GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo e del Consiglio recante modifica dell'istruzione consolare comune diretta alle rappresentanze diplomatiche e consolari di prima categoria in relazione all'introduzione di elementi biometrici e comprendente norme sull'organizzazione del ricevimento e del trattamento delle domande di visto (COM (2006) 269 defin.) — 2006/0088 (COD)

(2006/C 321/14)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, e in particolare l'articolo 286,

vista la Carta dei diritti fondamentali dell'Unione europea, e in particolare l'articolo 8,

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,

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, e in particolare l'articolo 41,

vista la richiesta di parere in conformità dell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001 ricevuta il 19 giugno 2006 dalla Commissione;

HA ADOTTATO IL SEGUENTE PARERE:

1. **INTRODUZIONE**

Il regolamento proposto ha due principali obiettivi, entrambi in vista dell'attuazione del Sistema d'informazione visti:

— fornire una base giuridica affinché gli Stati membri rilevino identificatori biometrici obbligatori dai richiedenti visto;

— fornire un quadro giuridico per l'organizzazione degli uffici consolari degli Stati membri, soprattutto organizzando un'eventuale cooperazione fra Stati membri per il trattamento delle domande di visto.

Questi due obiettivi sollevano diverse questioni in termini di protezione dei dati. Esse verranno affrontati in paragrafi distinti, anche se fanno parte della stessa proposta.

La presente proposta ha lo scopo di modificare le istruzioni consolari comuni (ICC). Queste sono state adottate dal comitato esecutivo istituito dalla convenzione che applica l'accordo di Schengen del 14 giugno 1985. Quale parte dell'accordo di Schengen, esse sono state recepite nella legislazione comunitaria da un protocollo allegato al trattato di Amsterdam e da allora sono state modificate in varie occasioni. Sebbene una serie di modifiche resti riservata, le ICC sono state pubblicate nel 2000. Quanto al contenuto, si tratta essenzialmente di un manuale contenente regole pratiche su come rilasciare visti per soggiorni di breve durata. Esse contengono disposizioni sull'esame delle domande, sulla procedura decisionale, su come compilare le vignette visto, ecc.

2. RACCOLTA DI IDENTIFICATORI BIOMETRICI

2.1. Osservazioni preliminari: specificità dei dati biometrici

Secondo la proposta sul sistema di informazione visti (VIS) ([1]) presentato dalla Commissione il 28 dicembre 2004, gli Stati membri introducono identificatori biometrici come le impronte digitali e le fotografie nel VIS per scopi di verifica (o) identificazione. L'attuale proposta di regolamento del Parlamento europeo e del Consiglio che modifica le ICC ha lo scopo di fornire una base giuridica per la raccolta di identificatori biometrici.

Sulla proposta VIS, il GEPD ha espresso un parere il 23 marzo 2005 ([2]). In esso si sottolinea l'importanza di applicare al trattamento di dati biometrici tutte le necessarie salvaguardie, considerate le loro caratteristiche specifiche: ([3])

> *«L'utilizzazione della biometria nei sistemi d'informazione non è mai una scelta irrilevante, specie allorché il sistema in questione riguarda un numero così elevato di persone. La biometria (…) modifica in maniera irrevocabile la relazione tra corpo e identità, in quanto le caratteristiche del corpo umano possono essere» lette «da una macchina e sottoposte a un successivo trattamento. Le caratteristiche biometriche, benché non possano essere lette dall'occhio umano, sono leggibili e utilizzabili mediante strumenti appropriati, in qualsiasi circostanza e ovunque si rechi la persona in questione.»*

Secondo il GEPD, la natura delicata dei dati biometrici esige che l'introduzione di obblighi per la loro utilizzazione intervenga soltanto dopo un'approfondita valutazione dei rischi e che si segua una procedura che consenta un totale controllo democratico. Queste osservazioni sono alla base dell'esame della presente proposta da parte del GEPD.

2.2. Contesto della proposta

Il contesto in cui viene elaborata questa proposta la rende ancor più delicata. Il regolamento proposto non può essere visto a prescindere dallo sviluppo di altri sistemi informatici su larga scala e dalla tendenza generale verso una maggiore interoperabilità fra sistemi informativi. Questo aspetto è menzionato nella comunicazione della Commissione del 24 novembre 2005, concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni ([4]).

