fundamental rights in the Member States and in the Union, on the basis of the Charter of Fundamental Rights. It issues reports on the situation of fundamental rights in the Member States and in the Union, as well as opinions on specific issues related to the protection of fundamental rights in the Union. The content of this opinion does not bind the European Commission. The Commission accepts no liability whatsoever with regard to the information contained in this document.

(*) http://europa.eu.int/comm/justice_home/cfr_cdf/doc/report_eu_2003_en.pdf

Autorità di controllo comune dell'Europol

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

Novembre 2002 - Ottobre 2004

L'Europol e l'autorità di controllo comune

L'Europol è l'organizzazione creata per assistere gli Stati membri dell'UE nella prevenzione e nella lotta di forme gravi di criminalità organizzata internazionale, soltanto ove ciò implichi una struttura criminale organizzata e riguardi almeno due Stati membri. A livello pratico, l'Europol si occupa principalmente di agevolare lo scambio d'informazioni tra gli Stati membri e fornire competenze in materia di analisi criminologiche.

Poiché l'Europol gestisce un'ingente quantità di dati sensibili a carattere personale, la convenzione Europol contiene una serie di disposizioni che impongono all'Europol di tenere conto dei diritti delle persone nell'utilizzare tali informazioni. La convenzione prevede inoltre l'istituzione dell'autorità di controllo comune (ACC), un organismo indipendente incaricato di assicurare l'ottemperanza dell'Europol ai principi relativi alla protezione dei dati personali.

Al fine di promuovere la trasparenza, la convenzione dell'Europol richiede all'autorità di controllo comune di pubblicare, a intervalli regolari, una relazione sulle attività svolte: il presente documento è la seconda di dette relazioni.

Premessa

Sono onorato di presentare la seconda relazione di attività dell'autorità di controllo comune dell'Europol (ACC). Il documento riguarda il periodo compreso tra novembre 2002 e ottobre 2004 e riflette i risultati conseguiti dall'ACC sotto la presidenza di Klaus Kalk. A nome dei miei colleghi dell'ACC, desidero rendere omaggio alla dedizione di Klaus Kalk al nostro lavoro, nonché alla sua ferma posizione a favore della dignità umana e del diritto fondamentale della protezione dei dati. Sono inoltre consapevole che i risultati ottenuti da questo organismo sono stati possibili soltanto grazie all'impegno e all'entusiasmo di Varges Gomes e Giuseppe Busia, i due presidenti del comitato per i ricorsi in carica nel periodo in questione, unitamente agli sforzi congiunti di tutti i membri dell'ACC e del suo segretariato.

La presente relazione fornisce una rassegna dettagliata dei temi principali di cui si è occupata l'ACC in un periodo fortemente caratterizzato dalle misure adottate per combattere il terrorismo dopo i tragici eventi dell'11 settembre 2001 negli Stati Uniti e, recentemente, dagli attentati di Madrid nel marzo 2004. Nei suoi pareri e nelle iniziative attuate, l'ACC ha dimostrato che è sicuramente possibile, e per nulla incompatibile, sostenere l'obiettivo comune della lotta al terrorismo internazionale e alla criminalità organizzata, salvaguardando nel contempo i diritti dei singoli.

Infine, considerato che i pilastri dell'UE continuano a convergere e la protezione dei dati di natura personale è stata inclusa come diritto fondamentale nella Carta dei diritti fondamentali dell'Unione europea e nel progetto del Trattato costituzionale, risulta sempre più

evidente che il campo della cooperazione di polizia e giudiziaria necessita di norme chiare e specifiche sulla protezione dei dati, con la formulazione di un parere indipendente e di un'attività di controllo armonica. Svariate iniziative riguardanti questo aspetto saranno valutate nei prossimi mesi ed è intenzione dell'ACC seguire con attenzione gli sviluppi, offrendo assistenza e consulenza, con l'intento di assicurare che ogni cambiamento proposto si traduca in un progetto pratico, sempre nel pieno rispetto dei diritti e dei valori della protezione dei dati.

Emilio Aced Félez
Presidente

Capitolo I - Introduzione

Dal momento che, sottoscrivendo il Trattato di Amsterdam, gli Stati membri hanno assunto l'impegno di creare "uno spazio di libertà, sicurezza e giustizia", uno degli obiettivi principali dell'Unione europea è stato quello di intensificare la cooperazione tra le autorità incaricate dell'applicazione della legge. La maggior parte delle volte, tale cooperazione comporta lo scambio di dati personali.

L'atrocità dei recenti attacchi terroristici ha dato nuovo slancio a questa tendenza, promuovendo una più stretta collaborazione; inoltre, la convinzione degli Stati membri della necessità di collaborare per far fronte al terrorismo ha determinato una riconsiderazione delle misure in atto nell'UE a salvaguardia della sicurezza.

Questo primo capitolo presenta un resoconto delle reazioni dell'ACC di fronte ad alcuni dei cambiamenti che si sono verificati in quest'area, concentrandosi in particolare su due situazioni che si sono venute a creare: una determinata dalla decisione presa dal direttore dell'Europol e l'altra conseguente all'iniziativa di aggiornare le disposizioni della convenzione Europol.

L'Europol e gli Stati Uniti

Poco dopo gli attacchi terroristici contro gli Stati Uniti avvenuti nel settembre 2001, il direttore dell'Europol decise di autorizzare la trasmissione di dati personali da parte dell'Europol agli Stati Uniti.

Le norme che disciplinano la trasmissione di dati personali detenuti dall'Europol a Stati terzi solitamente prevedono un accordo ufficiale tra l'Europol e lo Stato in questione, in cui sono indicate le disposizioni riguardanti le categorie di dati da trasmettere e le finalità per cui tali informazioni possano essere impiegate. Un accordo di questo genere non può essere concluso senza aver prima ottenuto il parere dell'autorità di controllo comune (ACC).

In casi eccezionali, tuttavia, il direttore dell'Europol può evitare questa procedura e decidere di trasmettere dei dati personali senza la stipulazione di un accordo, se ritiene che ciò sia assolutamente necessario per tutelare gli interessi fondamentali degli Stati membri oppure per impedire un pericolo imminente.

In risposta alla decisione del direttore, l'ACC ha formulato un parere in cui sottolineava che soltanto un accordo ufficiale avrebbe potuto costituire un fondamento giuridico soddisfacente per una cooperazione a lungo termine tra l'Europol e gli Stati Uniti, e che pertanto in alcun modo la decisione avrebbe potuto essere equivalente a un'autorizzazione illimitata alla trasmissione di dati agli Stati Uniti.

Nel corso delle negoziazioni per la stesura di un accordo tra Europol e gli Stati Uniti, entrambe le parti hanno cercato di risolvere numerose questioni nodali, tra cui le finalità per cui i dati avrebbero potuto essere utilizzati e il problema della supervisione dell'attuazione dell'accordo.

Nel suo parere sul progetto di accordo, l'ACC riconosceva l' "imperativo" di migliorare la cooperazione tra Stati Uniti ed Europol nella lotta contro la criminalità organizzata e, rimar-

cando i notevoli progressi compiuti durante i negoziati, l'ACC concludeva che il Consiglio poteva autorizzare la sottoscrizione dell'accordo da parte del direttore dell'Europol.

L'ACC, tuttavia, sottolineava che considerata la legislazione statunitense in materia di protezione di dati di natura personale, avrebbe dovuto essere esercitato un efficace controllo per garantire l'osservanza delle disposizioni dell'accordo da parte dei suoi sottoscrittori.

In che modo l'ACC controlla l'accordo tra Europol e gli Stati Uniti?

Dalla firma dell'accordo l'ACC ha operato come segue:

ha istituito dei collegamenti con il Chief Privacy Officer (responsabile per la protezione della vita privata) del Dipartimento statunitense della sicurezza interna. Il Chief Privacy Officer ha il compito di assicurare che il Dipartimento della sicurezza interna ottemperi alle disposizioni dell'accordo e ad altre importanti misure relative alla tutele della privacy. Nel marzo 2004, il sostituto del Chief Privacy Officer ha partecipato a una riunione dell'ACC per fornire informazioni sulla legislazione statunitense sulla privacy attualmente in vigore. I membri dell'ACC hanno colto l'occasione per rivolgere delle domande sul preciso ruolo del Chief Privacy Officer. L'ACC è desiderosa di sviluppare ulteriormente questo rapporto in futuro, in quanto costituirà un'opportunità non solo per accertare che cosa avviene dei dati inviati negli Stati Uniti nell'ambito dell'accordo, ma anche per permettere all'ACC di conoscere quali misure siano adottate negli Stati Uniti per verificare la correttezza dei dati inviati all'Europol.

Inoltre, l'ACC ha vigilato sugli sviluppi. L'ACC ha notato che in seguito a cambiamenti della legislazione statunitense, l'FBI non era più tenuto a garantire la correttezza dei dati conservati nel National Crime Information Center, la più grande banca dati penale-giudiziaria del Paese. Questa cambiamento suscita preoccupazione, in quanto l'FBI è una delle autorità federali che, ai sensi dell'accordo, è autorizzata allo scambio di dati personali con l'Europol. L'ACC ha richiesto ulteriori informazioni all'Europol per stabilire se questo cambiamento influirà sui dati personali trasmessi ai sensi del presente accordo. L'ACC si rammarica di non aver ricevuto fino ad oggi una risposta.

L'ACC mantiene fede all'impegno di vigilare sull'ottemperanza all'accordo. Dalla sua sottoscrizione, lo scambio della maggior parte delle informazioni tra l'UE e le autorità di polizia statunitensi sembrerebbe essere avvenuto ai sensi di accordi bilaterali esistenti tra gli Stati Uniti e singoli Stati membri. Tuttavia, dato che il volume di informazioni scambiate tra Europol e Stati Uniti aumenterà, le ispezioni future dell'Europol si concentreranno sull'esame dei dati di natura personale scambiati nell'ambito dell'accordo, per assicurare che vi sia conformità alle disposizioni pertinenti. Inoltre, l'ACC cercherà di coordinare l'attività di vigilanza, collaborando con le autorità nazionali incaricate della protezione dei dati personali negli Stati membri e con il Chief Privacy Officer presso il Dipartimento della sicurezza interna negli Stati Uniti.

L'emendamento della convenzione Europol: tempi di conservazione dei dati

Nel 2002, la Presidenza danese ha varato un'iniziativa per modificare la convenzione dell'Europol. L'autorità di controllo comune ha espresso un parere, in cui commentava le proposte legate al trattamento dei dati di natura personale. La Presidenza danese ha tenuto conto delle perplessità dell'ACC e molte proposte sono state emendate conseguentemente.

Al momento della sua pubblicazione nel dicembre 2002, un progetto di protocollo per emendare la convenzione Europol includeva una proposta di estensione del periodo di conservazione dei dati di natura personale negli archivi di lavoro per fini di analisi. L'Articolo 21 della convenzione Europol stabilisce che le informazioni su una persona conservate in archivi di lavoro per fini di analisi all'Europol devono essere cancellate al più tardi dopo tre anni dalla loro introduzione, se in tale periodo non sono state aggiunte ulteriori informazioni sulla persona in questione. Il progetto di protocollo si prefiggeva di estendere il periodo di conservazione a cinque anni.

Inizialmente l'ACC non riteneva giustificato il prolungamento del periodo di conservazione, nonostante l'Europol sostenesse che, nel caso di alcune forme di criminalità, ed in particolare del terrorismo, fossero necessari periodi di conservazione più lunghi per svolgere analisi efficaci.

Nel febbraio 2003, il gruppo d'ispezione dell'ACC esaminò approfonditamente gli archivi di lavoro per fini di analisi e concluse che periodi di conservazione più lunghi erano indubbiamente necessari in alcuni casi, ma che, per stabilire se dei dati di natura personale dovessero essere conservati o meno, sarebbe stato più utile ricorrere ad una verifica della necessità dell'archivio, anziché ad un limite temporale fisso.

Convinta di ciò, l'ACC ha quindi proposto di emendare la convenzione Europol in modo che il periodo di conservazione fosse collegato all'archivio anziché ai dati di natura personale in esso contenuti. L'Europol dovrebbe cancellare gli archivi di lavoro dopo un periodo di tre anni, salvo nel caso in cui, alla scadenza di tale periodo, l'Europol non ritenga assolutamente necessaria la prosecuzione di un particolare archivio. In tal caso, l'archivio potrebbe restare aperto per altri tre anni.

Sebbene in tal caso l'Europol avrebbe la possibilità di verificare la necessità dell'archivio alla fine di ogni triennio, una volta presa la decisione di tenere attivo un archivio, l'Europol dovrebbe ripetere la procedura per la costituzione di un archivio di lavoro per fini di analisi di cui all'articolo 10 della convenzione Europol. In tal modo, l'ACC e il consiglio di amministrazione dell'Europol avrebbero la possibilità di esaminare le ragioni per mantenere attivo un determinato archivio e il processo sarebbe tenuto sotto controllo, eliminando l'eventualità che un archivio resti aperto illimitatamente.

Per impedire che i dati personali siano conservati anche quando non è più necessario, è stato proposto che la convenzione continui a prevedere l'obbligo per l'Europol di valutare annualmente la necessità di conservare dati personali presenti negli archivi di lavoro. Inoltre, l'ACC potrà chiedere specificatamente al gruppo d'ispezione di esaminare qualsiasi archivio ancora attivo, nel corso di un'ispezione.

L'emendamento proposto dall'ACC è stato approvato e incluso nella versione finale del protocollo per la modificare la convenzione Europol[1].

Collaborare per promuovere la protezione dei dati

Attualmente le iniziative dell'UE che comportano la raccolta, la conservazione o lo scambio di dati personali ai fini dell'applicazione della legge, sono numerose; tra gli esempi più significativi vi sono misure per consentire lo scambio di dati sui passeggeri di voli aerei nonché proposte per richiedere la conservazione dei dati delle comunicazioni. Questi ed altri sviluppi, quali il suggerimento di trasformare un giorno l'Europol in un'agenzia investigativa, potrebbero avere rilevanti implicazioni per i diritti degli individui. Pertanto, l'ACC ha ricercato la collaborazione di altre autorità che si occupano della protezione dei dati per garantire che i responsabili delle decisioni politiche tengano conto dei problemi legati a questo aspetto.

Per un certo periodo di tempo l'ACC è stata schierata con istituzioni omologhe quali l'autorità di controllo comune di Schengen e l'autorità di controllo comune delle dogane, che hanno il compito di vigilare rispettivamente sul sistema d'informazione di Schengen e sul sistema d'informazione doganale. Tutte e tre le autorità di vigilanza si avvalgono dello stesso segretariato con sede a Bruxelles e, tra le iniziative volte a coordinare le loro attività, è rientrata la creazione di un gruppo di lavoro composto da esperti tecnici delle istituzioni nazionali incaricate della protezione dei dati. Questo gruppo, che è stato istituito per fornire sostegno tecnico alle autorità di controllo comune, sta attualmente sviluppando uno strumento standard per l'ispezione dei sistemi d'informazione del terzo pilastro.

