GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati 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 (COM(2004) 835 definitivo)

(2005/C 181/06)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

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

vista la Carta dei diritti fondamentali dell'Unione europea, 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, in particolare l'articolo 41,

vista la richiesta di parere, ricevuta il 25 gennaio 2005 dalla Commissione, a norma dell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001,

HA ADOTTATO IL SEGUENTE PARERE:

1. **INTRODUZIONE**

1.1 **Premessa**

L'istituzione del sistema d'informazione visti (VIS) costituisce una parte importante della politica comune dell'UE in materia di visti e ha formato oggetto di vari strumenti fra loro connessi.

— Nell'aprile 2003 è stato presentato uno studio di fattibilità [1] sul VIS, commissionato dalla Commissione.

— Nel settembre 2003 la Commissione ha proposto la modifica [2] di un precedente regolamento che istituisce un modello uniforme per i visti. L'obiettivo principale consiste nell'introdurre nel nuovo modello di visto i dati biometrici (immagine del volto e due impronte digitali) da memorizzare su chip.

[1] *Visa Information System*, relazione finale, commissionata dalla Commissione e realizzata dalla Trasys, aprile 2003.
[2] COM(2003) 558 defin. (2003/0217 (CNS) e 2003/0218 (CNS))

— Nel giugno 2004 una decisione del Consiglio ([1]) ha avviato il processo istitutivo del sistema d'informazione visti fornendo la base giuridica per la sua iscrizione nel bilancio dell'UE. La decisione propone una base di dati centrale comprendente informazioni connesse alle domande di visto e prevede il ricorso alla procedura di «comitologia» per gestire gli sviluppi tecnici del VIS.

Nel dicembre 2004 la Commissione ha presentato una proposta di regolamento concernente il VIS e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata ([2]) (di seguito «la proposta»), che forma oggetto del presente parere. Uno studio per la valutazione d'impatto estesa ([3]) (di seguito «VIE») è allegato alla proposta.

Tuttavia, come indicato nella relazione introduttiva alla proposta, saranno necessari ulteriori strumenti giuridici per completare il regolamento, in particolare al fine di:

— modificare l'Istruzione consolare comune diretta alle rappresentanze diplomatiche e consolari di prima categoria delle parti contraenti della convenzione di Schengen (di seguito «Istruzione consolare comune»), per quanto riguarda l'introduzione dei dati biometrici nelle procedure;

— sviluppare un nuovo meccanismo per lo scambio di dati con l'Irlanda e il Regno Unito;

— scambiare i dati relativi ai visti per soggiorni di lunga durata.

Come deciso dal Consiglio «Giustizia e affari interni» del 5 e 6 giugno 2003 e secondo quanto disposto dall'articolo 1, paragrafo 2 della succitata decisione del Consiglio del giugno 2004, il VIS sarà basato su un'architettura centralizzata comprendente una base di dati in cui sono memorizzati i fascicoli relativi alle domande di visto: il sistema centrale d'informazione visti (CS-VIS) e un'interfaccia nazionale (NI-VIS) situata in ciascuno Stato membro. Gli Stati membri designeranno ([4]) un'autorità centrale nazionale collegata all'interfaccia nazionale e attraverso la quale le rispettive autorità competenti avranno accesso al CS-VIS.

1.2 **Principali elementi della proposta sotto il profilo della protezione dei dati**

La proposta è intesa a migliorare la gestione della politica comune in materia di visti agevolando lo scambio di dati tra gli Stati membri, attraverso l'istituzione di una base di dati centrale. Il regolamento prevede l'introduzione di dati biometrici (fotografia e impronte digitali) nel corso della procedura di presentazione della domanda e la registrazione dei medesimi nella base di dati centrale.

I dati biometrici potrebbero essere usati anche sulla vignetta visto mediante l'inserimento della fotografia e delle impronte digitali memorizzate su chip, come previsto dal regolamento modificativo proposto dalla Commissione sul modello uniforme per i visti (con riserva della decisione del Consiglio basata sui risultati dell'attuale analisi).