Di conseguenza, una decisione presa in un determinato contesto e in vista di un determinato scopo ha maggiore probabilità di influire sullo sviluppo e sull'utilizzazione di altri sistemi creati per altri scopi. In particolare, i dati biometrici — compresi probabilmente i dati raccolti per l'attuazione della politica dei visti — una volta disponibili, potrebbero essere utilizzati in contesti diversi. Ciò potrebbe riguardare non soltanto il quadro del SIS, ma molto probabilmente anche Europol e FRONTEX.

2.3. Obbligo di fornire impronte digitali

Nel memorandum esplicativo dell'attuale proposta si afferma che: «Poiché il rilevamento degli identificatori biometrici farà ormai parte della procedura di rilascio del visto, occorre modificare l'istruzione consolare comune per creare una base giuridica adatta a questa misura.»

Il GEPD solleva obiezioni quanto alla scelta del legislatore di includere disposizioni relative all'esenzione o meno di taluni individui o gruppi di individui dall'obbligo di fornire impronte digitali nelle ICC anziché nel regolamento VIP stesso. In primo luogo, queste disposizioni hanno un impatto significativo sulla privatezza di un gran numero di individui e dovrebbero essere affrontate nel contesto della legislazione di base piuttosto che in istruzioni aventi un carattere ampiamente tecnico. In secondo luogo, per la chiarezza del regime giuridico sarebbe preferibile affrontare questo aspetto nel medesimo testo che istituisce il sistema informativo stesso.

([1]) Proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM(2004) 835 definitivo), presentato dalla Commissione il 28 dicembre 2004.

([2]) Parere del 23 marzo 2005 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata, GU C 181 del 23.7.2005, pag. 13.

([3]) *«[i dati biometrici]* offrono una *distinguibilità quasi assoluta*, ossia ciascuna persona possiede caratteristiche biometriche uniche. Esse si mantengono quasi inalterate nel corso della vita di una persona e ciò conferisce loro un carattere di *permanenza*. Tutti hanno gli stessi» elementi «fisici, il che fornisce alla biometria anche una dimensione di *universalità.*», ibid.

([4]) COM(2005) 597 definitivo.

(a) Innanzitutto, creare una base giuridica per la registrazione obbligatoria di impronte digitali e adottare identificatori biometrici è ben più che un tecnicismo; ha un significativo impatto sulla privatezza degli individui interessati. In particolare la scelta dell'età minima e/o massima per la registrazione di impronte digitali è una decisione politica e non soltanto tecnica. Di conseguenza, il GEPD raccomanda di affrontare questa materia, soprattutto per gli aspetti che non sono puramente tecnici, nel testo di base (proposta VIS) anziché in un manuale di istruzioni sugli aspetti prevalentemente tecnici della procedura dei visti ([1]).

A questo riguardo è anche utile ricordare le esigenze della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e la sua giurisprudenza. Secondo il suo articolo 8, paragrafo 2, qualsiasi ingerenza da parte di un'autorità pubblica nell'esercizio del diritto di privatezza è permessa unicamente qualora «sia prevista dalla legge» e «necessaria in una società democratica» per la protezione di interessi importanti. Nella giurisprudenza della Corte europea dei diritti dell'uomo, queste condizioni hanno portato a requisiti aggiuntivi quanto alla qualità della base giuridica per l'ingerenza (deve essere prevista in una legislazione accessibile ed essere prevedibile), alla proporzionalità di ogni misura e alla necessità di salvaguardie adeguate contro gli abusi.

A prescindere dal fatto che l'approccio frammentario alla legislazione descritto in appresso non consente una regolamentazione chiara ed accessibile, è lecito chiedersi se addirittura le ICC possono essere qualificate tali. Si potrebbero sollevare domande sulla procedura per una futura (eventuale) modifica del testo in questione. Si dovrebbe in ogni caso garantire che una decisione di questa importanza non possa essere modificata senza una procedura che preveda adeguata trasparenza e consultazione democratica.

b) La seconda questione riguarda la chiarezza del regime giuridico. La relazione della proposta non precisa i motivi per cui per il rilevamento e il trattamento degli identificatori biometrici occorra dotarsi di una base giuridica diversa. La relazione precisa che «la presente proposta … tratta del rilevamento dei dati biometrici mentre la proposta sul VIS riguarda la trasmissione e lo scambio di dati» ([2]). Tuttavia, dal punto di vista della protezione dei dati, il trattamento di dati personali include il rilevamento dei medesimi. Se in una catena di attività le operazioni normative sono disciplinate da testi giuridici diversi, ciò può nuocere alla chiarezza del regime. Ciò crea un problema per le persone interessate (dalla proposta) nonché per il controllo democratico del sistema. In effetti diventa sempre più difficile avere un quadro d'insieme in questo settore in cui atti legislativi diversi disciplinano ciò che costituisce fondamentalmente lo stesso trattamento di dati.