Inoltre, in vista di un invito a presentare resoconto dinanzi a un comitato ristretto della "Camera dei Lord" (House of Lords), le tre autorità di controllo comune hanno di recente tenuto una riunione congiunta insieme ai rappresentanti dell'autorità di controllo comune di Eurjoust, da cui è scaturito un parere comune sulla protezione dei dati nell'ambito del terzo pilastro. Sono previsti ulteriori incontri di questo tipo, per consentire alle autorità di controllo comune di esaminare le questioni di mutuo interesse.

È chiaro, tuttavia, che molte delle nuove iniziative dell'Unione europea che riguardano dati personali non fanno parte di mandati specifici delle autorità di controllo comune e,

(1) Atto del Consiglio del 27 novembre 2003 che stabilisce un protocollo recante modifica alla convenzione Europol.

sicuramente, non tutte rientrano in modo netto in uno dei tradizionali pilastri dell'UE.

Per questo motivo, in occasione della conferenza delle autorità incaricate della protezione dei dati svoltasi a Rotterdam nel 2004, è stato deciso che i rappresentanti di quelle autorità che operano a livello comunitario, si riuniscano per coordinare la loro attività. Alla prima riunione di questo gruppo "di pianificazione", che ha avuto luogo nel giugno 2004, hanno partecipato il garante europeo della protezione dei dati, i presidenti delle autorità di controllo comune, la presidenza del gruppo di lavoro dell'articolo 29, che ha il compito di fornire consulenza alla Commissione su questioni inerenti alla protezione dei dati nell'ambito del primo pilastro.

La situazione si è ulteriormente evoluta nel settembre 2004 in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati a Wroclaw, quando una sessione a porte chiuse delle autorità europee ha approvato una risoluzione in cui si chiede che le istituzioni dell'UE promuovano un forum in cui le autorità europee incaricate della protezione dei dati possano discutere le implicazioni a livello di protezione dei dati degli sviluppi del terzo pilastro. Fino alla creazione di tale forum, le iniziative del terzo pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune, saranno esaminate da un gruppo di lavoro delle autorità europee incaricate della protezione dei dati.

Capitolo II
Parte A - Attività di vigilanza

1. Ispezione dell'Europol

La conduzione d'ispezioni in loco delle attività dell'Europol è uno dei modi adottati dall'autorità di controllo comune per ottemperare al suo mandato generale.

Ispezione - Febbraio 2003

Nel dicembre 2003, l'ACC ha dato incarico al suo gruppo d'ispezione di esaminare gli archivi di lavoro per fini di analisi e i sistemi d'informazione dell'Europol, nonché il grado di conformità agli accordi ufficiali tra Europol e Stati terzi.

Nel febbraio 2003, detto gruppo ha condotto un'ispezione di tre giorni presso l'Europol. Nella relazione finale, approvata nel luglio 2003, si dichiarava che il livello di protezione dei dati all'Europol era migliorato dalla prima ispezione effettuata nel 2000, pur notando che l'Europol aveva incontrato problemi per quanto riguarda la salvaguardia della qualità dei dati. Questo era da imputarsi soprattutto al fatto che l'Europol deve affidarsi alla qualità dei dati ricevuti dagli Stati terzi. L'ACC, pertanto, ha proposto alle autorità nazionali incaricate della protezione dei dati di cercare di risolvere questo problema a livello nazionale.

Nel complesso, il gruppo di ispezione ha concluso che, sulla base dei controlli effettuati durante l'ispezione, il trattamento dei dati di natura personale da parte dell'Europol avveniva nel pieno rispetto delle relative disposizioni in materia, osservando che in alcuni campi particolari, quali la verifica e la registrazione dei dati, l'Europol aveva applicato sistemi conformi ad elevati standard di protezione dei dati.

Sono state quindi formulate delle raccomandazioni con l'intento di migliorare ulteriormente la conformità dell'Europol; un'ispezione di verifica ha avuto luogo nel novembre 2003.

Ispezioni - Obiettivi strategici

È chiaro che il ruolo dell'Europol si sta sviluppando rapidamente, con un numero sempre maggiore di dati trattati. Poiché è ferma convinzione dell'ACC che le ispezioni dell'Europol debbano tenere il passo con tali evoluzioni, nel 2003 l'autorità di controllo comune ha fissato una serie di obiettivi volti a guidare le ispezioni future. In sintesi, gli obiettivi sono i seguenti:

- le ispezioni dell'Europol devono avvenire con scadenza annuale;
- occorre ispezionare con particolare attenzione la qualità dei dati personali conservati da Europol;
- infine, il gruppo di ispezione deve godere di una maggior discrezionalità relativamente

alla portata dell'ispezione, disponendo della duttilità necessaria per esaminare particolari aree di interesse nel momento in cui queste si presentino.

Ispezione - marzo 2004

Tenendo conto di questi obiettivi, l'ACC ha approvato una nuova ispezione dell'Europol, sottolineando che avrebbe dovuto incentrarsi sulla qualità dei dati trattati negli archivi per fini di analisi.

L'ispezione, durata tre giorni, è iniziata il 30 marzo 2004. Prima dell'ispezione, il gruppo aveva scelto un certo numero di archivi di lavoro da esaminare. Per ognuno di essi il gruppo valutava la conformità alla decisione costitutiva dell'archivio per stabilire se le categorie di dati personali conservati e gli Stati membri partecipanti all'attività dell'archivio corrispondessero a quelli elencati nella decisione. Da ogni archivio venivano poi estrapolati dei campioni di dati e la loro qualità era confrontata con quella del documento originale.

Nonostante siano state individuate alcune imprecisioni, nel complesso la qualità dei dati è stata ritenuta soddisfacente, almeno per quanto riguarda la rispondenza dei dati negli archivi con quelli forniti dagli Stati membri. Tuttavia, è stata riscontrata un'incapacità generale da parte degli Stati membri di valutare correttamente i dati (verificando la fonte, l'affidabilità e così via). Ancora una volta, l'ACC ha sottolineato che, per risolvere questo problema, occorre migliorare la cooperazione tra Stati Membri ed Europol.

Inoltre, il gruppo ha rilevato che, in alcuni casi, si presentava una palese divergenza tra quanto indicato nella decisione costitutiva di un particolare file e quanto avveniva in realtà. Per esempio, le decisioni costitutive non sempre comprendevano un elenco recente delle parti che contribuivano all'archivio e, in alcuni casi, soltanto alcune delle categorie di dati riportate nella decisione costitutiva venivano realmente trattate nell'archivio. Il gruppo, pertanto, ha raccomandato all'Europol di procedere ad un esame dell'archivio dopo un certo periodo di tempo dalla sua costituzione (per esempio un anno), per chiarire la natura dei contributi degli Stati partecipanti. La decisione costitutiva dovrebbe poi essere aggiornata per rispecchiare la reale portata della partecipazione.

Il sistema d'informazione dell'Europol

All'epoca dell'istituzione dell'Europol, una delle sue priorità era quella di sviluppare un sistema d'informazione a livello europeo, che avrebbe raccolto informazioni su persone sospettate di essere coinvolte in reati che rientrassero nell'area di competenza dell'Europol. Uno dei compiti principali dell'ACC è quello di controllare detto sistema (il sistema d'informazione dell'Europol) e verificare la sua ottemperanza alle disposizioni sulla protezione dei dati.

È opportuno fornire un breve resoconto dello sviluppo del sistema, che è stato irto di difficoltà.

Il processo di pianificazione e sviluppo del sistema ebbe inizio nel 1996. Questioni di carattere contrattuale emersero sin dall'inizio, aggravati da richieste di aggiunte al sistema (per esempio fu deciso di ampliare il sistema per includere funzionalità relative alla falsificazione dell'euro). Pertanto, ci sono state numerose versioni del sistema nel corso del suo sviluppo. Una versione limitata del sistema che consente all'Europol di scaricare la proprie responsabilità relativamente all'euro, è entrata in funzione nel 2001.

Nella relazione annuale 2003 dell'Europol sono stati illustrati i recenti problemi incontrati con la versione finale del sistema.

"Delivery of the Europol Information System (EIS) … was planned for February 2003. However, it was not delivered due to the underestimation of the number of problems that would arise… The expected revised delivery date of June was met but when delivered, the product was not up to standard." [La consegna del sistema di informazione dell'Europol (Europol Information System - EIS)… era prevista per febbraio 2003. Tuttavia, la consegna non ha potuto aver luogo perché sono stati sottovalutati gli eventuali problemi… . La prevista data di consegna rivista di giugno è stata rispettata ma, il prodotto si è rivelato al di sotto dello standard richiesto.]

Quando la versione finale del sistema sarà operativa negli Stati membri (è stato anticipato che ciò potrebbe avvenire prima della fine del 2004), l'ACC ha intenzione di collaborare con le autorità nazionali incaricate della protezione dei dati per vigilare attentamente sul sistema, tenendo sotto costante sorveglianza il modo in cui viene utilizzato. Inoltre, una buona parte delle ispezioni future saranno dedicate a esaminare il sistema per garantire che ci si attenga alle disposizioni pertinenti sulla protezione dei dati.

2. Europol - Un ruolo di sostegno

Si continua a discutere in merito alla forma che con precisione deve assumere il sostegno in materia di analisi dell'Europol agli Stati membri. Il problema è sorto inizialmente alla luce di una scoperta fatta dal gruppo di ispezione dell'ACC.

Progetti operativi degli Stati membri con il supporto dell'Europol (MSOPES)

Nel corso della prima ispezione dell'Europol avvenuta nel novembre 2000 il gruppo di ispezione scoprì che l'Europol forniva sostegno in materia di analisi a indagini condotte dagli Stati membri. Questi progetti (noti come *Member States' Operational Projects with Europol Support – MSOPES*, ovvero Progetti operativi degli Stati membri con il supporto dell'Europol) prevedevano la creazione di archivi di lavoro per fini di analisi presso l'Europol, la cui responsabilità, tuttavia, era degli Stati membri anziché dell'Europol.

Nonostante l'Europol abbia il compito generico di contribuire alle indagini negli Stati membri, l'articolo 10 della convenzione Europol stabilisce una procedura da seguire quando si costituiscono archivi per fini di analisi all'Europol. Oltre a stabilire le categorie di dati di carattere personale che possono essere conservate in questi archivi, l'articolo prevede che il direttore dell'Europol dia all'ACC la possibilità di esprimersi sulla decisione costitutiva di un archivio. Gli archivi dei MSOPES, tuttavia, non erano costituiti conformemente a questa procedura. L'ACC puntualizzò che la creazione e l'uso di archivi per fini di analisi all'Europol, doveva essere limitato a quanto previsto dall'articolo 10 della convenzione Europol e che, pertanto, la costituzione degli archivi dei MSOPES era illegittima. In considerazione delle preoccupazioni dell'ACC, il Consiglio ha deciso di non creare un fondamento giuridico per i MSOPES, con la conseguente cessazione del funzionamento degli archivi associati.

Squadre investigative comuni

L'ACC sta attualmente valutando la portata del sostegno in materia di analisi fornito dall'Europol nell'ambito di un'altra struttura. Il Trattato di Amsterdam contemplava l'impegno a creare delle "squadre investigative comuni", con l'auspicio che questi gruppi contribuissero a indagini comuni condotte da due o più Stati.

Una decisione quadro del Consiglio[1] ha introdotto delle regole comuni per queste squadre e ha specificato che potevano includere "funzionari di organismi costituiti ai sensi del Trattato sull'Unione europea", una definizione che interessa anche il personale dell'Europol. I particolari specifici riguardanti la partecipazione di Europol a squadre investigative comuni sono quindi stati definiti in un Protocollo adottato dal Consiglio[2]. Anche se le disposizioni del protocollo stabilivano che il personale dell'Europol doveva partecipare con "funzioni di supporto", gli agenti dell'Europol che seguivano una squadra investigativa comune sarebbero stati inseriti nella catena di comando della squadra e le informazioni dell'Europol sarebbero state condivise direttamente attraverso il componenti della squadra dell'Europol; inoltre le informazioni raccolte dalla squadra sarebbero state inserite nelle banche dati dell'Europol.

L'ACC riconosce che dopo la ratifica da parte degli Stati membri del protocollo recante modifica della convenzione, l'Europol potrà partecipare a squadre investigative comuni e scambiare informazioni con gli altri componenti di una squadra in particolare. Ciò tuttavia non comporta un'aggiunta nell'elenco delle autorità con cui l'Europol è attualmente autorizzato a scambiare informazioni. Tuttavia, se la partecipazione ad una squadra investigativa comune dovesse comportare la creazione di archivi per fini di analisi presso l'Europol, si potrebbe stabilire un parallelo con la situazione verificatasi nel caso dei MSOPES, soprattutto dal momento che nel protocollo non si rinviene alcun fondamento giuridico per la costituzione di archivi per fini di analisi al di fuori di quanto previsto dall'articolo 10.

(1) Decisione quadro del Consiglio del 13 giugno 2002 relativa alle squadre investigative comuni.
(2) Atto del Consiglio del 28 novembre 2002 che stabilisce un protocollo recante modifica della convenzione.

L'ACC ha chiesto informazioni in merito all'esistenza di una eventuale politica formulata dall'Europol riguardante il tipo di sostegno che sarebbe offerto alle squadre investigative comuni. In particolare l'ACC si è informata sul modo in cui l'Europol intende utilizzare i suoi servizi di analisi.

Apparentemente il processo decisionale relativamente al tipo di sostegno da fornire alle squadre investigative comuni quando il protocollo sarà stato ratificato da tutti gli Stati membri, è attualmente in corso. Fino alla ratifica del protocollo, l'Europol potrà assistere le squadre investigative comuni conformemente a quanto previsto dalla convenzione Europol. L'Europol ha comunicato all'ACC che il sostegno fornito alle squadre investigative comuni nel frattempo si limiterà all'analisi di informazioni e di dati in linea con le disposizioni della convenzione, all'individuazione di divari nelle informazioni, alla divulgazione di relazioni analitiche che forniscono valutazioni di informazioni assemblate e all'identificazione di nuovi progetti in seguito all'analisi.

L'ACC ha intenzione di vigilare sulla situazione per assicurare il rispetto della convenzione Europol. Sarà particolarmente interessante vedere come l'Europol interpreterà il suo ruolo nelle squadre investigative comuni dopo la modifica della convenzione.

3. Decisione costitutiva di archivi per fini di analisi

Ogni qual volta l'Europol intenda costituire un nuovo archivio di lavoro per fini di analisi ai sensi dell'articolo 10 della convenzione Europol, è necessario adottare una decisione costitutiva. Tale decisione deve stabilire, tra i vari aspetti, le finalità dell'archivio e le categorie di dati di natura personale che possono essere conservati. Le decisioni devono essere approvate dal consiglio di amministrazione dell'Europol, che è obbligato a sottoporle al parere dell'autorità di controllo comune. È politica dell'ACC esprimere il proprio parere su ogni decisione costitutiva.