La proposta descrive nei particolari le varie operazioni effettuate con i dati (inserimento, modifica, cancellazione e consultazione) e i vari dati da aggiungere nel VIS a seconda dei casi (domanda accolta, domanda respinta, ecc.).

La proposta prevede un periodo di cinque anni per la conservazione dei dati relativi a ciascuna domanda.

La proposta elenca limitativamente le autorità competenti diverse dalle autorità competenti per i visti, abilitate ad accedere al VIS e definisce i diritti di accesso loro attribuiti:

— le autorità competenti in materia di controlli alle frontiere esterne e all'interno del territorio degli Stati membri

— le autorità competenti in materia di immigrazione

([1]) Decisione 2004/512/CE, GU L 213 del 15.6.2004, pag. 5.
([2]) COM(2004) 835 defin. (2004/0287 (COD)).
([3]) *Study for the Extended Impact Assessment of the Visa Information System*, relazione finale, EPEC, dicembre 2004
([4]) Articolo 24, paragrafo 2, della proposta.

— le autorità competenti in materia di asilo.

Nel descrivere il funzionamento del VIS e le responsabilità ad esso relative, la proposta indica che la Commissione tratta i dati del VIS per conto degli Stati membri. Illustra la necessità di usare le registrazioni delle operazioni di trattamento dei dati per garantire la sicurezza dei medesimi e descrive le singole responsabilità per assicurare tale livello di sicurezza.

La proposta contiene un capo dedicato alla protezione dei dati in cui sono definiti i ruoli delle autorità nazionali e del garante europeo della protezione dei dati (di seguito «GEPD»).

La proposta affida la realizzazione tecnica del VIS e la scelta delle necessarie tecnologie ad un comitato istituito dall'articolo 5, paragrafo 1 del regolamento (CE) n. 2424/2001 sullo sviluppo del Sistema d'informazione Schengen di seconda generazione (SIS II).

Una valutazione d'impatto estesa del VIS, commissionata dalla Commissione e realizzata dall'EPEC, è allegata alla proposta. Essa conclude che l'opzione di un VIS che si avvalga dell'utilizzo di dati biometrici è attualmente la soluzione migliore per migliorare la politica comune in materia di visti.

2. **QUADRO PERTINENTE**

La proposta avrà un'incidenza rilevante sul diritto alla vita privata e su altri diritti fondamentali delle persone; è pertanto soggetta ad un controllo alla luce dei principi relativi alla protezione dei dati. L'esame è effettuato secondo i seguenti parametri:

— il rispetto della vita privata è sancito in Europa dal 1950 con l'adozione da parte del Consiglio d'Europa della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (di seguito «la CEDU»). L'articolo 8 di tale convenzione prevede il «diritto al rispetto della vita privata e familiare».

  A norma dell'articolo 8, paragrafo 2 può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto soltanto se tale ingerenza è «prevista dalla legge» e costituisce «una misura che, in una società democratica, é necessaria» per tutelare interessi importanti. Secondo la giurisprudenza della Corte europea dei diritti dell'uomo, tali condizioni hanno portato ad obblighi supplementari in termini di qualità delle basi giuridiche sull'ingerenza, proporzionalità delle misure e necessità di adeguate salvaguardie contro gli abusi.

  I principi che sottendono la protezione delle persone rispetto al trattamento di dati di carattere personale sono stati sviluppati nella convenzione sulla protezione dei dati, elaborata dal Consiglio d'Europa e adottata nel 1981.

— Il diritto al rispetto della vita privata e il diritto alla protezione dei dati di carattere personale sono stati sanciti più di recente dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, inserita nella parte II della nuova Costituzione UE.

  A norma dell'articolo 52 della Carta è riconosciuta la possibilità di assoggettare tali diritti a limitazioni purché siano soddisfatte condizioni uguali a quelle previste dall'articolo 8 della CEDU. Dette condizioni devono essere prese in considerazione ogniqualvolta si esamini una proposta di possibile ingerenza.