2.4. **Dispensa dal rilevamento obbligatorio delle impronte digitali**

Questo aspetto è illustrato molto bene dalla questione delle categorie di persone dispensate dall'obbligo di fornire le loro impronte digitali, in particolare nel caso dei bambini.

È opportuno esaminare, tenuto conto dell'obiettivo stesso del VIS, la possibilità di autorizzare il rilevamento delle impronte digitali dei bambini. In altre parole, l'obbligo per talune categorie di persone di fornire identificatori biometrici o la dispensa da tale obbligo deve essere una misura proporzionata nell'ambito della politica in materia di visti e di obiettivi connessi conformemente alla proposta sul VIS. Tale proporzionalità dovrebbe essere valutata nell'ambito di una procedura democratica.

Tale misura dovrebbe essere valutata anche dal punto di vista dell'uso di tale impronte digitali, come previsto nella proposta sul VIS. Gli elementi biometrici saranno utilizzati a fini di verifica o di identificazione: un identificatore biometrico potrebbe essere considerato tecnicamente attendibile in un caso ma non in un altro. Il trattamento delle impronte digitali dei bambini di età inferiore a 14 anni è generalmente considerato attendibile soltanto a fini di verifica. Ciò dovrebbe influenzare l'analisi della proposta in questione ma, ancora una volta, i necessari elementi si trovano nella proposta sul VIS (e al riguardo non è stata ancora presa alcuna decisione).

In conclusione, il GEPD raccomanda vivamente che le dispense dal rilevamento di identificatori biometrici nel quadro del regolamento relativo al VIS siano rigorosamente regolamentate per motivi di chiarezza e di coerenza. La regolamentazione del rilevamento di identificatori biometrici e in particolare delle impronte digitali nel presente caso dovrebbe essere considerata accessoria rispetto allo strumento giuridico principale e pertanto dovrebbe essere oggetto del testo principale stesso.

([1]) Il fatto che la base giuridica sia diversa — articolo 62, paragrafo 2, lettera b), punto ii per le ICC e articolo 66 per la proposta — non impedisce al legislatore di affrontare la materia nello stesso testo.

([2]) Relazione, pag. 5.

2.5. **Età delle persone che chiedono un visto**

La proposta precisa che soltanto i bambini di età inferiore a 6 anni sono dispensati dall'obbligo di fornire le impronte digitali. Ciò crea numerosi problemi (a prescindere dalla proposta interessata, sia essa quella relativa al VIS o all'istruzione consolare comune).

Anzitutto, il GEPD ritiene che il rilevamento generalizzato delle impronte digitali dei bambini non possa essere considerato una pura tecnicalità ma debba formare oggetto di un serio dibattito democratico nell'ambito delle istituzioni competenti. Siffatta decisione non dovrebbe basarsi unicamente sulla fattibilità tecnica, ma anche, per lo meno, sui vantaggi che presenterebbe per l'attuazione del VIS. Tuttavia, ad eccezione di un numero ristretto di Stati membri, non sembra che la questione sia attualmente oggetto di un dibattito pubblico, il che è estremamente deplorabile.

Occorre inoltre ricordare che il VIS è stato istituito in linea di massima allo scopo di facilitare le procedure per il rilascio del visto per i viaggiatori in buona fede (ossia la maggioranza dei viaggiatori). È pertanto opportuno tener conto di aspetti di ordine pratico e ergonomico ([1]). L'uso di identificatori biometrici nell'ambito della procedura per il rilascio dei visti oppure dei controlli alle frontiere non dovrebbe rendere eccessivamente difficile il rispetto delle procedure in materia di visto per i bambini.