Nel periodo trattato dalla presente relazione, l'ACC ha formulato osservazioni relativamente a nove decisioni costitutive di archivi per fini di analisi. Nella maggior parte dei casi non ha espresso alcun commento, anche se in un'occasione l'ACC ha chiesto chiarimenti su un certo numero di punti e ha posto domande in merito all'inclusione di alcune categorie di dati nella decisione costitutiva. Europol ha risposto eliminando queste categorie di dati dalla decisione.

Al momento della stesura della presente relazione, Europol stava trattando dati personali in diciannove diversi archivi per fini di analisi.

4. Accordi con Stati/organismi terzi

Se l'Europol intende trasmettere dati personali al di fuori dell'UE, tale trasmissione deve essere preceduta dalla firma di un accordo ufficiale tra l'Europol e lo Stato in questione. Prima della stipulazione di un accordo di questo genere l'Europol deve ricevere il parere dell'ACC.

Negli ultimi due anni l'Europol ha siglato accordi con i seguenti Stati terzi: Repubblica slovacca, Cipro, Lettonia, Lituania e Malta (tutti questi paesi sono nel frattempo entrati a far parte dell'UE, cessando di essere Stati terzi) nonché Bulgaria e Romania. In tutte le occasioni, ha formulato numerose osservazioni a carattere generale, concludendo, tuttavia, che, sotto l'aspetto della protezione dei dati, non sussistevano impedimenti alla sottoscrizione dell'accordo da parte dell'Europol.

Eurojust

L'Europol ha altresì firmato un accordo ufficiale con Eurojust, l'autorità incaricata di migliorare la cooperazione giudiziaria nell'Unione europea. Nel suo primo parere formulato sull'accordo di massima tra Europol e Eurojust, l'ACC ha rilevato che la decisione del Consiglio che istituiva Eurojust prevedeva che il Consiglio consultasse l'autorità di controllo comune dell'Eurojust prima di approvare l'accordo stesso. Poiché in questo caso la procedura coinvolgeva due organismi di controllo comune, l'ACC dell'Europol ha chiarito che, prima di adottare la posizione definitiva, avrebbe voluto conoscere il parere dell'ACC dell'Eurojust. Visto che l'ACC dell'Eurojust non era ancora operativa all'epoca della formu-

lazione del primo parere dell'ACC dell'Europol (maggio 2003), tale primo parere doveva essere considerato un parere provvisorio sull'accordo di massima.

Nel suo parere provvisorio l'ACC sottolineava che, anche dopo la sottoscrizione dell'accordo, i membri nazionali del collegio di Eurojust avrebbero avuto diritto di ricevere dati personali dall'Europol soltanto nell'ambito dell'articolo 6 della decisione del Consiglio relativa alla costituzione di Eurojust e per nessun'altra finalità. Nel parere si suggeriva anche di modificare l'accordo in modo che Europol ed Eurojust fossero obbligati a rispettare eventuali condizioni relativamente all'uso dei dati trasmessi nell'ambito dell'accordo.

Una volta costituita l'ACC dell'Eurojust, il suo presidente e il sig. Kalk (all'epoca presidente dell'ACC dell'Europol) si sono incontrati per discutere l'accordo. Nel dicembre 2003, l'ACC dell'Europol ha espresso un secondo parere in cui si affermava che non sussistevano più impedimenti al perfezionamento dell'accordo, a condizione che lo scambio di dati iniziasse soltanto dopo l'applicazione da parte di Eurojust di misure supplementari per salvaguardare la sicurezza dei dati.

È possibile prendere visione dei pareri dell'ACC sui vari accordi nel sito web dell'ACC all'indirizzo: http://europoljsb.ue.eu.int.

5. Diritti

La convenzione Europol conferisce ai singoli individui numerosi diritti. Ai sensi dell'articolo 19 della convenzione, chiunque ha diritto di accesso a qualsiasi informazione detenuta da Europol che lo riguarda. Se l'informazione relativa al richiedente risulta errata, la persona interessata può domandare all'Europol di sopprimere o correggere l'informazione in questione.

Dai dati forniti dall'Europol emerge che sono state presentate dieci richieste di accesso nel 2002; nel 2003 sono state inoltrate soltanto sei domande e nel 2004 l'Europol ha fino ad ora ricevuto dieci richieste di accesso (a tutto settembre).

Gli interessati possono chiedere all'ACC di garantire la legittimità e la correttezza delle modalità di raccolta, memorizzazione, trattamento e impiego dei dati personali che li riguardano. Sinora, l'ACC ha ricevuto due richieste di questo tipo e, dopo aver effettuato l verifiche necessarie, è risultato che in entrambi i casi l'Europol aveva agito conformemente alla convenzione Europol.

Parte B - Gestione dell'autorità di controllo comune

L'autorità di controllo comune si è riunita nove volte dal novembre 2002 all'ottobre 2004. L'ACC è costituita da rappresentanti delle autorità nazionali incaricate della protezione dei dati degli Stati membri. Un elenco dei membri è riportato nel sito web dell'ACC.

I preparativi all'allargamento hanno costituito una delle sfide che l'ACC ha dovuto affrontare; contestualmente, l'autorità di controllo comune ha riflettuto su come garantire maggiore trasparenza e accessibilità più agevole ai suoi utenti. Una breve sintesi di entrambi gli aspetti è illustrata qui di seguito.

1. Preparativi all'allargamento

In occasione della riunione del giugno 2003, l'ACC ha dato il benvenuto a colleghi degli Stati in fase di adesione. Anche se i dieci Paesi avrebbero aderito all'Unione soltanto nel 2004, i rappresentanti degli Stati in fase di adesione sono stati invitati a partecipare a questa riunione e a quelle future in qualità di osservatori, con la speranza che in tal modo acquisiscano familiarità con i lavori dell'ACC. Prima della riunione, è stato distribuito un questionario con l'intento di raccogliere informazioni sia sulla legislazione in materia di protezione dei dati di natura personale in detti Stati, sia sulla misura in cui tale legislazione si applica alle forze di polizia.

Particolarmente incoraggiante è stato apprendere che le autorità incaricate della prote-

zione dei dati negli Stati in fase di adesione si sono impegnate a fondo per creare rapporti di lavoro con le autorità di polizia. Dai risultati del questionario è emerso che, tra le varie iniziative, le autorità incaricate della protezione dei dati hanno condotto ispezioni sulle procedure adottate dalla polizia, hanno svolto verifiche delle condizioni di sicurezza, hanno tenuto riunioni per discutere la politica da adottare e hanno tenuto formazioni per la polizia su questioni relative alla protezione dei dati personali.

L'ACC ha organizzato una visita dell'Europol per gli osservatori per dare loro un'idea di come l'Europol svolge i suoi vari compiti. Nell'ottobre 2003, le delegazioni di cinque Stati in fase di adesione hanno trascorso due giorni al quartiere generale dell'Europol a L'Aia. Erano presenti anche i rappresentanti delle autorità incaricate della protezione dei dati di Islanda e Norvegia, Stati terzi che beneficiano del diritto di partecipare allo scambio di dati personali.

Nonostante gli Stati in fase di adesione siano entrati a far parte dell'UE nel maggio 2004, le loro delegazioni sono diventate membri a pieno titolo dell'ACC soltanto dopo che i rispettivi Paesi hanno aderito alla convenzione Europol, soddisfacendo tutte le condizioni dell'articolo 46. Dal 1° ottobre 2004, le delegazioni che rappresentano le autorità incaricate della protezione dei dati di Cipro, Repubblica ceca, Ungheria, Lettonia, Lituania e Slovacchia sono diventate membri a tutti gli effetti.

In qualità di membri dell'ACC, questi nuovi colleghi ricopriranno un ruolo cruciale nella protezione dei diritti fondamentali in tutta l'Unione europea allargata.

2. Trasparenza

L'ACC svolge le sue funzioni per conto del pubblico e quindi è importante che l'Accstessa e i suoi processi decisionali siano trasparenti.

Il regolamento interno dell'ACC stabilisce che i documenti prodotti dall'autorità di controllo comune sono riservati, tranne nel caso in cui essa non decida altrimenti. È attualmente in corso una modifica del regolamento che prevede l'inversione di questo principio, per cui tutti i documenti saranno accessibili al pubblico a meno non si ritenga che esiste un interesse pubblico prevalente contro la pubblicazione, per esempio nel caso in cui rendere noto un particolare documento possa compromettere seriamente l'attività dell'Europol.

I documenti saranno messi a disposizione del pubblico o direttamente in forma elettronica (nel sito *web* dell'Acc), oppure in seguito ad una richiesta scritta. Ogni domanda di accesso ad un documento comporterà una valutazione dell'eventuale esistenza di motivi per cui il documento non possa essere messo a disposizione. Nei casi in cui soltanto una parte del documento sia esente dalla proibizione di pubblicazione, il documento sarà nuovamente redatto e sarà fornita la versione parziale.

L'ACC si propone di pubblicare tutti i nuovi pareri unitamente alle decisioni del comitato per i ricorsi nel suo sito web all'indirizzo: *http://europoljsb.ue.eu.int*

Capitolo III - Il comitato per i ricorsi

Chiunque ha accesso alle informazioni che lo riguardano in possesso dell'Europol ed ha il diritto di richiedere che tali informazioni siano verificate, corrette o soppresse. Chiunque volesse esercitare uno di questi diritti e non fosse soddisfatto della risposta dell'Europol, può appellarsi al comitato per i ricorsi dell'ACC. Nonostante i suoi componenti facciano parte dell'ACC, il comitato per i ricorsi è un organismo autonomo ed imparziale, e non è condizionato da istruzioni dell'ACC. Le decisioni del comitato per i ricorsi sono definitive per tutte le parti interessate.

Sebbene il comitato per i ricorsi abbia deciso in merito a due casi soltanto nel corso degli ultimi due anni, il numero dei ricorsi è aumentato e attualmente vi sono parecchi casi su cui il comitato deve esprimersi. È ragionevole supporre che il numero di ricorsi continuerà ad aumentare a mano a mano che i cittadini impareranno a conoscere l'Europol e saranno mag-

54

giormente consapevoli dei propri diritti; il comitato per i ricorsi si è pertanto preoccupato di snellire le sue procedure per assicurare che i ricorsi futuri siano trattati celermente.

I due casi illustrati dettagliatamente qui di seguito hanno portato a decisioni relative a importanti questioni di principio.

Nel primo caso, il comitato per i ricorsi ha deciso che l'Europol deve considerare nel merito ogni richiesta di accesso, anziché applicare un approccio generale.

Nel secondo caso, il comitato per i ricorsi ha deciso che l'Europol deve rispondere ad una richiesta di accesso nella lingua in cui tale richiesta è stata formulata, purché essa sia una delle lingue ufficiali dell'Unione europea.

1. Sintesi del ricorso presentato dal signor Y

Il signor Y si è rivolto all'autorità olandese incaricata delle protezione dei dati per chiedere di accedere ad eventuali dati che lo riguardano in possesso dell'Europol. La richiesta è stata inoltrata all'Europol.

Nella sua risposta, l'Europol ha concluso affermando che:

"Ai sensi dell'articolo 19 della convenzione Europol e della legislazione dei Paesi Bassi, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della convenzione Europol".

In risposta a quest'argomentazione, il sig. Y ha presentato un ricorso al comitato per i ricorsi, lamentandosi del "velo di segretezza" che circondava la decisione dell'Europol.

Il diritto di accesso è sancito dall'articolo 19, paragrafo 1, della convenzione Europol e, nonostante l'estensione di tale diritto non sia specificatamente definita alla luce dell'articolo 14, paragrafo 1 delle convenzione Europol, deve essere considerata alla stregua del diritto definito dall'articolo 8 della convenzione d'Europa del 28 gennaio 1981. Tale diritto consente a chiunque di accertare se sono archiviati dati di carattere personale che lo riguardano e, in caso affermativo, gli conferisce il diritto di prenderne conoscenza. Il ricorso del sig. Y riguardava entrambi gli aspetti del diritto di accesso.

Ai sensi dell'articolo 19, paragrafo 3, il diritto di accesso deve essere esercitato conformemente alla legislazione dello Stato membro presso il quale la persona interessata l'ha fatto valere, in questo caso i Paesi Bassi. L'articolo 19, paragrafo 3, stabilisce altresì che, qualora la legislazione dello Stato membro interpellato preveda la "comunicazione relativa ai dati" (con cui si intende sia la comunicazione di un'eventuale trattamento dei dati, sia la comunicazione dei dati che sono trattati), quest'ultima è rifiutata dall'Europol se ciò è necessario per: il corretto svolgimento delle funzioni dell'Europol; per la protezione della sicurezza e dell'ordine pubblico; per la lotta contro i crimini; oppure per la protezione dei diritti di terzi.

Le eccezioni previste al diritto di accesso agli archivi di polizia ai sensi della legislazione olandese sono molto simili a quelli elencati nella convenzione Europol e il comitato per i ricorsi ha stabilito che le disposizioni sia della convenzione Europol, sia della legislazione olandese impongono che, per ogni richiesta di accesso, si proceda a una verifica della necessità di applicare un'eccezione al pieno esercizio del diritto di accesso. Le eccezioni sono ammesse soltanto se gli interessi della polizia o di terzi contano di più dell'interesse della persona interessata nell'esercizio del proprio diritto di accesso.

L'argomentazione dell'Europol per non confermare, né negare l'esistenza di informazioni in suo possesso riguardanti il sig. Y si basa sull'articolo 19, paragrafo 4 della convenzione Europol. In base a questo articolo, se uno Stato membro obietta alla comunicazione dei dati, l'Europol notifica al richiedente che le verifiche sono state effettuate *senza fornire informazioni che possano rivelargli se abbia o meno informazioni sul suo conto.* L'Europol sosteneva che, per poter adempiere a questo obbligo, non avrebbe mai potuto informare apertamente una persona interessata l'effettiva inesistenza presso l'Europol di dati sul suo conto, poiché, facendolo, si consentirebbe ad altri di dedurre che l'Europol detiene informazioni su di loro,

confrontando le varie risposte ricevute dall'Europol. Pertanto, dire al sig. Y che l'Europol non è in possesso di informazioni che lo riguardano, costituirebbe, stando all'argomentazione, un indiretto inadempimento dell'obbligo di cui all'articolo 19, paragrafo 4.

Il comitato per i ricorsi ha rilevato che anche se l'articolo 19, paragrafo 4, impone all'Europol di tenere conto dei desideri delle parti interessate nel trattamento dei dati di natura personale in questione, le disposizioni non stabiliscono la procedura nei casi in cui non sono conservati dati. Il comitato per i ricorsi ha pertanto decretato che la procedura di cui all'articolo 19, paragrafo 4, non doveva essere considerata come un obbligo per l'Europol alla stessa stregua dell'articolo 19, paragrafo 3. Una richiesta di accesso, quando non ci sono dati trattati, deve sempre essere valutata caso per caso e l'Europol non è libero di decidere in merito alla richiesta basandosi soltanto su di un obbligo che esiste in situazioni in cui è in possesso dati personali trattati.