Attualmente, le disposizioni di base relative alla protezione dei dati nella normativa UE sono stabilite:

— nella direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31). La direttiva, di seguito denominata «direttiva 95/46/CE», prevede i principi particolareggiati alla luce dei quali sarà effettuata l'analisi della proposta, nella misura in cui si applica agli Stati membri. Ciò è tanto più importante se si considera che la proposta si applicherà congiuntamente alla legislazione nazionale di attuazione della direttiva. L'efficacia delle disposizioni e salvaguardie proposte dipenderà pertanto dall'efficacia di tale combinazione nei singoli casi;

— nel 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 (GU L 8, pag. 1). Il regolamento, di seguito denominato «regolamento n. 45/2001», prevede principi analoghi a quelli contenuti nella direttiva 95/46/CE ed è pertinente in questo contesto in quanto la proposta si applicherà alle attività della Commissione congiuntamente alle disposizioni del regolamento. Anche tale combinazione merita pertanto attenzione.

La direttiva 95/46/CE e il regolamento n. 45/2001 devono essere letti in combinato disposto con altri strumenti. In altri termini, la direttiva e il regolamento, poiché disciplinano il trattamento di dati personali che possono ledere le libertà fondamentali e, in particolare, il diritto alla vita privata, devono essere interpretati alla luce dei diritti fondamentali. Ciò si desume anche dalla giurisprudenza della Corte di giustizia europea. ([1])

— Infine, il GEPD includerà nella sua analisi il parere n. 7/2004, dell'11 agosto 2004, del Gruppo dell'articolo 29 per la protezione dei dati ([2])«sull'inclusione di elementi biometrici nei permessi di residenza e nei visti tenuto conto dell'istituzione del sistema europeo d'informazione visti (VIS)». In tale parere il Gruppo ha espresso preoccupazioni riguardo a vari elementi della proposta. Il GEPD intende verificare se e come la proposta ha tenuto conto delle preoccupazioni espresse.

3. **ANALISI DELLA PROPOSTA**

3.1 **Osservazioni generali**

Il GEPD riconosce che l'ulteriore sviluppo della politica comune in materia di visti richiede uno scambio efficace di dati pertinenti. Uno dei meccanismi capaci di assicurare una trasmissione fluida di informazioni è il VIS. Tuttavia, tale nuovo strumento andrebbe limitato alla raccolta e allo scambio di dati nella misura necessaria allo sviluppo di una politica comune in materia di visti e proporzionata per la realizzazione di tale obiettivo.

L'istituzione del VIS può avere conseguenze positive per altri interessi pubblici legittimi senza tuttavia alterare la finalità del sistema. Il suo scopo limitato riveste un'importanza decisiva nel determinare il contenuto e l'uso legittimi del sistema e quindi anche nel concedere il diritto di accesso al VIS (o ad una parte dei suoi dati) alle autorità degli Stati membri per interessi pubblici legittimi.

Inoltre, la proposta introduce l'uso di elementi biometrici nel VIS. Il GEPD riconosce i vantaggi legati all'uso di elementi biometrici, sottolineandone tuttavia il notevole impatto e proponendo l'introduzione di salvaguardie rigorose circa l'uso dei dati biometrici.

Il presente parere deve essere letto alla luce di queste considerazioni essenziali. Esso dovrebbe essere citato nel preambolo del regolamento prima dei considerando («visto il parere ...»).

([1]) È utile al riguardo riferirsi alla sentenza della Corte di giustizia nella causa Österreichischer Rundfunk e altri (cause riunite C-465/00, C-138/01 e C-139/01, sentenza della Corte riunita in seduta plenaria del 20 maggio 2003, Racc. 2003, I-4989). La Corte si è pronunciata in merito ad una legge austriaca che prevede la trasmissione alla Corte dei conti austriaca di dati riguardanti i redditi percepiti da dipendenti di enti pubblici e la loro successiva divulgazione. Nella sentenza la Corte stabilisce una serie di criteri derivanti dall'articolo 8 della convenzione europea dei diritti dell'uomo che dovrebbero essere adottati nell'applicare la direttiva 95/46/CE, in quanto questa ammette alcune restrizioni al diritto alla vita privata.