Bisogna infine ricordare che tutti i sistemi di identificazione biometrica comportano imperfezioni tecniche. La letteratura scientifica non contiene prove concludenti secondo cui il rilevamento delle impronte digitali dei bambini di età inferiore a 14 anni permette un'identificazione attendibile. Le sole esperienze sinora compiute su un ampio campione demografico sono i sistemi Eurodac e Us-Visit. È piuttosto interessante notare che entrambi i sistemi utilizzano le impronte digitali dei bambini a partire dai 14 anni di età. Il rilevamento delle impronte digitali dei bambini di età inferiore a 14 anni dovrebbe essere supportato da studi che diano la prova della loro precisione e della loro utilità nel contesto di una banca dati su grande scala come il VIS.

In ogni caso sarebbe auspicabile utilizzare le impronte digitali dei bambini a fini di confronto di due serie di impronte anziché di più serie di impronte. Questo aspetto dovrebbe essere regolamentato in maniera esplicita.

Infine, la maggior parte delle osservazioni formulate precedentemente riguardano non soltanto i bambini, ma anche gli adulti. La precisione e la possibilità di utilizzare le impronte digitali diminuiscono con l'età ([2]) e gli aspetti di ordine pratico e ergonomico sono parimenti di particolare importanza.

2.6. **Fotografie**

Le stesse considerazioni potrebbero essere formulate per quanto riguarda le fotografie, per le quali non sono previsti limiti di età né nella presente proposta né nella proposta sul VIS. Ci si potrebbe tuttavia chiedere se le fotografie scattate prima che l'interessato abbia i lineamenti da adulto siano davvero utili ai fini dell'identificazione o anche della verifica.

Il riconoscimento facciale dei bambini (automatizzato in futuro o «umano») basato su fotografie di riferimento vecchie di qualche anno rischia di essere problematico. Anche se la tecnologia del riconoscimento facciale ha compiuto progressi significativi, è poco probabile che un software possa compensare, in un prossimo futuro, gli effetti della crescita sul volto di un bambino. Occorre pertanto precisare nel regolamento relativo al VIS che le fotografie possono essere utilizzate soltanto come elementi di sostegno per la verifica o l'identificazione di persone finché la tecnologia del riconoscimento facciale non sarà sufficientemente attendibile, tenuto conto che questo sarà probabilmente il caso per quanto riguarda i bambini in un futuro più lontano.

In generale, per entrambi gli identificatori biometrici il GEPD raccomanda di valutare attentamente se i vantaggi (lotta contro l'immigrazione illegale e tratta di bambini) siano superiori agli inconvenienti summenzionati.

2.7. **Altre eccezioni**

La proposta prevede che le persone «per cui è fisicamente impossibile» il rilevamento delle impronte digitali siano esentate dall'obbligo di tale rilevamento.

([1]) Come evidenziato in uno studio commissionato dal governo olandese, «*How do you measure a child? A study into the use of biometrics in children*, 2005, TNO», di J.E. DEN HARTOGH e altri.

([2]) Cfr. per es. A. HICKLIN e R. KHANNA, *The Role of Data Quality in Biometric Systems*, MTS, 9 febbraio 2006.

Il GEPD ha già sottolineato nel suo parere sulla proposta relativa al VIS che questa situazione riguarda un numero rilevante di persone: non potrebbe essere registrato fino al 5 % delle persone. Per una banca dati di 20 000 registrazioni all'anno, ciò significa che ci potrebbe essere fino a 1 000 000 di casi all'anno con difficoltà di registrazione. Questo aspetto dovrebbe essere certamente tenuto presente in sede d'esame della proposta in questione. Il GEPD ha insistito sulla necessità di procedure di ripiego efficaci:

> *«Si dovrebbe disporre di procedure di ripiego al fine di stabilire garanzie essenziali per l'inserimento di dati biometrici, poiché essi non sono né accessibili a tutti né completamente esatti. Siffatte procedure dovrebbero essere attuate e utilizzate per rispettare la dignità delle persone che non potranno seguire con esito positivo il processo di registrazione e per evitare di trasferire su di loro l'onere delle imperfezioni del sistema».*

Il regolamento proposto prevede in tali casi l'introduzione della menzione «non applicabile». Questa disposizione è certamente una cosa buona. Tuttavia potrebbe sorgere il timore che l'impossibilità di registrare i dati possa portare più facilmente al rifiuto del visto. Non è accettabile che un'altissima percentuale di tali casi si concluda con un rifiuto del visto.