Dopo aver considerato la risposta dell'Europol alla richiesta di accesso del sig. Y, il comitato per i ricorsi ha concluso che la decisione dell'Europol non si basava su di una valutazione del singolo caso e pertanto non era conforme all'articolo 19, paragrafo 3 della convenzione Europol. L'Europol avrebbe almeno dovuto verificare se le eccezioni menzionate nell'articolo 19, paragrafo 3 della convenzione Europol erano applicabili a questo caso in particolare. In assenza di tale evidenza, o anche di elementi che la suggeriscano, l'Europol non avrebbe dovuto rifiutare una comunicazione.

La decisione dell'Europol è stata ritenuta contravvenire alla legislazione olandese applicabile e all'articolo 19, paragrafo 3, della convenzione Europol. Dopo un'attenta valutazione delle informazioni disponibili, il comitato per i ricorsi ha concluso che in questo caso l'articolo 19, paragrafo 3 della convenzione Europol non poteva giustificare un'eccezione al diritto di accesso e ai sensi dell'articolo 19, paragrafo 7 di tale convenzione e ha decretato che l'Europol avrebbe dovuto chiarire al sig. Y che nessun dato che lo riguardava era stato trattato.

2. Sintesi del ricorso presentato dal sig. Z

Dopo aver inoltrato una richiesta di accesso (attraverso l'autorità incaricata della protezione dei dati), il sig. Z ha ricevuto una risposta dall'Europol, in cui si dichiarava quanto segue:

"In conformità con la procedura stabilita dalla convenzione Europol e della legislazione del Belgio, desidero comunicarLe che, facendo seguito alla sua richiesta sono state compiute le verifiche negli archivi dell'Europol. Ai sensi dell'articolo 19 della convenzione Europol e della legislazione del Belgio, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della convenzione Europol".

Il sig. Z ha presentato ricorso al comitato per i ricorsi, comunicandogli successivamente che poiché aveva "scelto l'olandese come lingua ufficiale" voleva una traduzione della decisione dell'Europol, che era stata fornita soltanto in inglese. Il ricorso del sig. Z è stato riconosciuto ammissibile per quanto attiene al suo reclamo di non aver ricevuto una risposta nella propria lingua.

Il comitato per i ricorsi ha chiesto all'Europol perché avesse risposto in inglese, dato che tutta la corrispondenza con il sig. Z era stata in olandese.

L'Europol, a sua volta, ha informato il comitato che rispondere alle domande relative all'articolo 19 in inglese costituiva la procedura standard, tranne nel caso in cui il richiedente chiedesse esplicitamente di volere ricevere una risposta nella propria lingua, nel qual caso l'Europol cercava di soddisfare la richiesta purché ciò non richiedesse eccessivo sforzo. L'Europol non era stato informato, se non dal comitato per i ricorsi, del desiderio del sig. Z di ricevere la traduzione in olandese della risposta alla sua domanda di accesso.

La convenzione Europol non prevede un regime linguistico specifico per l'Europol. Tuttavia, ai sensi dell'articolo 14 della convenzione, il diritto di accesso alle informazioni in possesso dell'Europol deve essere considerato alla stessa stregua di quello contemplato dall'articolo 8 della convenzione del 1981 del Consiglio d'Europa relativo alla protezione dei

dati. L'articolo 8 della convenzione del Consiglio d'Europa dispone che ogni persona deve ottenere la conferma dell'esistenza o meno nel casellario automatizzato dei dati di carattere personale a essa relativi, come pure la trasmissione di tali dati "in forma intelleggibile". Il comitato per i ricorsi ha ritenuto che la lingua in cui le informazioni sono state fornite era rilevante per stabilire se una risposta poteva essere considerata intelleggibile.

Considerando l'Europol un organismo dell'Unione europea che prevede l'attiva partecipazione delle autorità incaricate del rispetto della legge nei singoli Stati membri, il comitato per i ricorsi ha suggerito che, nei casi di domande di accesso ai sensi dell'articolo 19 della convenzione Europol, esso applichi un regola simile a quella contemplata dall'articolo 21 del Trattato che istituisce la Comunità europea, il quale prevede che chiunque scriva a uno qualsiasi degli organismi dell'UE in una lingua ufficiale dell'Unione, riceva una risposta in quella stessa lingua.

Il comitato per i ricorsi ha pertanto deciso che l'Europol non aveva ottemperato ai principi dell'articolo 8 della convenzione del 1981 del Consiglio d'Europa nel rispondere alla richiesta di accesso del sig. Z: l'Europol avrebbe dovuto comunicare la sua decisione nella lingua impiegata dal sig. Z, anche se egli non l'aveva richiesto esplicitamente. Poiché il diritto di accesso ha lo scopo di consentire alle persone interessate di accertarsi che le informazioni che le riguardano siano archiviate conformemente alla legge, l'Europol deve rispondere ai richiedenti nella loro lingua, se questa è una lingua ufficiale dell'UE.

In conclusione il comitato ha osservato che, poiché l'Europol aveva poi fornito al sig. Z una traduzione in olandese della decisione originale, il caso era chiuso. Il comitato per i ricorsi ritiene che l'Europol da allora abbia aggiornato le sue procedure e che adesso risponda alle richieste di accesso nella lingua utilizzata dal richiedente.

È possibile prendere visione di tutte le decisioni del comitato per i ricorsi, unitamente ad altre informazioni sui diritti sanciti dalla convenzione Europol, nel sito web dell'ACC all'indirizzo: http://europoljsb.ue.eu.int

Capitolo IV - Gli ultimi due anni

Il primo capitolo della presente relazione fornisce un resoconto del modo in cui l'ACC ha affrontato due situazioni diverse che si sono verificate proprio nel momento in cui l'UE è stata costretta a riflettere sulla sua sicurezza.

Nel trattare questi due casi, l'ACC ha adottato un approccio pragmatico. Il parere dell'ACC sull'accordo dell'Europol con gli Stati Uniti, con il suo riconoscimento della necessità di migliorare la cooperazione, è stato oggetto di critiche da parte di certi ambienti. Ciononostante, l'ACC continua a tener fede al suo impegno di vigilare sull'attuazione dell'accordo per assicurare che questa sia conforme con le disposizioni dell'accordo stesso.

L'ACC ha adottato un atteggiamento proattivo nel proporre la modifica della convenzione Europol e la proposta in sé rispecchia la convinzione dell'ACC che le disposizioni relative alla protezione dei dati contenute nella convenzione Europol non vogliono essere un ostacolo al lavoro dell'Europol, bensì esistono per garantire il rispetto dei diritti dei singoli da parte dell'Europol nello svolgimento dei suoi compiti legittimi.

Anche se l'aggiunta di nuovi colleghi provenienti da dieci nuovi Stati membri ha ovviamente fatto una notevole differenza per l'ACC come organismo, l'allargamento è risultato un fatto positivo e l'ACC sta oggi beneficiando del patrimonio di esperienze dei suoi nuovi membri.

L'ACC ha continuato a svolgere la sua funzione di vigilanza, esaminando tutti gli accordi che l'Europol ha formulato con Stati ed organismi terzi e verificando le decisioni di costituzione di archivi. L'ACC attribuisce una notevole importanza alle ispezioni dell'Europol, in quanto forniscono ai gruppi d'ispezione un'esperienza diretta del lavoro dell'Europol e danno un'idea di come le procedure scritte volte alla salvaguandia dei diritti funzionano realmente nella pratica. L'ACC ha riscontrato che durante queste ispezioni il personale

dell'Europol è estremamente collaborativo e dalle ispezioni di controllo è emerso che l'Europol considera prioritaria l'attuazione delle raccomandazioni dell'ACC.

Nel corso degli ultimi due anni, l'ACC ha cercato di adottare un approccio costruttivo, garantendo nel contempo l'adozione di misure di tutela per salvaguardare i diritti fondamentali.

Il futuro

Ci sono stati molti sviluppi che hanno coinvolto l'Europol negli ultimi due anni e ci sono indicazioni che il ruolo dell'Europol continuerà ad evolversi. La creazione di squadre investigative comuni, per esempio, lascia supporre che le attività dell'Europol siano destinate a diventare di natura sempre più operativa.

Contemporaneamente, degli sviluppi altrove (in particolare i progetti di un sistema d'informazione di Schengen di seconda generazione) hanno suggerito l'idea di rendere interoperativi i sistemi d'informazione dell'Unione con finalità collegate. Tutti questi cambiamenti devono essere affrontati con cautela, specialmente in considerazione dei problemi che sono stati incontrati nello sviluppare il sistema d'informazione dell'Europol. Inoltre qualsiasi intervento in questa direzione dovrebbe essere preceduto da una valutazione del suo impatto sulla privacy, per stabilire le potenziali implicazioni per i diritti delle persone.

Le misure per salvaguardare la protezione dei dati devono andare di pari passo con gli sviluppi, e sarà particolarmente importante assicurare una reale vigilanza dell'Europol, oltreché degli altri sistemi d'informazione a livello europeo. Da parte sua l'ACC ha intrapreso azioni per migliorare la cooperazione con altre autorità incaricate della protezione dei dati nel tentativo di superare le intese alquanto rigide per vigilare sulla protezione dei dati a livello UE. L'ACC si aspetta di contribuire a qualsiasi dibattito relativo a modi per migliorare queste soluzioni.

C'è anche la questione di più vasta portata del controllo parlamentare dell'Europol. Nel 2002 la Commissione ha concluso che le misure di controllo esistenti, adottate per vigilare sull'operato dell'Europol (esercitate dai parlamenti nazionali, dal Parlamento europeo, dalle autorità incaricate della protezione dei dati, dall'ACC e dal consiglio di amministrazione dell'Europol), non erano da considerarsi "giuridicamente insufficienti". Si osservava, tuttavia, che "era necessario qualcosa di più chiaro e trasparente".(1)

Questioni di questo genere non rientrano nell'ambito di responsabilità dell'ACC, ma è chiaro che nel momento in cui i compiti dell'Europol diventeranno sempre più operativi, l'attività di controllo e vigilanza dell'operato dell'Europol dovrà adeguarsi per tenere conto di questo cambiamento.

Obiettivi per i prossimi due anni

Nei prossimi due anni l'ACC si adopererà per:

- svolgere le ispezioni annuali dell'Europol, riservando una particolare attenzione all'attuazione del sistema d'informazione dell'Europol;
- elevare il suo profilo all'interno delle istituzioni dell'UE per assicurare che i problemi relativi alla protezione dei dati siano presi in considerazione al momento della formulazione di nuove iniziative che coinvolgono l'Europol. In particolare, l'ACC ha intenzione di proporre l'instaurazione di regolari contatti con il comitato del Parlamento europeo sulle libertà civili, giustizia e affari interni;
- collaborare con i colleghi dei nuovi Stati membri, aiutandoli a fornire informazioni alle autorità di polizia sulle disposizioni in materia di protezione dei dati della convenzione Europol;
- collaborare con le autorità omologhe e la più vasta comunità che si occupa della protezione dei dati per formulare una risposta coerente e costruttiva alle nuove iniziative che coinvolgono l'impiego di dati personali per finalità legate all'applicazione della legge;
- accrescere la consapevolezza dei diritti conferiti alle persone dalla convenzione Europol;
- continuare a esaminare le decisioni costitutive di archivi e gli accordi per lo scambio di dati di carattere personale con Stati e organismi terzi.

(1) Comunicazione della Commissione al Parlamento europeo e al Consiglio - Controllo democratico dell'Europol 26 febbraio 2002 COM (2002) 95 finale.

Autorità di controllo comune Schengen

55 Il parere 2004 SIS II

1. Introduzione

Nell'intento di garantire che il sistema informativo Schengen di seconda generazione – SIS II – rispettasse gli standard più elevati di protezione dei dati, l'Autorità Comune di Controllo (ACC) si è adoperata per incidere sullo sviluppo del sistema fin dall'inizio.

Nonostante che il Consiglio, nelle conclusioni raggiunte in data 5 e 6 giugno 2003, avesse previsto alcuni requisiti generali per il nuovo sistema, non si è pervenuti ad una decisione definitiva rispetto agli specifici contenuti ed alle funzionalità da includere nel sistema stesso né, elemento questo di essenziale importanza, in merito alle specifiche finalità di questo sistema di seconda generazione[1].

Il presente parere prende in esame l'evoluzione subita dalle finalità per le quali il SIS è stato inizialmente costituito, e passa in rassegna le varie proposte concernenti il SIS II analizzando quali possibili modifiche esse comportino rispetto alla natura del sistema. Infine, sono esposte le motivazioni per le quali l'ACC ritiene che sia necessario giungere quanto prima ad una decisione sui compiti che si intende attribuire al nuovo sistema.

L'ACC continuerà a seguire gli sviluppi del SIS II e fornirà indicazioni più puntuali non appena siano confermate proposte specifiche in merito al sistema.

2. Il Sistema Informativo Schengen

2.1. Il contesto di riferimento

Il SIS è stato costituito inizialmente quale una delle misure compensative previste al fine di consentire la libera circolazione delle persone. Il sistema in quanto tale offriva lo strumento per effettuare controlli alle frontiere ed altri controlli di polizia e doganali.

Poiché le competenti autorità dovevano avere la possibilità di effettuare rapidamente tali controlli, il sistema fu sviluppato secondo una configurazione hit/no-hit. In pratica, ciò significava che la ricerca effettuata nel SIS rispetto ad una determinata persona avrebbe indicato se tale persona era oggetto di una segnalazione e, in caso affermativo, le misure da adottare immediatamente. Si prevedeva che il SIS avrebbe trattato esclusivamente i dati necessari a tal fine, e che ogni ulteriore informazione dovesse essere ottenuta attraverso gli uffici SIRENE.

La Convenzione Schengen ha stabilito chi fosse responsabile del trattamento dei dati contenuti nel SIS, ed ha previsto una serie di garanzie per i diritti degli interessati. Secondo i dati più recenti, nel SIS sono contenute attualmente informazioni relative a circa un milione di individui.

2.2. Il contesto si modifica

Nel 2003, si leggeva quanto segue nelle conclusioni del Consiglio:

"Il SIS è un sistema a configurazione hit/no-hit che consente lo scambio di informazioni

(1) Nel presente documento ogni riferimento alle conclusioni del Consiglio deve intendersi come relativo alle conclusioni dell'incontro del Consiglio europeo nel settore giustizia ed affari interni tenutosi a Lussemburgo il 5 e 6 giugno 2003.

al fine di regolamentare la libera circolazione delle persone e mantenere la pubblica sicurezza, ed in particolare assistere autorità nazionali nella lotta contro la criminalità transnazionale, nel quadro dell'obiettivo fissato dall'UE di mantenere e sviluppare l'Unione come un'area di libertà, sicurezza e giustizia".

Si tratta di una definizione più ampia di quella prevista dall'Articolo 93 della Convenzione di Schengen, e ben segnala il contesto in cui il SIS è venuto a collocarsi dopo l'incorporazione dell'acquis di Schengen nella struttura giuridica e istituzionale dell'Unione europea.

Il potenziamento della cooperazione fra le autorità di polizia nazionali e la creazione di nuovi organismi, come Europol, hanno dato luogo ad una situazione in cui le informazioni detenute nel SIS sono considerate una preziosa risorsa nella lotta alla criminalità ed al terrorismo.