([2]) È un gruppo a carattere consultivo e indipendente, composto da rappresentanti delle autorità di controllo degli Stati membri, del GEPD e della Commissione e istituito dalla direttiva 95/46/CE.

3.2 **Finalità**

La finalità del VIS riveste un'importanza cruciale, alla luce sia dell'articolo 8 della CEDU che del quadro generale sulla protezione dei dati. In conformità dell'articolo 6 della direttiva 95/46/CE, i dati personali devono essere «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità». Solo una chiara definizione della finalità consentirà una corretta valutazione della proporzionalità e dell'adeguatezza del trattamento dei dati personali, il che è fondamentale tenuto conto della natura di tali dati (compresi quelli biometrici) e della portata dell'operazione di trattamento prevista.

La finalità del VIS è definita chiaramente all'articolo 1, paragrafo 2 della proposta:

> «Il VIS contribuisce a migliorare la realizzazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra autorità consolari centrali agevolando lo scambio di dati tra Stati membri in merito alle domande e alle relative decisioni».

Pertanto, tutti gli elementi del VIS devono essere strumenti necessari e proporzionati per conseguire questo obiettivo nell'interesse della politica comune in materia di visti.

L'articolo 1, paragrafo 2 della proposta elenca inoltre ulteriori vantaggi legati al miglioramento della politica in materia di visti, quali:

a) prevenire minacce alla sicurezza interna;

c) agevolare la lotta contro la frode;

d) agevolare i controlli ai valichi delle frontiere esterne.

Il GEPD considera questi elementi come esempi dei vantaggi derivanti dall'istituzione del VIS e dal miglioramento della politica comune in materia di visti, ma non come finalità a se stanti.

Ne derivano due conseguenze principali in questa fase:

— il GEPD è consapevole del fatto che le strutture di contrasto sono interessate ad avere accesso al VIS; il 7 marzo 2005 il Consiglio ha adottato conclusioni in tal senso. Poiché il VIS ha la finalità di migliorare la politica comune in materia di visti, va osservato che la concessione di un accesso sistematico alle strutture di contrasto sarebbe in contrasto con tale finalità. Benché ai sensi dell'articolo 13 della direttiva 95/46/CE l'accesso possa essere concesso su base *ad hoc*, in circostanze specifiche e fatte salve adeguate garanzie, un accesso sistematico non può essere autorizzato.

  In termini più generali, una valutazione della proporzionalità e della necessità dell'accesso è fondamentale se in futuro fossero adottate decisioni sulla concessione o meno dell'accesso al VIS a talune altre autorità. I compiti per i quali è autorizzato l'accesso devono essere coerenti con le finalità del VIS.

— Il riferimento esplicito alla prevenzione delle minacce alla sicurezza interna di qualunque Stato membro di cui alla lettera a) è inopportuno. I principali vantaggi del VIS saranno la prevenzione delle frodi e del «visa shopping» (la lotta contro le frodi è anche la ragione principale dell'inclusione di dati biometrici nel sistema) ([1]). La prevenzione delle minacce alla sicurezza dovrebbe pertanto essere considerata un vantaggio «secondario», benché assai utile.

  Il GEPD raccomanda di rendere più esplicita la distinzione tra «finalità» e «vantaggi» nel testo dell'articolo 1, paragrafo 2, ad esempio come segue:

  > «Il VIS ha la finalità di migliorare la realizzazione della politica comune in materia di visti, la cooperazione consolare e la consultazione tra autorità consolari centrali agevolando lo scambio di dati tra Stati membri in merito alle domande e alle relative decisioni. In tal modo contribuisce altresì a ...».