È pertanto opportuno aggiungere nel regolamento relativo al VIS una disposizione in virtù della quale l'impossibilità di registrazione non comporti automaticamente un parere negativo sul rilascio del visto. Sarebbe inoltre opportuno prestare particolare attenzione a tale questione nell'ambito delle relazioni la cui elaborazione è prevista nel regolamento relativo al VIS: bisognerà verificare se un gran numero di rifiuti è legato all'impossibilità fisica di registrazione.

3. **ESTERNALIZZAZIONE DELLE DOMANDE DI VISTO**

Al fine di alleviare l'onere per gli Stati membri (dovuto tra l'altro all'acquisto ed alla manutenzione delle attrezzature) la proposta rende possibili vari meccanismi di cooperazione:

— coubicazione: il personale di uno o più Stati membri tratta la domanda (compresi gli identificatori biometrici) che ha ricevuto nella sede diplomatica e nella missione consolare di un altro Stato membro e condivide le attrezzature di tale Stato membro;

— Centri comuni per l'introduzione delle domande: il personale delle missioni diplomatiche di uno o più Stati membri è riunito in un unico edificio dove riceve le domande di visto inviate (compresi gli identificatori biometrici);

— Infine, la proposta prevede che il ricevimento del modulo di domanda ed il rilevamento degli identificatori biometrici possano essere effettuati da un fornitore esterno di servizi (tale opzione sembra essere l'unica via possibile per gli Stati membri che non possono utilizzare le altre due, anche se non è totalmente chiaro).

La proposta precisa accuratamente che soltanto fornitori esterni di servizi affidabili possono essere selezionati e che questi devono essere in grado di prendere tutte le misure necessarie per tutelare i dati dalla «distruzione accidentale o illecita, da un'alterazione o perdita accidentale, dall'accesso o divulgazione non autorizzati (…)» (punto 1.B.2 della proposta).

Tale disposizione è redatta con grande accuratezza e considerazione per la tutela dei dati, ed il GEPD se ne compiace. Tuttavia, il fatto di affidare il trattamento delle domande di visto ad un fornitore esterno di servizi in un paese terzo comporta una serie di conseguenze per quanto riguarda la tutela dei dati (talvolta molto delicati) raccolti ai fini del rilascio di visti.

Il GEPD sottolinea in particolare i seguenti punti:

— può risultare molto difficile, e talvolta impossibile, effettuare verifiche degli antecedenti sui dipendenti a causa della legislazione e delle prassi vigenti nel paese terzo;

— analogamente, non sarà necessariamente possibile imporre sanzioni ai dipendenti di un fornitore esterno per violazione della legislazione sulla privacy (anche se possono essere applicate sanzioni contrattuali al contraente principale);

— l'impresa privata può essere coinvolta in disordini o cambiamenti di natura politica e non essere in grado di assolvere ai suoi obblighi in termini di sicurezza del trattamento;

— può essere difficile prevedere una sorveglianza ufficiale, sebbene questa sia ancora più necessaria nel caso di partner esterni.

Qualsiasi contratto concluso con fornitori esterni di servizi dovrebbe pertanto contenere le necessarie salvaguardie per garantire l'osservanza delle norme in materia di tutela dei dati, compresi gli audit esterni, regolari controlli a sorpresa, relazioni, meccanismi che garantiscano la responsabilità del contraente in caso di violazione delle norme sulla privacy, ivi compreso l'obbligo di indennizzare i singoli interessati nel caso abbiano subito un danno risultante da un'azione del fornitore di servizi.

Oltre a queste preoccupazioni, un aspetto forse ancora più importante da considerare è che gli Stati membri non saranno in grado di garantire la tutela del trattamento dei dati esternalizzati (o del trattamento dei dati effettuato in un Centro comune per l'introduzione delle domande se ciò avviene in un edificio al di fuori delle sedi diplomatiche) nei confronti di un eventuale intervento (ad esempio perquisizione o sequestro) da parte delle autorità pubbliche del paese del richiedente ([1]).