È stato proposto un nuovo Sistema informativo Schengen per fare fronte all'allargamento dell'UE, nella convinzione che tale nuovo sistema avrebbe potuto beneficiare delle nuove tecnologie tenendo conto, al contempo, di altri sviluppi nel settore della giustizia e degli affari interni. È in questo contesto, ed alla luce di questi obiettivi generali, che sono state messe a punto le proposte concernenti il SIS II.

3. SIS II

3.1. Lo sviluppo di un nuovo sistema

Si potrebbe affermare che lo sviluppo di un nuovo sistema del tipo descritto si svolge su tre fronti: il processo decisionale di natura politica, che dovrebbe definire quali siano le finalità previste per il sistema e le relative modalità di funzionamento; il quadro giuridico, che dovrebbe fornire la base giuridica specificando le finalità del sistema e stabilendo le norme relative all'accesso e ad altri elementi; lo sviluppo tecnico del sistema in quanto tale.

La previsione iniziale era che dal Consiglio del giugno 2003 sarebbero dovute emergere proposte ben definite sulle finalità e le funzionalità del SIS II; tuttavia, come sottolineato dal Parlamento europeo nella raccomandazione adottata sul punto, "il Consiglio non ha ancora adottato decisioni in merito a questioni concrete come le nuove categorie di oggetti o persone da inserire".(1)

Questa mancanza di indicazioni univoche ha generato una situazione tale da obbligare la Commissione a formulare una proposta in cui si chiede di garantire la massima flessibilità possibile al nuovo sistema. Pertanto, la messa a punto del sistema avviene sotto l'impulso delle mutevoli istanze provenienti dal settore giustizia e affari interni dell'UE, anziché sulla base di obiettivi espressi e definiti all'interno di un quadro giuridico preciso. Se questo stato di cose dovesse permanere, la natura del sistema potrebbe modificarsi in misura radicale trasformando il SIS II in uno strumento investigativo ed amministrativo multiscopo. Sarebbe un fatto preoccupante che lo sviluppo del SIS II proseguisse in questo modo frammentario, poiché la mancanza di trasparenza connaturata a tale approccio complica la valutazione delle modifiche che tutto ciò comporta rispetto alla natura del sistema stesso.

3.2. SIS II – Uno strumento flessibile

"Fin dalle prime riflessioni sul SIS II è stato chiaro che il sistema dovrebbe essere uno strumento flessibile, … in grado di adattarsi al mutare delle circostanze e di rispondere, in tempi ragionevoli e senza eccessivi costi e sforzi aggiuntivi, alle richieste formulate dagli utenti durante il suo periodo di operatività".

Il brano sopra riportato è tratto dalle conclusioni del Consiglio del giugno 2003 ed evidenzia un elemento basilare nello sviluppo del SIS II. In effetti, nella sua più recente Comunicazione in merito, la Commissione ha indicato la "flessibilità" fra i requisiti essenziali del nuovo sistema, affermando che "Il SIS II dovrebbe avere le potenzialità per trattare un numero di dati molto più grande e per essere inoltre in grado, una volta che il sistema sarà operativo, di gestire nuovi tipi di informazioni, nuovi oggetti e nuove funzioni, di cui si sta discutendo all'interno del Consiglio".(2)

(1) Raccomandazione del Parlamento europeo al Consiglio sul Sistema informativo Schengen di seconda generazione (SIS II), del 20 novembre 2003.
(2) Comunicazione della Commissione al Consiglio ed al Parlamento europeo: Sviluppo del Sistema di informazione Schengen II e possibili sinergie con un futuro Sistema di informazione visti, dell'11 dicembre 2003.

55

Il requisito di configurare un sistema flessibile di natura indefinita comporta vari problemi.

In primo luogo, esiste la preoccupazione che un sistema flessibile si presti più facilmente ad una "deriva funzionale", nel senso che le richieste provenienti da un'ampia gamma di organismi ed enti potrebbero dare luogo ad una situazione per cui le informazioni detenute nel sistema verrebbero utilizzate per scopi diversi da quelli inizialmente previsti.

In secondo luogo, è difficile comprendere come sia possibile valutare adeguatamente le implicazioni potenziali del SIS II se il suo sviluppo deve essere flessibile al punto da non fare luce sulla configurazione finale del sistema. La creazione di un sistema caratterizzato da un tale margine di flessibilità in assenza di limitazioni di alcun genere non può che rendere più difficile per chi sta lavorando alla sua messa a punto tenere conto del principio di proporzionalità, che dovrebbe essere uno dei cardini nella definizione di qualsiasi progetto di tale natura.

Man mano che procede lo sviluppo del sistema, ed aumentano gli utenti e le categorie di dati, anche la cornice giuridica dovrà subire un'evoluzione conseguente – non da ultimo perché le garanzie attualmente in vigore per tutelare i diritti degli interessati sono state progettate soltanto in rapporto al SIS nella sua configurazione originale. A parere dell'ACC, il primo passo da compiere al riguardo dovrebbe consistere in una valutazione dell'impatto-privacy per stabilire in quali termini il SIS II e le sue nuove e molteplici funzionalità potrebbero incidere sui diritti degli interessati. Le risultanze di tale valutazione potrebbero successivamente fungere da base per la definizione di una nuova cornice giuridica.

4. SIS II – Le proposte di modifica del sistema

4.1. Accesso al sistema

Le istanze avanzate nei confronti del SIS durante gli ultimi anni riflettono gli sviluppi intervenuti nell'UE per quanto riguarda la lotta alla criminalità ed al terrorismo. Vi è stata, ad esempio, un'iniziativa del Regno di Spagna finalizzata a consentire ad Europol ed Eurojust di accedere al SIS.[1] Permettere a tali soggetti di accedere al sistema comporterà alcune conseguenze sulla natura del SIS II, essendo maggiormente probabile che i dati ricavati dal sistema siano utilizzati operativamente dai due soggetti in questione, ad esempio per quanto riguarda le Squadre Investigative Comuni in ambito Europol. L'ACC resta dell'opinione che le attività in rapporto alle quali si consente l'accesso debbano essere conformi agli articoli della Convenzione Schengen che regolamentano l'accesso a e l'utilizzazione delle informazioni contenute nel sistema.

Consentire che soggetti esterni accedano al SIS può persino modificare radicalmente le finalità per le quali si utilizzano le informazioni presenti nel sistema. In un recente parere su una proposta della Commissione che mirava a concedere l'accesso al SIS alle autorità responsabili dell'immatricolazione dei veicoli, l'ACC ha rilevato che una scelta del genere avrebbe costituito una deviazione rispetto alle finalità originali del sistema in quanto, dando corso alla proposta, il SIS sarebbe stato utilizzato a sostegno della politica comune dell'UE in materia di trasporti.

Ciononostante, la tendenza a consentire ad un numero crescente di soggetti di accedere al SIS sembra destinata a continuare. Il Consiglio ha concluso che altre autorità devono avere la possibilità di accedere al SIS, anche se ciò dovesse comportare la possibilità di "un accesso parziale o per scopi diversi da quelli inizialmente previsti dalla segnalazione".

L'ACC è consapevole dell'essenzialità di un potenziamento della cooperazione fra autorità giudiziarie e di polizia per migliorare la sicurezza in Europa e, in tal senso, potrebbe risultare opportuno consentire ad altri soggetti, in determinati casi, di accedere ai dati presenti nel SIS. Tuttavia, si dovrebbe permettere l'accesso al sistema soltanto se ciò risulti necessario e proporzionato, e non semplicemente perché ne è data la possibilità. È per tale motivo che l'ACC ritiene necessario che si chiariscano le specifiche finalità per le quali Europol ed Eurojust – e qualsiasi altro ente – chiedono di accedere al SIS II. L'adeguamento normativo che dovrebbe accompagnare la messa a punto del nuovo sistema sembra offrire

(1) L'iniziativa è culminata, da ultimo, nell'adozione del Regolamento del Consiglio (CE) n. 871/2004 del 29 aprile 2004.

l'occasione ideale per garantire che le finalità ed i rapporti in questione siano fissati nell'ambito di una chiara cornice giuridica.

Tale cornice giuridica dovrebbe prevedere una serie di limiti all'utilizzabilità dei dati ricavati dal sistema, ed è importante garantire che i soggetti abilitati ad accedere al SIS siano tenuti a rispettare gli stessi standard di protezione dei dati previsti nella Convenzione Schengen ed in altri atti normativi pertinenti, come la Convenzione del Consiglio d'Europa del 1981 sulla protezione dei dati.

L'approccio frammentario seguito nello stabilire quali autorità debbano accedere al SIS continua ad essere fonte di preoccupazione per l'ACC. Nonostante le conclusioni del Consiglio del giugno 2003, e l'intenzione manifestata dalla Commissione di configurare il nuovo sistema con la massima flessibilità possibile, l'ACC ritiene di fare propria la raccomandazione formulata dal Parlamento europeo secondo cui "l'uso dei dati [deve avvenire] per motivi espressamente dichiarati in anticipo". Nella raccomandazione, il Parlamento si opponeva a qualsiasi deroga rispetto a tale principio, "come quella di cui alle conclusioni del Consiglio del 5 e 6 giugno 2003 che chiede lo studio ulteriore della "possibilità per talune autorità di utilizzare i dati SIS a scopi diversi da quelli per i quali essi sono stati inizialmente inseriti nel SIS".

Se si vuole assicurare la possibilità che altri soggetti siano abilitati ad accedere al SIS II una volta che quest'ultimo sia operativo, devono essere stabiliti chiaramente i parametri sui quali basare ogni decisione in materia. Tali parametri dovrebbero essere fissati attraverso norme di rango legislativo che prendano in considerazione, ad esempio, la possibilità di consentire l'accesso sia ai soggetti privati sia a quelli pubblici.

4.2. Le informazioni presenti nel sistema

4.2.1. Ulteriori categorie di dati

Appare verisimile un aumento delle pressioni finalizzate all'ampliamento delle categorie di dati presenti nel sistema, soprattutto perché la proposta di configurare il SIS II come sistema flessibile faciliterà l'aggiunta in futuro di nuove categorie. Vi sono già stati alcuni sviluppi in questo campo. La decisione-quadro del Consiglio che stabilisce un mandato di arresto europeo prevede che le informazioni contenute nel nuovo mandato di arresto siano trattate in ambito SIS. L'aggiunta di nuove categorie di dati potrebbe trasformare il SIS II in un doppione di altri sistemi informativi UE quali il sistema di informazione Europol o il sistema informativo doganale, ed uno sviluppo del genere potrebbe avere riflessi sul livello di protezione dei dati.

L'ACC ritiene che siano necessari parametri univoci onde stabilire quali informazioni possano essere contenute nel SIS II e, ancora una volta, il punto di partenza per giungere ad una decisione in materia non può che essere la valutazione delle finalità del sistema.

4.2.2. Nuove tipologie di dati: identificatori biometrici

Vi sono progetti che prevedono l'introduzione di nuove tipologie di dati, e particolare interesse hanno suscitato i dati biometrici.

Si afferma che è necessario che il SIS II contenga identificatori univoci allo scopo di consentire alle competenti autorità nazionali di risolvere eventuali problemi legati all'identità di singoli individui, e nelle conclusioni del Consiglio si legge che il SIS II dovrebbe permettere "la conservazione, il trasferimento e l'eventuale ricerca di dati biometrici, in particolare fotografie ed impronte digitali".

La Comunicazione della Commissione (dicembre 2003) fornisce alcuni esempi di situazioni nelle quali sarebbe utile disporre di identificatori biometrici. Una di esse riguarda il caso in cui le autorità arrestino una persona in possesso di documenti falsi. Attualmente non sarebbe possibile stabilire, sulla base delle informazioni presenti nel SIS, se sia stata inserita una segnalazione concernente la stessa persona ma sotto altro nome. Tuttavia, se nel sistema fossero conservati anche identificatori biometrici, come le impronte digitali, si potrebbe riuscire a confrontare i rilievi dattiloscopici della persona in oggetto con tutti quelli conservati

55

nel sistema. In tal modo gli utenti potrebbero stabilire se sia stata inserita o no una segnalazione concernente la stessa persona sotto un altro nome.

In un altro esempio citato per dimostrare l'utilità di accedere a identificatori biometrici, la Commissione menzionava il caso in cui il sistema rilevi uno hit ma la persona in oggetto affermi che la segnalazione riguarda un'altra persona (risulta che i "falsi positivi" siano molto frequenti quando si ha a che fare con nomi di larga diffusione). Si affermava che casi del genere troverebbero rapida soluzione se le autorità potessero confrontare l'identificatore biometrico della persona in oggetto con quello conservato unitamente alla segnalazione presente nel sistema. In tal modo, le autorità sarebbero in grado di stabilire se la persona in oggetto sia realmente quella nei cui confronti era stata inserita una precedente segnalazione.

Questi esempi illustrano i due possibili campi di applicazione delle tecnologie biometriche incorporate in un sistema di informazione. La prima opzione, in cui l'utente effettua una ricerca su tutti gli identificatori biometrici nel sistema fino a trovare una corrispondenza (one-to-many), è nota come sistema di "identificazione"; la seconda opzione, in cui l'identificatore biometrico di uno specifico individuo viene confrontato con una specifica segnalazione presente nel sistema per stabilire se si tratti della stessa persona (one-to-one), è nota come sistema di "verifica".

L'affidabilità dei due sistemi è diversa, come diversi sono gli scopi per i quali i due sistemi possono essere utilizzati; tuttavia, quale che sia il sistema prescelto, siamo di fronte ad un altro esempio di decisione da assumere partendo dalla valutazione delle finalità del sistema ed applicando un test di proporzionalità.

4.2.3. Nuove tipologie di dati: alcune garanzie fondamentali

L'inserimento di dati biometrici comporta tutta una serie di problemi di natura pratica che attendono ancora soluzione (ad esempio, le modalità di raccolta degli identificatori biometrici), e fin quando non saranno disponibili progetti più dettagliati sarà difficile individuare le garanzie ulteriori da prevedere; tuttavia, l'inserimento di dati biometrici richiederebbe quantomeno la definizione di un chiaro quadro giuridico, in cui si stabilisca con precisione in quali circostanze e per quali scopi sia consentito effettuare interrogazioni su dati biometrici. Si tratta di un elemento di particolare importanza, poiché l'inserimento di dati biometrici aumenta la probabilità di una deriva funzionale: vari soggetti, ed in particolare le autorità giudiziarie e di polizia, potrebbero sfruttare la prevista flessibilità del SIS II per chiedere l'accesso a dati biometrici in rapporto ad una molteplicità di scopi.

I rischi sarebbero ancora più consistenti se i dati biometrici fossero conservati nelle sezioni nazionali oltre che nella sezione centrale del SIS II, in quanto le autorità giudiziarie e di polizia dei singoli Stati avrebbero maggiori occasioni di utilizzare tali dati per finalità che esulano da quelle previste nella Convenzione di Schengen.