([1]) La VIE stabilisce ciò in termini assai chiari (pag. 6, §2.7): *«le inefficienze nella lotta al "visa shopping", alle frodi e in materia di controlli provocano inefficienze anche in relazione alla sicurezza interna degli Stati membri»*. Ciò implica che le minacce alla sicurezza sono in parte dovute all'inefficacia della politica in materia di visti. A tale riguardo occorre innanzitutto migliorare tale politica, principalmente lottando contro le frodi ed effettuando controlli più accurati. Da un miglioramento della politica in materia di visti risulterà un miglioramento della sicurezza.

È inoltre opportuno osservare al riguardo che gli «Orientamenti per la creazione di un sistema comune di scambio di dati in materia di visti», adottati dal Consiglio «GAI» il 13 giugno 2002 [1], hanno posto la prevenzione delle minacce alla sicurezza interna alla fine dell'elenco. Si potrebbe fare lo stesso nel testo in esame; siffatta redazione sarebbe assai più coerente con la finalità del VIS.

3.3 **Qualità dei dati**

Ai sensi dell'articolo 6 della direttiva 95/46/CE, i dati personali devono anche essere «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati». Tale requisito fa riferimento alla proporzionalità del VIS in quanto tale, ma anche ai dati da raccogliere e memorizzare nel VIS e alla loro successiva utilizzazione, nonché alle garanzie supplementari applicabili in questo contesto. Detti elementi sono parimenti essenziali per la valutazione della proposta ai sensi dell'articolo 8 della CEDU.

L'istituzione del VIS rappresenta indubbiamente una notevole ingerenza nell'esercizio del diritto alla vita privata, se non altro per la sua portata e le categorie di dati personali trattate. Per tale motivo il Gruppo dell'articolo 29 ha chiesto, nel suo parere n. 7/2004, che gli vengano comunicati gli studi sulla portata e la gravità dei fenomeni in questione, nei quali sono addotte ragioni imprescindibili inerenti alla sicurezza pubblica o all'ordine pubblico che giustificano siffatto approccio.

Il GEPD ha preso attentamente atto delle prove presentate dalla VIE. Benché esse non siano del tutto decisive, sembra che vi siano ragioni sufficienti per giustificare l'istituzione del VIS al fine di migliorare la politica comune in materia di visti.

In tale contesto sembrerebbe rientrare nel margine di valutazione del legislatore la decisione relativa all'istituzione del VIS quale strumento volto a migliorare le condizioni di rilascio dei visti da parte degli Stati membri. Siffatto sistema potrebbe in quanto tale inserirsi efficacemente nella creazione progressiva di uno spazio di libertà, sicurezza e giustizia, come previsto nel trattato CE, nonché sostenere tale processo.

Tuttavia l'istituzione e l'impiego del VIS non potranno in nessun caso avere l'effetto di impedire che un elevato livello di protezione dei dati personali possa continuare a essere garantito in questo settore. Rientra nelle funzioni consultive del GEPD esaminare sino a che punto il VIS influirà sul livello attuale di protezione dei dati relativi alle persone interessate.

Considerato quanto precede, il GEPD esaminerà in particolare, nel presente parere, le questioni seguenti:

— proporzionalità e adeguatezza dei dati, e loro utilizzazione (ad es. categorie di dati, accesso ai dati per ciascuna autorità interessata e periodo di conservazione dei dati);

— funzionamento del sistema (ad es. responsabilità e sicurezza);

— diritti delle persone interessate (ad es. informazione, possibilità di correggere o cancellare dati inesatti o non pertinenti);

— monitoraggio e supervisione del sistema.

Ad eccezione dei punti seguenti, la proposta non solleva osservazioni di rilievo per quanto riguarda le categorie di dati da inserire nel VIS e la loro utilizzazione. Le disposizioni pertinenti sono state redatte con debita cura e appaiono nel complesso coerenti e adeguate.

[1] Decisione quadro del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo (2002/475/GAI), GU L 164 del 22.6.2002, pag. 3.

3.4 **Biometria**

3.4.1 *Impatto dell'utilizzazione della biometria*

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 non costituisce solo un'altra tecnologia dell'informazione: essa 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.