In effetti, nonostante tutte le altre disposizioni contrattuali, i fornitori esterni di servizi saranno soggetti alla legislazione nazionale del paese terzo in cui sono stabiliti. Eventi recenti relativi all'accesso da parte delle autorità di un paese terzo a dati finanziari trattati da una società UE mostrano che il rischio è tutt'altro che teorico. Ciò potrebbe tra l'altro comportare un rischio grave per le persone interessate in alcuni paesi terzi che potrebbero avere un interesse particolare a sapere quali loro cittadini hanno presentato una domanda di visto (ai fini di un controllo politico sugli oppositori ed i dissidenti). Il personale di un'impresa privata, nella maggior parte dei casi personale locale, non sarebbe in grado di resistere alle pressioni finalizzate all'ottenimento di dati che potrebbero essere esercitate del governo o delle autorità di contrasto del paese del richiedente.

Si tratta di una carenza fondamentale di questo sistema rispetto ai casi in cui i dati sono trattati presso un ufficio consolare o una sede diplomatica. In tal caso i dati sarebbero protetti ai sensi della convenzione di Vienna del 18 aprile 1961 sulle relazioni diplomatiche, il cui articolo 22 stipula che:

> *«I locali della missione sono inviolabili. Non è consentito agli agenti dello Stato accreditatario di penetrarvi, tranne che con il consenso del capo missione. (…) I locali della missione, il loro mobilio e gli altri oggetti che visi trovano, nonché i mezzi di trasporto della missione, non possono essere oggetto di nessuna perquisizione, confisca o provvedimento esecutivo».*

Inoltre, ai sensi dell'articolo 4, paragrafo 1, lettera b) della direttiva 95/46/CE, le disposizioni nazionali di attuazione della direttiva si applicherebbero anche esplicitamente al trattamento dei dati personali, rafforzandone in tal modo la tutela.

Sembra pertanto evidente che l'unica maniera efficace per tutelare i dati relativi ai richiedenti dei visti e dei cittadini o società UE patrocinanti consiste nel fornire loro una tutela garantita ai sensi della convenzione di Vienna. ciò significa che i dati dovrebbero essere trattati nei locali che godono di protezione diplomatica. Questo non impedirebbe agli Stati membri di esternalizzare il trattamento delle domande di visto, nella misura in cui il contraente esterno può svolgere le sue attività nei locali della sede diplomatica. Ciò si applicherebbe anche ai Centri comuni per l'introduzione delle domande.

Il GEPD esprime pertanto un parere contrario alla possibilità di esternalizzare il trattamento a fornitori esterni di servizi come previsto a pagina 15 della proposta, nuovo punto 1.B.1., lettera b). A tale proposito, opzioni accettabili sono:

— esternalizzare il trattamento della domanda di visto verso un'impresa privata a condizione che questa sia situata in un luogo avente status di sede diplomatica;

— esternalizzare soltanto la fornitura di informazioni verso un centralino, come proposto al punto 1.B.1., lettera a).

4. **CONCLUSIONE**

Il GEPD si compiace del fatto che la proposta di modifica dell'Istruzione consolare comune debba essere adottata secondo la procedura di codecisione, rafforzando in tal modo l'esame democratico in un settore dove tale esigenza si fa particolarmente sentire.

([1]) Questo problema si è già presentato nel caso del trattamento di domande da parte di agenzie di viaggio; si tratta tuttavia di una materia ancora più delicata poiché riguarda anche i dati biometrici e poiché in linea di principio il ricorso ad un'agenzia di viaggio non è obbligatorio.

Sulla sostanza, il GEPD formula le seguenti raccomandazioni:

— le esenzioni dall'obbligo di fornire le impronte digitali devono essere trattate nell'ambito del regolamento sul VIS piuttosto che di quello sull'Istruzione consolare comune, al fine di garantire la chiarezza e la coerenza del regime;

— occorre esaminare accuratamente i limiti di età per il rilevamento delle impronte digitali e delle fotografie, tenendo conto degli aspetti di fattibilità, ma anche di fattori etici, pratici e di accuratezza;

— le fotografie non devono essere considerate come metodi di identificazione autonomi, ma soltanto come elementi di sostegno;

— l'esternalizzazione del trattamento delle domande di visto a società private dovrebbe essere ammesso solo se ha luogo in locali che godono della protezione diplomatica ed è fondata su clausole contrattuali che garantiscono una sorveglianza efficace e la responsabilità del contraente.

Fatto a Bruxelles, addì 27 ottobre 2006

Peter HUSTINX

Garante europeo della protezione dei dati