Per garantirsi contro una simile eventualità, si dovrebbe prevedere la registrazione degli accessi a queste nuove categorie di dati e l'effettuazione di verifiche periodiche del sistema onde assicurare che ai dati si acceda soltanto per scopi legittimi e da parte di soggetti autorizzati. Inoltre, nelle norme concernenti la conservazione di nuove tipologie di dati deve essere specificato con chiarezza che tali dati possono essere conservati esclusivamente per il periodo necessario a raggiungere uno scopo determinato.

4.3. Nuove funzionalità tecniche

Uno dei motivi alla base dello sviluppo del SIS II era la volontà di beneficiare delle nuove tecnologie introducendo nuove funzionalità. Si propone che il SIS II consenta la "interconnessione" delle segnalazioni presenti nel sistema al fine di migliorarne l'efficienza. L'ACC ha indicato che, prima di procedere in tal senso, è necessario prevedere il quadro giuridico di riferimento e, in un precedente parere, ha segnalato che l'interconnessione delle segnalazioni potrebbe permettere agli utenti di accedere ad informazioni per le quali non sono abilitati. Pertanto, l'ACC accoglie con favore l'affermazione contenuta nelle conclusioni del Consiglio, secondo cui è necessario prevedere garanzie atte ad assicurare che l'interconnessione di segnalazioni "non modifichi i diritti di accesso in essere rispetto alle singole categorie di segnalazioni".

Ciononostante, l'interconnessione di segnalazioni rappresenta un esempio di funzionalità in grado di modificare la natura del sistema, che da sistema di informazione diventerebbe un sistema di investigazione.

5. Controllo del SIS II

L'architettura proposta per il nuovo sistema solleva alcuni interrogativi in materia di controllo e monitoraggio. Se il sistema aumenta il proprio grado di centralizzazione, quale dovrà essere l'evoluzione dei meccanismi di controllo? Può darsi che l'ACC abbia bisogno di maggiori poteri per far fronte ad eventuali modifiche nell'architettura del sistema.

Nella Comunicazione della Commissione si afferma che le Parti contraenti sono libere di scegliere se mantenere un database nazionale, oppure prevedere soltanto un'interfaccia nazionale ed interrogare direttamente il sistema centrale. Quali potrebbero essere le implicazioni di una modifica del genere?

Attualmente, la Convenzione di Schengen conferisce alle autorità nazionali di protezione dei dati il potere di controllo sulla rispettiva sezione nazionale del sistema. Se le sezioni nazionali fossero sostituite da un'interfaccia, ciò avrebbe ripercussioni sul controllo nazionale e potrebbe rendersi necessario modificare in conseguenza i poteri conferiti alle autorità nazionali. Sorgerebbe, inoltre, l'esigenza di garantire che tutte le pertinenti autorità nazionali dispongano di risorse sufficienti per svolgere in modo efficace la propria funzione di controllo del sistema. In ogni caso, nel dibattito a venire sul controllo ed il monitoraggio del SIS II dovrebbero essere coinvolte le autorità nazionali di protezione dei dati nonché l'ACC ed il Garante europeo della protezione dei dati, da poco nominato.

6. Conclusioni

Anche ammettendo che non vi sia l'intento di modificare la natura del SIS, che è un sistema di controllo del tipo hit/no-hit, l'ACC ritiene che l'aggiunta di nuove funzionalità (come l'interconnessione di segnalazioni), l'inserimento di nuove categorie di dati, e la tendenza ad ampliare il novero dei soggetti autorizzati ad accedere al sistema possano dar luogo, congiuntamente alla prevista flessibilità del nuovo sistema, ad una modifica de facto della natura del sistema stesso, trasformando il SIS II in uno strumento di indagine.

Non si tratta di una novità assoluta, visto che nel 2001 la stessa Commissione ha affermato quanto segue:

"La Commissione desidera sottolineare l'importanza di progredire nella definizione delle funzionalità del SIS. In particolare, alcune delle proposte attualmente in discussione comporterebbero modifiche sostanziali delle finalità del SIS, trasformandolo da sistema di informazione in sistema di informazione e di indagine."(1)

Ci sono validi motivi per nutrire preoccupazioni rispetto a questo tipo di sviluppi. In primo luogo, esiste la possibilità che il SIS II, man mano che incorporerà nuove categorie di dati, duplichi sistemi di informazione già esistenti in ambito UE. In secondo luogo, è necessario aggiornare le norme sulla protezione dei dati per garantire che il nuovo sistema, con le sue mutate potenzialità, non incida sui diritti degli interessati – e queste norme saranno sempre un passo indietro se non si fisseranno limiti alle modalità di sviluppo del sistema. Inoltre, è essenziale che il SIS II si sviluppi in conformità con il principio di proporzionalità, ossia che le funzionalità e le categorie di dati presenti nel SIS II non eccedano quanto è necessario per raggiungere gli scopi del sistema. Tuttavia, prima occorre stabilire quali siano queste finalità, e successivamente si potrà procedere a tale verifica.

L'ACC ribadisce che non è possibile risolvere le questioni tecniche e giuridiche senza che vi sia prima una decisione politica sulle finalità prefigurate per il SIS II, e che sarebbe opportuno stabilire in modo particolareggiato quali siano le funzionalità e le categorie di dati delle quali il sistema dovrebbe disporre per raggiungere tale obiettivo.

Inoltre, non sembra che, al momento, vi siano iniziative in seno al Consiglio finalizzate

(1) Comunicazione della Commissione al Consiglio ed al Parlamento europeo: Sviluppo del Sistema di informazione Schengen II, 18 dicembre 2001.

55

alla definizione di un nuovo quadro giuridico per il SIS II e, per le motivazioni esposte in questo parere, l'ACC sollecita a dare corso quanto prima a queste iniziative. Le risultanze di una valutazione dell'impatto-privacy potrebbero rivelarsi utili nella formulazione di tale cornice giuridica e, attraverso una valutazione di questo tipo, si potrebbero prendere in considerazione le tematiche attinenti al controllo del sistema ed alla necessità di garanzie ulteriori, oltre ad esaminare eventuali proposte connesse quali la ventilata sinergia fra SIS II ed un nuovo Sistema di informazione visti.

Per parte sua, l'ACC è pronta a collaborare in ogni modo possibile. Inoltre, alla luce delle significative implicazioni per il SIS II legate alle proposte in oggetto, l'ACC ritiene auspicabile che ogni ulteriore sviluppo le sia comunicato con tempestività in modo da disporre del tempo necessario per formulare indicazioni che possano successivamente essere tenute presenti dagli attori del processo decisionale.

Bruxelles, 19 maggio 2004

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

(*) www.schengen-jsa.dataprotection.org/garante/document?ID=571347

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

(art. 29 direttiva 95/46/CE)

57

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

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10031/03/IT
WP 85

PARERE 1/2004 SUL LIVELLO DI PROTEZIONE GARANTITO IN AUSTRALIA PER LA TRASMISSIONE DEI DATI DELLE REGISTRAZIONI DEI NOMI DEI PASSEGGERI DA PARTE DELLE COMPAGNIE AEREE

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp85_it.pdf

Adottato il 16 gennaio 2004

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

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11816/03/FR
WP 86

DOCUMENTO DI LAVORO SULLE PIATTAFORME INFORMATICHE FIDATE, IN PARTICOLARE PER QUANTO RIGUARDA IL LAVORO EFFETTUATO DA TRUSTED COMPUTING GROUP (GRUPPO TCG)

Adottato il 23 gennaio 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp86_it.pdf

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

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10019/04/IT
WP 87

PARERE 2/2004 SUL LIVELLO DI PROTEZIONE ADEGUATO DEI DATI A CARATTERE PERSONALE CONTENUTI NELLE PRATICHE PASSEGGERI (PNR - PASSENGER NAME RECORDS) TRASFERITE ALL'UFFICIO DELLE DOGANE E DELLA PROTEZIONE DI FRONTIERA DEGLI STATI UNITI (BUREAU OF CUSTOMS AND BORDER PROTECTION - US CBP)

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_it.pdf

Adottato il 29 gennaio 2004

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

ARTICLE 29 Data Protection Working Party

10037/04/EN
WP 88

OPINION 3/2004 ON THE LEVEL OF PROTECTION ENSURED IN CANADA FOR THE TRANSMISSION OF PASSENGER NAME RECORDS AND ADVANCED PASSENGER INFORMATION FROM AIRLINES

Adopted on 11th February 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp88_en.pdf

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

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11750/02/IT
WP 89

PARERE 4/2004 RELATIVO AL TRATTAMENTO DEI DATI PERSONALI MEDIANTE VIDEOSORVEGLIANZA.

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp89_it.pdf

Adottato l'11 febbraio 2004

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

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11601/IT
WP 90

PARERE 5/2004 RELATIVO ALLE COMUNICAZIONI INDESIDERATE A FINI DI COMMERCIALIZZAZIONE DIRETTA AI SENSI DELL'ARTICOLO 13 DELLA DIRETTIVA 2002/58/CE.

Adottato il 27 febbraio 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_it.pdf

63 Documento di lavoro sui dati genetici (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

12178/03/IT
WP 91

DOCUMENTO DI LAVORO SUI DATI GENETICI

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp91_it.pdf

Adottato il 17 marzo 2004

64 Dichiarazione comune in risposta agli attentati terroristici di Madrid (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10649/04/IT
WP 93

DICHIARAZIONE COMUNE IN RISPOSTA AGLI ATTENTATI TERRORISTICI DI MADRID

Adottata il 17 marzo 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp93_it.pdf

65

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

ARTICLE 29 Data Protection Working Party

11221/04/EN
WP 95

OPINION 6/2004 ON THE IMPLEMENTATION OF THE COMMISSION DECISION OF 14-V-2004 ON THE ADEQUATE PROTECTION OF PERSONAL DATA CONTAINED IN THE PASSENGER NAME RECORDS OF AIR PASSENGERS TRANSFERRED TO THE UNITED STATES' BUREAU OF CUSTOMS AND BORDER PROTECTION, AND OF THE AGREEMENT BETWEEN THE EUROPEAN COMMUNITY AND THE UNITED STATES OF AMERICA ON THE PROCESSING AND TRANSFER OF PNR DATA BY AIR CARRIERS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY, BUREAU OF CUSTOMS AND BORDER PROTECTION

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp95_en.pdf

Adopted on 22nd June 2004

66

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

ARTICLE 29 Data Protection Working Party

11224/04/EN
WP 96

OPINION NO 7/2004 ON THE INCLUSION OF BIOMETRIC ELEMENTS IN RESIDENCE PERMITS AND VISAS TAKING ACCOUNT OF THE ESTABLISHMENT OF THE EUROPEAN INFORMATION SYSTEM ON VISAS (VIS)

Adopted on 11 August 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp96_en.pdf

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

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

*1173*30/04/IT*
WP 97

PARERE 8/2004 SULL'INFORMAZIONE DEI PASSEGGERI
IN MERITO AL TRASFERIMENTO DI SCHEDE NOMINATIVE DEI PASSEGGERI AEREI (PNR)
SUI VOLI TRA L'UNIONE EUROPEA E GLI STATI UNITI D'AMERICA

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp97_it.pdf

Adottato il 30 settembre 2004

68 Documento strategico (*)

ARTICLE 29 Data Protection Working Party

11648/04/EN
WP 98

STRATEGY DOCUMENT

Adopted on 29 September 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp98_en.pdf

69

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

ARTICLE 29 Data Protection Working Party

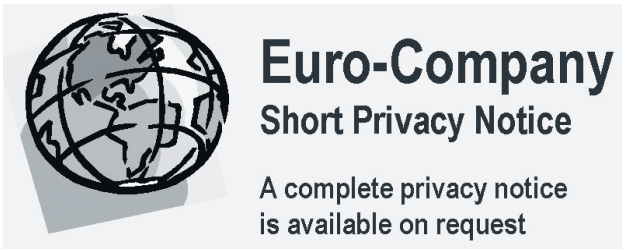
11885/04/EN
WP 99

OPINION 9/2004 ON A DRAFT FRAMEWORK DECISION ON THE STORAGE OF DATA PROCESSED AND RETAINED FOR THE PURPOSE OF PROVIDING ELECTRONIC PUBLIC COMMUNICATIONS SERVICES OR DATA AVAILABLE IN PUBLIC COMMUNICATIONS NETWORKS WITH A VIEW TO THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL ACTS, INCLUDING TERRORISM. [PROPOSAL PRESENTED BY FRANCE, IRELAND, SWEDEN AND GREAT BRITAIN (DOCUMENT OF THE COUNCIL 8958/04 OF 28 APRIL 2004)]

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_en.pdf

Adopted on 9th November 2004

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



Dated: October 2004

• We keep the personal information you give us to help provide you with the products and services you require

• We may also pass on your details to other companies who may contact you about their products. You can opt out of this byticking the box below

For the full privacy notice or for access or correction, contact:

• Privacy Department
Euro Company ******

•Call 00 ******

•Or go to the Privacy notice on our website at euro.com

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100appendix1_en.pdf

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

ARTICLE 29 Data Protection Working Party

12067/04/EN
WP 101

DECLARATION OF THE ARTICLE 29 WORKING PARTY ON ENFORCEMENT

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp101_en.pdf

Adopted on 25th November 2004

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

ARTICLE 29 Data Protection Working Party

12110/04/EN
WP 102

MODEL CHECKLIST
APPLICATION FOR APPROVAL OF BINDING CORPORATE RULES

Adopted on 25th November 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp102_en.pdf

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

INTRODUZIONE

I comitati del Consiglio d'Europa che si occupano di questioni attinenti la protezione dei dati desideravano richiamare l'attenzione su alcuni aspetti specifici della tutela dei dati personali in relazione all'impiego di "carte intelligenti" (smart cards). Il Gruppo di progetto sulla protezione dei dati (CJ-PD) del Consiglio d'Europa ha, pertanto, chiesto ad un consulente, il dr. Karel Neuwirt (Presidente dell'Autorità ceca per la protezione dei dati), di redigere una Relazione sulla protezione dei dati in rapporto all'impiego di smart cards. Nella Relazione si riconosceva che qualunque studio in materia sarebbe stato necessariamente connesso agli sviluppi tecnologici e, pertanto, avrebbe dovuto essere collocato nel rispettivo contesto storico. Si esprimeva dunque l'auspicio di redigere un elenco di principi-guida specifici dei quali tenere conto in riferimento all'impiego di smart cards.

Dopo avere esaminato la Relazione del dr. Neuwirt ed i principi-guida ad essi allegati, il CJ-PD ha accettato di rivedere e specificare meglio alcuni di essi ed ha predisposto il documento di seguito riportato.

Ai fini dei presenti principi-guida, per "smart card" si intende un vettore mobile di dati personali dotato di funzioni automatiche di elaborazione, il quale viene rilasciato ad un interessato ed è in grado di trattare dati personali secondo le finalità e le specifiche del soggetto che lo rilascia in rapporto ad un sistema informativo cui tale vettore è collegato. La carta può essere utilizzata, ad esempio, al fine di identificare l'interessato, di svolgere operazioni che non possono essere effettuate in forma anonima, o di consentire l'accesso a luoghi o database specifici. È necessario distinguere la *smart card* dalle carte a banda magnetica o di memorizzazione, le quali non possono essere utilizzate per effettuare autonome operazioni sui dati secondo criteri logici ed aritmetici.