Per quanto utile possa essere la biometria per determinati scopi, la sua utilizzazione generalizzata avrà un impatto enorme sulla società e dovrebbe essere oggetto di un dibattito ampio e aperto. Il GEPD non può che osservare che tale dibattito non ha ancora avuto veramente luogo prima dell'elaborazione della proposta. Ciò evidenzia ancor più la necessità di garanzie rigorose per l'utilizzazione di dati biometrici, come pure di una riflessione e di un dibattito approfonditi nel corso del processo legislativo.

3.4.2 *Specificità della biometria*

Come già sottolineato in vari pareri del Gruppo dell'articolo 29 ([1]), l'inserimento e il trattamento di dati biometrici ai fini dei documenti di identità dovranno essere accompagnati da garanzie particolarmente coerenti e rigorose. Infatti, a causa di alcune caratteristiche specifiche, i dati biometrici sono altamente sensibili.

È vero che la perdita di dati biometrici è quasi impossibile per la persona interessata, contrariamente a una password o a una chiave. Essi 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*.

Cionondimeno è quasi impossibile annullare i dati biometrici: un dito o un viso difficilmente si modificano. Questa caratteristica, positiva sotto vari punti di vista, presenta un grave inconveniente in caso di *furto di identità*: le memorizzazione in una base di dati di impronte digitali e di una fotografia associate a un'identità usurpata potrebbe causare problemi gravi e permanenti al possessore effettivo di tale identità. Inoltre, in virtù della loro stessa natura, i dati biometrici *non sono segreti* e possono persino *lasciare tracce* (impronte digitali, DNA) che consentono la raccolta di tali dati *senza che il possessore ne sia consapevole*.

A causa di questi rischi inerenti alla natura della biometria, occorre porre in atto importanti garanzie (specie in termini di rispetto del principio della limitazione dello scopo, di restrizione dell'accesso e di misure di sicurezza).

3.4.3 *Imperfezione tecnica delle impronte digitali*

I principali vantaggi della biometria sopra descritti (universalità, distinguibilità, permanenza, usabilità dei dati, ecc.) non sono mai assoluti. Ciò ha un impatto diretto sull'efficacia delle procedure previste nel regolamento per la registrazione e la verifica dei dati biometrici.

In base alle stime effettuate ([2]), la percentuale delle persone che non possono essere registrate tocca il 5 % (poiché le loro impronte digitali non sono leggibili, o neppure esistono). La VIE allegata alla proposta ha previsto circa 20 milioni di richiedenti il visto per il 2007: ciò significa che potrà arrivare a 1 milione il numero di persone che non potranno seguire la procedura «normale» di registrazione, con evidenti conseguenze per la domanda di visto e il controllo alle frontiere.

([1]) Parere 7/2004 sull'inserimento di elementi biometrici nei permessi di soggiorno e nei visti, tenendo conto dell'istituzione del sistema europeo di informazione visti (VIS) (MARKT/11487/04/EN - WP 96) e documento di lavoro sulla biometria (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention:Usability and Trust in Information Systems*, *in*«Foresight cybertrust and crime prevention project». 04/1151, 10 giugno 2004, pag. 7, e Technology Assessment, «Using Biometrics for Border Security», United States General Accounting Office, GAO-03-174, novembre 2002.

L'identificazione biometrica è anche, per definizione, un processo statistico. Una percentuale di errore dello 0,5-1 % è normale ([1]): ciò significa che il sistema di controllo alle frontiere esterne avrà un tasso di respingimento ingiustificato (False Reject Rate) tra lo 0,5 e l'1 %. Questa percentuale vari in funzione di una soglia basata sulla politica in materia di gestione dei rischi delle autorità competenti (ciò equivale a creare un equilibrio tra il numero di persone respinte per errore e quelle ammesse per errore). Pertanto è esagerato ritenere che queste tecnologie garantiscano «un'identificazione esatta» della persona in questione, come affermato nel considerando n. 9 del regolamento proposto.

Conformemente a un recente studio prospettivo ([2]) richiesto dalla commissione LIBE del Parlamento europeo, 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 ([3]).