Le *smart card* trovano impiego crescente per una vasta gamma di applicazioni. Le caratteristiche e le potenzialità delle smart card sollevano numerosi interrogativi in termini di protezione dati, ai quali è necessario fornire risposta. Ad esempio, chi ha la titolarità dei dati personali utilizzati dal sistema? Chi è responsabile dell'accuratezza e della sicurezza dei dati qualora il sistema sia accessibile ad una pluralità di soggetti diversi? Come evitare il moltiplicarsi dei rischi di possibili violazioni della privacy dei cittadini a causa dell'impiego di tecnologie legate alle smart card? Chi deve accedere ai dati personali dell'interessato, ed a quali condizioni? ecc.

I sistemi d'informazione che utilizzino smart card associate al trattamento di dati personali ricadono nell'ambito di applicazione della Convenzione del Consiglio d'Europa per la protezione delle persone con riguardo al trattamento automatizzato di dati personali [ETS 108] (nel prosieguo, "Convenzione 108"). Tale Convenzione è stata elaborata quando ci si è resi conto che, al fine di garantire un'efficace tutela giuridica dei dati personali, sarebbe stato necessario sviluppare in modo più specifico ed organico il riferimento generico al rispetto per la vita privata contenuto nell'Articolo 8 della Convenzione per la tutela dei diritti umani e delle libertà fondamentali (nel prosieguo, "CEDU").

Diritti e garanzie ulteriori sono previsti in varie Raccomandazioni del Consiglio d'Europa, fra cui in particolare:

(*) Adottati dal CDCJ [Gruppo di progetto sulla cooperazione giuridica] in occasione della sua 79ma riunione plenaria (11-14 maggio 2004).

a) la Raccomandazione N. R(2002)9 sulla protezione dei dati personali raccolti e trattati per scopi assicurativi,
b) la Raccomandazione N. R(99)14 sul servizio universale, relativa ai nuovi servizi di comunicazione ed informazione,
c) la Raccomandazione N. R(99)5, per la tutela della privacy su Internet,
d) la Raccomandazione N. R(97)5, sulla protezione dei dati sanitari,
e) la Raccomandazione N. R(95)4, sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici,
f) la Raccomandazione N. R(90)19, sulla protezione dei dati personali utilizzati per operazioni di pagamento e per altre operazioni connesse,
g) la Raccomandazione N. R(89)2, sulla protezione dei dati personali utilizzati nel rapporto di lavoro,
h) la Raccomandazione N. R(86)1, sulla protezione dei dati personali utilizzati per scopi di previdenza sociale,
i) la Raccomandazione N. R(85)20, sulla protezione dei dati personali utilizzati per scopi di marketing diretto.

Numerosi sono i documenti e le attività del Consiglio d'Europa, in particolare attraverso i gruppi di esperti che si occupano di protezione dei dati personali, connessi indirettamente alle questioni sollevate dall'utilizzazione di smart card. In particolare, poiché le smart card possono essere utilizzate per la memorizzazione di dati biometrici, si richiama l'attenzione sui principi-guida relativi alla protezione dei dati personali sotto forma di dati biometrici attualmente in via di definizione da parte del T-PD. Le tecnologie moderne arrecano molteplici vantaggi alla vita quotidiana dei cittadini, ma comportano anche alcuni rischi legati alla possibilità di ingerenze nella privacy delle persone. Pertanto, il presente documento non si propone di descrivere i vantaggi dell'utilizzazione di smart card, bensì di specificare l'approccio da seguire per migliorare la tutela dei dati personali qualora si utilizzino tecnologie connesse alle smart card.

La raccolta ed il trattamento di dati personali in sistemi che utilizzino smart card devono rispettare tutti i principi fissati dalla normativa nazionale in materia di protezione dei dati personali.

I principi-guida che seguono non intendono fornire una risposta esauriente a tutti gli interrogativi concernenti la protezione dei dati che nascono dall'utilizzazione di smart card. Una smart card viene sempre utilizzata nell'ambito di un sistema d'informazione più ampio, e l'effettività della protezione complessiva dei dati personali utilizzati in un sistema del genere dipende da fattori e circostanze numerosi e di natura diversa. Anche la sicurezza del sistema dipende in larga parte dal comportamento di coloro che vi hanno a che fare. La tecnologia legata alle smart card sta attraversando una fase di rapidissimo sviluppo. I principi-guida in questione vogliono fissare alcuni principi fondamentali che non subiranno modifiche significative in rapporto alle innovazioni introdotte in campo tecnologico. Cionondimeno, può essere opportuno integrare tali principi alla luce degli incessanti sviluppi in questo settore.

È necessario ricordare che, nella misura in cui i presenti principi-guida contengano garanzie per i diritti e le libertà fondamentali di ognuno, ed in particolare per il diritto al rispetto della vita privata, sanciti negli Articoli 5, 6 ed 8 della Convenzione 108 e nell'Articolo 8 della CEDU, è possibile derogare a tali diritti, ai sensi dell'Articolo 9 della Convenzione 108, elaborato sulla base dell'Articolo 8 della CEDU, se ciò è previsto da norme di legge e costituisce una misura necessaria in una società democratica nell'interesse
a. della tutela della sicurezza dello Stato, della sicurezza pubblica, degli interessi economici dello Stato, o della repressione dei reati;
b. della tutela dell'interessato o dei diritti e delle libertà altrui.

Per quanto concerne tali deroghe, è opportuno sottolineare che esse vanno interpretate in maniera restrittiva e devono essere applicate solo in casi eccezionali, secondo le indicazioni fornite dalla giurisprudenza della Corte europea dei diritti umani relativa al comma 2 dell'Articolo 8 della CEDU.

I principi-guida sono rivolti precipuamente ai soggetti che rilasciano la carta, i quali hanno la responsabilità primaria della protezione dei dati personali in essa contenuti. I prin-

cipi si rivolgono, inoltre, a tutti gli altri soggetti che partecipano ai sistemi d'informazione: progettisti, gestori, operatori, e gli stessi interessati. Tutti i soggetti in questione dovrebbero tenere presenti i principi enunciati nel prosieguo. I principi elaborati dovrebbero essere applicati con la massima coerenza possibile; solo in tal modo sarà possibile contribuire alla diffusione di applicazioni basate su smart card che consentano la massima interoperabilità a livello internazionale e gli standard più elevati di sicurezza.

PRINCIPI GUIDA

1. La raccolta ed il trattamento di dati personali attraverso smart card devono avvenire in modo lecito e leale. Si deve prevedere di raccogliere e memorizzare sulla carta soltanto i dati personali necessari a raggiungere gli scopi per i quali la carta stessa è utilizzata. I sistemi che utilizzano smart card devono essere trasparenti[1] per gli interessati i cui dati personali siano oggetto di trattamento.

2. I dati personali devono essere raccolti e memorizzati su una smart card soltanto per scopi legittimi, specifici ed espliciti. Non devono essere utilizzati successivamente secondo modalità che siano incompatibili con tali scopi.

3. Gli obblighi attinenti la protezione dei dati personali pertengono al soggetto che determina gli scopi del sistema e gli strumenti utilizzati per raggiungere tali scopi. Ciò comporta, nel caso di carte multifunzionali, che titolari diversi siano responsabili ciascuno per la parte che gli compete.

4. Qualora una smart card sia utilizzata per scopi di tipo diverso, il trattamento deve essere organizzato in modo da non utilizzare i dati per scopi diversi da quelli per cui sono stati raccolti. Qualora gli stessi dati siano utilizzati per scopi di tipo diverso, essi devono limitarsi a quelli strettamente necessari.[2]

5. La raccolta di dati personali sensibili[3] da registrare nella memoria della carta deve essere effettuata soltanto se prevista da norme di legge oppure se l'interessato vi ha acconsentito esplicitamente.[4] Tali dati devono essere trattati soltanto nel rispetto di opportune garanzie previste per legge.[5] Qualora la raccolta ed il trattamento dei dati in questione si fondino sul consenso esplicito, l'interessato deve avere il diritto di ritirare tale consenso in qualsiasi momento. Il rifiuto o il ritiro del consenso non devono comportare conseguenze negative per l'interessato.[6]

6. I dati registrati su una smart card devono essere tutelati da accessi, alterazioni e/o cancellazioni non autorizzati o accidentali. La carta deve assicurare un livello adeguato di sicurezza alla luce delle conoscenze tecnologiche, della natura sensibile o non sensibile dei dati registrati, del numero e della tipologia delle applicazioni, e della valutazione dei possibili rischi.[7] È necessario stabilire in anticipo, relativamente a ciascuno dei diversi scopi per i quali la carta viene utilizzata, a quali condizioni sia consentito a soggetti terzi di accedere ai dati registrati sulla carta stessa.[8]

7. Qualora si raccolgano e memorizzino dati personali su una smart card, l'interessato deve essere informato delle finalità del trattamento, dell'identità del titolare, delle categorie di dati in oggetto e dei destinatari, o delle categorie di destinatari, dei dati memorizzati. L'interessato deve ricevere ulteriori informazioni[9] se ciò è necessario per garantire la lealtà del trattamento di dati personali.

8. All'atto del rilascio della carta, il titolare deve essere informato adeguatamente delle modalità di utilizzazione e dei passi da compiere in caso di frode o comunicazione non autorizzata.[10]

9. Ogniqualvolta si realizzi uno scambio di dati personali fra una smart card ed il sistema, l'interessato deve esserne informato, a meno che sia già in possesso di tale informazione. Ciò riveste particolare importanza con riguardo alle carte contactless, ossia qualora l'interessato non debba provvedere direttamente all'inserimento o alla presentazione della carta al sistema.

(1) Il concetto di trasparenza implica che l'interessato sia informato dei dati memorizzati e della loro utilizzazione.
(2) Ad esempio, nel caso di una smart card utilizzata da un'istituzione scolastica sia per i servizi di mensa sia per quelli di biblioteca, devono essere memorizzati soltanto i dati comuni alle due funzionalità, come il nome dell'alunno e la rispettiva classe di appartenenza.
(3) Ai sensi dell'Articolo 6 della Convenzione 108, per dati sensibili si intendono "i dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale [...] [e] i dati a carattere personale relativi a condanne penali". Si considerano dati sensibili anche gli altri dati definiti come tali dal diritto nazionale.
(4) Tuttavia, in taluni casi il diritto nazionale può prevedere che il consenso non è sufficiente a conferire liceità alla raccolta e/o al trattamento dei dati.
(5) Tali opportune garanzie atte a tutelare ulteriormente i dati possono trovare applicazione, ad esempio, attraverso la cifratura dei dati stessi, che attualmente rappresenta l'approccio più sofisticato. Tuttavia, è necessario tenere conto dei possibili sviluppi futuri in campo tecnologico.
(6) Se la memorizzazione di dati sensibili è necessaria per fornire un servizio all'interessato, e quest'ultimo rifiuta il proprio consenso esplicito ovvero ritira tale consenso, non sarà ovviamente più

segue nota 6, 7, 8, 9, 10

10. Gli interessati devono avere il diritto di accedere ai dati personali che li riguardano contenuti nella carta, e devono avere il diritto di farli correggere o, se necessario, aggiornare.[11]

11. I dati derivanti dall'utilizzazione di una smart card[12] devono essere cancellati se non sono più necessari per lo scopo specifico in relazione al quale la carta è stata utilizzata.

segue nota 6
possibile continuare la prestazione del servizio a favore dell'interessato.
(7) Ad esempio, se si utilizzano carte con un chip di memoria, è ammessa, in linea di principio, soltanto la registrazione di dati identificativi. Vi possono essere anche altri criteri da tenere presenti, come la quantità dei dati, il numero di potenziali lettori, le finalità del trattamento, ecc.
(8) Il rischio di utilizzazioni improprie dei dati registrati nella carta aumenta se quest'ultima è dotata di funzioni di pagamento. Si sconsiglia l'associazione fra funzioni di pagamento ed applicazioni che comportino la registrazione sulla carta di dati sensibili relativi al titolare della carta stessa.
(9) Le informazioni da fornire all'interessato possono comprendere anche le specifiche tecniche relative al sistema utilizzato.
(10) In particolare, è necessario richiamare l'attenzione del titolare della carta sulle possibili conseguenze in caso di utilizzazione impropria, comunicazione delle modalità di accesso ai dati (ad esempio, il codice) o comunicazione dei dati, nonché sulla circostanza che, in taluni casi, egli può essere chiamato a rispondere personalmente.
(11) Una possibilità per garantire l'accesso consiste nell'installazione di lettori di smart card.
(12) Ad esempio, le informazioni relative alla data ed al luogo di utilizzazione della carta.

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

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

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

Il Trattato dell'Unione Europea (TUE), nella versione adottata il 2 ottobre 1997 (Trattato di Amsterdam) contiene, nel Titolo VI, ampie disposizioni relative alla cooperazione giudiziaria e di polizia in materia penale. Il Trattato di Nizza prevede che le autorità giudiziarie e di polizia degli Stati membri dell'UE intensifichino ulteriormente tale cooperazione. Si tratta di una delle priorità dell'Unione.

Le Autorità di protezione dei dati degli Stati Membri dell'Unione europea hanno piena coscienza della necessità di una cooperazione più stretta fra le autorità responsabili dell'azione penale negli Stati Membri, al fine di garantire ai cittadini dell'Unione un livello elevato di sicurezza in un'area di libertà, sicurezza e giustizia. Tuttavia, occorre garantire un equo bilanciamento fra tale esigenza e la difesa delle libertà civili, compresi i diritti di protezione dei dati, la cui tutela è sancita dalla Carta dei diritti fondamentali dell'Unione europea.

Uno dei compiti più importanti delle Autorità di protezione dei dati è rappresentato dall'attività consultiva in materia di protezione dei dati svolta per gli enti che si occupano di legiferazione; in tale ambito, le Autorità devono sottolineare i rischi che determinate iniziative di legge possono comportare per le libertà sopra ricordate, e proporre soluzioni più vicine ai cittadini. La Commissione, il Consiglio ed il Parlamento europeo usufruiscono di tale attività consultiva con sempre maggiore frequenza.

Naturalmente le Autorità di protezione dei dati sono liete di rispondere a tali richieste nella maniera migliore possibile. Tuttavia, è bene chiarire che, al momento, sono insuffi-

cienti o assenti le strutture organizzative necessarie all'adempimento di questa importante missione, e che pertanto le Autorità non possono garantire un intervento consultivo in fase precoce, sulla base di un'analisi condotta a livello paneuropeo e secondo i dovuti standard di qualità. Ciò dipende dall'inesistenza, all'interno del Terzo Pilastro, di un forum comune e della necessaria struttura organizzativa.

Questa situazione contrasta con quella rinvenibile nel Primo Pilastro, dove è stato costituito il Gruppo di lavoro "Articolo 29" che garantisce un'idonea struttura organizzativa alle Autorità di protezione dei dati. Tale struttura comprende un segretariato permanente (messo a disposizione dalla Commissione) e le risorse utili a consentire l'organizzazione di incontri periodici a Bruxelles con i necessari servizi di traduzione. Le autorità di controllo comuni all'interno del Terzo Pilastro (ad esempio per quanto riguarda Europol, Schengen, Eurojust) hanno un mandato specifico, ed occorre un approccio più ampio per garantire l'uniformità delle garanzie concernenti la protezione dei dati nell'intero settore della cooperazione giudiziaria e di polizia.

I partecipanti alla Conferenza attualmente stanno intensificando la propria collaborazione nelle materie giudiziarie e di polizia. A tal fine, un gruppo di lavoro "Polizia", costituito sotto l'egida della Conferenza delle Autorità europee di protezione dei dati, funge da forum strategico, analizzando tematiche che esulano dal mandato degli organismi attualmente esistenti a livello UE in materia di protezione dei dati. È stato inoltre costituito un altro sottogruppo della Conferenza. Tale gruppo di progetto, formato, fra gli altri, dai presidenti delle autorità comuni di controllo (Europol, Schengen, Dogane ed Eurojust), dal presidente del Gruppo di lavoro "Articolo 29", e dal Garante europeo per la protezione dei dati, ha il compito di sviluppare approcci strategici rispetto a nuove iniziative che riguardino l'utilizzazione di dati personali per scopi giudiziari e di polizia in una prospettiva europea.

Cionondimeno, sono necessarie ulteriori misure strutturali. In concomitanza con il rafforzamento e l'avanzamento dell'architettura europea di sicurezza nel Terzo Pilastro, è essenziale incorporare l'attività consultiva in materia di protezione dei dati nella struttura del Consiglio dell'Unione europea. Per tale motivo, la Conferenza delle Autorità europee di protezione dei dati invita il Consiglio e la Commissione ad attuare senza indugi le misure necessarie, in termini di risorse umane ed organizzative, onde consentire all'ente incaricato della protezione dei dati di iniziare l'importante attività di tutela degli interessi dei cittadini prima della fine dell'anno in corso. Il Garante europeo per la protezione dei dati, nominato ai sensi dell'Articolo 286(2) del Trattato delle Comunità europee, dovrebbe partecipare all'ente istituendo con un ruolo attivo.

La Conferenza, inoltre, invita il Consiglio e la Commissione a creare i presupposti giuridici per l'armonizzazione delle attività di controllo nell'ambito del Terzo Pilastro, in stretta cooperazione con i soggetti competenti.

La Presidenza è invitata a trasmettere la presente Risoluzione al Consiglio, alla Commissione ed al Parlamento.

Wroclaw, 14 settembre 2004

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

Sulla base di una proposta formulata dall'Autorità di Berlino per la protezione dei dati e l'accesso alle informazioni, l'Autorità per la protezione dei dati e l'accesso alle informazioni dello Stato di Brandeburgo, l'Autorità belga per la protezione dei dati, l'Information Commissioner del Regno Unito, l'Autorità federale tedesca per la protezione dei dati, il Centro indipendente per la protezione dei dati dello Schleswig-Holstein, l'Autorità per le informazioni e la *privacy* dello Stato di Ontario, l'Ispettore generale per la protezione dei dati personali della Polonia, l'Autorità per la protezione dei dati personali di Hong Kong, l'Autorità spagnola per la protezione dei dati, l'Ispettorato statale per la protezione dei dati della Repubblica di Lituania, e l'Autorità svizzera per la protezione dei dati propongono che la Conferenza internazionale adotti la seguente risoluzione:

Considerato che l'Organizzazione internazionale per la standardizzazione (ISO) ha istituito un Gruppo di studio sulle tecnologie della *privacy* (PTSG) nell'ambito del Comitato tecnico congiunto 1 (JTC1) con il compito di valutare la necessità di mettere a punto uno standard tecnologico in materia di *privacy* e, in caso affermativo, le modalità procedurali e la relativa portata, e quindi presentare una relazione entro il mese di novembre 2004;

Considerato che il Comitato tecnico congiunto 1 (JTC1) dell'ISO trasmette al Sottocomitato 27 (Sicurezza nelle tecnologie dell'informazione) le richieste di decisione su schemi attinenti alla *privacy* secondo una procedura accelerata;

Considerato che l'International Security, Trust, and Privacy Alliance (ISTPA, Alleanza internazionale per la sicurezza, la fiducia e la *privacy*) è un'alleanza mondiale di imprese, istituzioni e fornitori di tecnologie operanti congiuntamente allo scopo di chiarire e definire questioni attuali o in via di evoluzione connesse a sicurezza, fiducia e *privacy*;

Considerato che l'ISO ha ricevuto una proposta di standard internazionale (ISO/IEC (PAS) DIS 20886) relativa ad Quadro di riferimento per la *privacy*, presentata dall'ISTPA[1] nell'ambito di una procedura accelerata, sulla quale è aperto il voto per corrispondenza con scadenza all'11 dicembre 2004;

Considerato che il Privacy Enhancing Technology Testing and Evaluation Project (PETTEP[2], Progetto per la verifica e valutazione delle tecnologie di potenziamento della *privacy*) è una coalizione mondiale di autorità per la *privacy* e la protezione dei dati, esponenti del mondo universitario, autorità governative e organismi del settore privato, ed esperti in materia di *privacy*, la cui missione consiste nella definizione di criteri di verifica e valutazione riconosciuti a livello internazionale rispetto alle caratteristiche dichiarate da sistemi e tecnologie dell'informazione relativamente alla *privacy*;

Considerato che l'International Working Group on Data Protection in Telecommunications (Gruppo di lavoro internazionale sulla protezione dei dati nelle telecomunicazioni), in occasione del suo 35mo incontro tenutosi a Buenos Aires il 14 e 15 aprile 2004, ha adottato un Documento di lavoro su un futuro standard ISO in materia di *privacy*;[3]

Considerato che la Conferenza internazionale delle Autorità di protezione dati e della *privacy* (in appresso, la "Conferenza") desidera sostenere la definizione di uno standard internazionale delle tecnologie in materia di *privacy* efficace e riconosciuto su base globale, e mettere a disposizione dell'ISO le proprie competenze ai fini della definizione di tale standard;

Considerato che la Conferenza riconosce che la conformità a standard ISO attuali o futuri non comporta né surroga necessariamente la conformità a disposizioni di legge. La

(1) V. http://www.istpa.org
(2) Il PETTEP è un progetto condotto sotto la guida dell'Autorità per la privacy e le informazioni dello stato di Ontario, che ha svolto ricerche ed analisi finalizzate alla definizione di criteri di verifica e valutazione degli aspetti connessi alla privacy nei sistemi e nelle tecnologie dell'informazione.
(3) www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm

Conferenza in realtà considera la definizione degli standard IT in oggetto uno strumento che può essere d'ausilio onde rispettare le norme di legge in materia di protezione dati e *privacy*. La Conferenza riconosce senza alcun dubbio che, da un lato, i propri membri, ciascuno per il rispettivo ambito di giurisdizione, hanno e continueranno a mantenere in vigore norme di legge in materia di *privacy*, le quali in realtà si differenziano per alcuni profili, e che, d'altro canto, esiste complessivamente un grado elevato di concordanza fra le norme di legge in questione, il quale troverebbe il riconoscimento ottimale divenendo parte integrante di meccanismi basati sulle tecnologie dell'informazione attraverso la messa a punto di uno standard internazionale, o di più standard internazionali;

La conferenza adotta le seguenti Risoluzioni:

1. La Conferenza raccomanda rispettosamente che l'ISO metta a punto uno o più standard globali in materia di *privacy*, ed in particolare uno standard delle tecnologie in materia di *privacy*, tale da supportare l'attuazione di norme di legge in materia di *privacy* e protezione dei dati, se già esistenti, e la formulazione di tali norme ove esse non siano ancora definite.
2. La Conferenza ritiene che la definizione di uno standard internazionale in materia di *privacy* debba fondarsi sulle prassi di leale informazione e sui principi di parsimonia, necessità ed anonimizzazione nell'uso dei dati. Per essere efficace, uno standard relativo alle tecnologie dell'informazione deve
    - offrire criteri di valutazione e verifica riferiti alle funzionalità connesse alla *privacy* di qualsiasi sistema o tecnologia, onde facilitare il rispetto da parte dei titolari degli strumenti giuridici nazionali e internazionali in materia di protezione dei dati,
    - offrire assicurazioni sulle caratteristiche dichiarate di rispetto della *privacy* relativamente a tecnologie e sistemi utilizzati per la gestione di dati personali,
    - essere in grado di supportare le specifiche concernenti la *privacy* riferite ai dati personali relativi a una determinata persona, indipendentemente dalle combinazioni e dal numero di soggetti che possono intervenire nella gestione e nell'interscambio di tali dati personali.
3. La Conferenza appoggia la recente istituzione di un Gruppo di studio temporaneo sulle tecnologie della *privacy* (PTSG) con il compito di valutare l'esigenza di uno standard nonché gli ambiti e le metodologie di sviluppo di tale standard nel quadro dell'ISO.
4. La Conferenza sostiene con forza l'accelerazione, e non già il procrastinamento, dell'istituzione di un nuovo Sottocomitato permanente dell'ISO per la definizione di standard delle tecnologie dell'informazione riferiti alla *privacy*. Tale nuovo Sottocomitato dovrebbe tenere presente l'attività svolta attualmente nei Sottocomitati esistenti in rapporto a specifici temi connessi alla *privacy*.
5. La Conferenza sostiene con forza l'inserimento del *Privacy Enhancing Technology* Testing and Evaluation Project (PETTEP) quale organismo ufficiale di collegamento con il PTSG del JTC1 dell'ISO. In tal modo le Autorità di protezione dati potranno disporre di uno strumento per operare direttamente all'interno del PTSG dell'ISO, e si conferisce ai membri del PETTEP un ruolo ufficiale che consentirà loro di presentare, analizzare e contribuire all'attività del PTSG.
6. La Conferenza promuove e sostiene l'adesione al PETTEP delle Autorità di protezione dati interessate, il che consentirà loro, in quanto membri del PETTEP, di far sentire immediatamente la propria voce nel dibattito relativo alla definizione di uno standard ISO delle tecnologie della *privacy*.
7. La Conferenza riconosce che il PETTEP gode già di uno status ufficiale all'interno del PTSG, e chiede rispettosamente al PETTEP di adottare le risoluzioni della Conferenza e di presentarle quanto prima al PTSG.
8. La Conferenza, pur riconoscendo l'impegno e la determinazione dell'ISTPA nel settore della *privacy*, chiede rispettosamente il ritiro dello schema ISTPA quale specifica pubblica (PAS) fintanto che non siano state affrontate le questioni di seguito delineate:
    - Il concetto di *privacy* su cui si fonda la Proposta di standard-quadro in materia di *privacy*, ed il fatto che tale quadro deve tenere conto dell'esistenza di limiti alla raccolta di dati. Nella Proposta si definisce *privacy* "la

gestione ed utilizzazione corrette di dati personali per l'intero ciclo di vita di tali dati, conformemente a principi di protezione dati ed alle preferenze espresse dal soggetto".[4] Gli Autori della Proposta giudicano che la raccolta ed il trattamento di dati personali siano fondamentali ai fini del funzionamento corretto della società e delle relazioni commerciali moderne.[5] Tale considerazione si fonda sul presupposto che non ci siano limiti alla raccolta di dati personali. Possono sussistere circostanze in cui la raccolta ed il trattamento di dati personali sono fondamentali nel senso indicato; tuttavia, non si deve supporre che ciò costituisca la regola.

9. La Conferenza chiede rispettosamente all'ISO di sospendere eventuali richieste già avanzate per il riconoscimento di specifiche pubbliche tramite procedura accelerata di adozione nel settore della *privacy* e della protezione dei dati (ovvero di sospendere la presentazione di nuove richieste per il riconoscimento di specifiche pubbliche nel settore della *privacy* e della protezione dei dati), in quanto la definizione di uno standard in materia di *privacy* necessita di un approfondito dibattito.
10. La Conferenza chiede rispettosamente all'ISO di considerare le richieste di riconoscimento di specifiche pubbliche ed ogni altra richiesta concernente la protezione dei dati e la *privacy* come indicazioni e contributi utili alla definizione di un quadro generale nonché di potenziali standard futuri all'interno del quadro suddetto.

(4) Ibid., pag. 13.
(5) Ibid., pag. 10.

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

L'ufficio dell'Autorità australiana federale per la *privacy*, l'Autorità per l'informazione e la *privacy* dello stato di Ontario, l'Autorità per i dati personali di Hong Kong, e l'Autorità per la protezione dei dati e l'accesso alle informazioni dello stato di Brandeburgo propongono che la Conferenza Internazionale adotti la seguente risoluzione:

1. La Conferenza rileva con preoccupazione che le case produttrici di software in tutto il mondo fanno sempre più ricorso a meccanismi non trasparenti per trasferire aggiornamenti di software nel computer degli utenti.

Così facendo, esse
- sono in grado di leggere e raccogliere dati personali memorizzati nel computer dei singoli utenti (ad esempio, le impostazioni dei programmi di navigazione, e informazioni sulle abitudini di navigazione del singolo utente) senza che questi abbiano la possibilità di accorgersene, intervenire o impedirlo,
- possono assumere il controllo, almeno parziale, del *computer* terminale e, quindi, limitare la capacità dell'utente di far fronte agli obblighi ed alle responsabilità previsti dalla legge nei suoi riguardi, in quanto titolare del trattamento, al fine di garantire la sicurezza dei dati personali eventualmente oggetto di trattamento,
- modificano il *software* installato sul *computer*, che sarà quindi utilizzato senza essere collaudato o approvato nei modi previsti, e
- possono provocare malfunzionamenti del computer senza che sia possibile individuarne la causa nell'aggiornamento.

Tutto ciò può comportare particolari problemi per la pubblica amministrazione e le aziende private, nella misura in cui sussistano specifici obblighi di legge a loro carico relativamente alle modalità di trattamento dei dati personali.

2. La Conferenza, pertanto, invita le società produttrici di *software*
a. ad offrire procedure per l'aggiornamento online del *software* soltanto in associazione ad un'informativa, e ad effettuare l'aggiornamento una volta ottenuto il consenso dell'utente, senza travalicare o abusare di tale consenso, secondo modalità trasparenti e senza consentire accessi non controllati al computer dell'utente;
b. a chiedere la comunicazione di dati personali soltanto con il consenso informato dell'utente e nella misura in cui ciò risulti necessario per effettuare l'aggiornamento online. Gli utenti non dovrebbero essere obbligati a fornire le proprie credenziali di identificazione –anziché di autenticazione– per dare inizio alla procedura di caricamento remoto;
c. a prevedere servizi di aggiornamento che consentano di effettuare verifiche preventive su server separati prima di procedere all'installazione.

3. La Conferenza promuove la definizione e l'applicazione di tecnologie per l'aggiornamento del software che siano rispettose della *privacy* e dell'autonomia degli utenti.

Progetto grafico:
Vertigo Design