Il GEPD raccomanda pertanto che siano elaborate e incluse nella proposta procedure di ripiego. Tali procedure non dovrebbero né ridurre il livello di sicurezza della politica in materia di visti né ledere la dignità delle persone con impronte digitali illeggibili.

3.5 **Categorie speciali di dati**

Alcune categorie di dati (oltre ai dati biometrici) richiedono particolare attenzione: i dati relativi ai motivi di rifiuto del visto (punto 3.4.1) e i dati relativi ad altri membri di un gruppo (punto 3.4.2).

3.5.1 *Motivi di rifiuto del visto*

L'articolo 10, paragrafo 2 della proposta prevede, qualora sia adottata una decisione di rifiuto del visto, il trattamento dei dati relativi ai motivi del rifiuto. Questi ultimi sono del tutto standardizzati.

— I primi due motivi figuranti alle lettere a) e b) sono di natura piuttosto amministrativa: mancata presentazione di un documento di viaggio valido, o documenti validi che dimostrino gli scopi e le condizioni del previsto soggiorno.

— Nella lettera c) è menzionata «una segnalazione sul richiedente ai fini del rifiuto dell'ingresso», che implica una consultazione della base di dati del SIS.

— Infine, nella lettera d) è indicato, come motivo di rifiuto del visto, il fatto che il richiedente «costituisce una minaccia all'ordine pubblico, alla sicurezza interna, alla salute pubblica e alle relazioni internazionali di uno Stato membro».

([1])

Elemento biometrico	Viso	Dito	Iride
FTE non registrazione (%)	n/d	4	7
FNMR tasso di respingimento (%)	4	2.5	6
FMR1 tasso di errore nelle verifiche (%)	10	<0,01	<0,001
FMR2 tasso di errore nelle identificazioni in BD > 1 m (%)	40	0,1	N/D
FMR3 tasso di errore nei controlli in BD=500 (%)	12	<1	N/D

A. K. Jain et al., *Biometrics: A grand Challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK., agosto 2004.

([2]) A*Biometrica alle frontiere: valutare l'impatto sulla società*, febbraio 2005, Istituto di studi delle prospettive tecnologiche, DG Centro comune di ricerca, CE.

([3]) *Relazione sull'andamento dell'applicazione dei principi della convenzione 108 alla raccolta e al trattamento dei dati biometrici*, Consiglio d'Europa, 2005, pag. 11.

Tutti i motivi di rifiuto del visto devono essere applicati con grande cautela per le conseguenze che ne risultano per le persone interessate. Inoltre alcuni di essi, ossia quelli figuranti alle lettere c) e d), comportano il trattamento di «dati sensibili» ai sensi dell'articolo 8 della direttiva 95/46/CE.

Il GEPD desidera richiamare l'attenzione più specificamente sulla condizione relativa alla salute pubblica, che appare vaga e implica il trattamento di dati assai sensibili. Conformemente al commento sugli articoli allegato alla proposta, il riferimento alla minaccia per la salute pubblica si basa sulla «proposta di regolamento del Consiglio che istituisce un Codice comunitario relativo al regime di attraversamento delle frontiere da parte delle persone» (COM(2004) 391 defin.).

Il GEPD è consapevole del fatto che il criterio della «salute pubblica» è ampiamente utilizzato nella normativa comunitaria sulla libertà di circolazione delle persone ed è applicato con grande rigore, come dimostrato dalla direttiva 2004/38/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri. L'articolo 29 di detta direttiva stabilisce le condizioni alle quali si tiene conto della minaccia alla salute pubblica: «Le sole malattie che possono giustificare misure restrittive della libertà di circolazione sono quelle con potenziale epidemico, quali definite dai pertinenti strumenti dell'Organizzazione mondiale della sanità, nonché altre malattie infettive o parassitarie contagiose, sempreché esse siano oggetto di disposizioni di protezione che si applicano ai cittadini dello Stato membro ospitante.».

— Occorre tuttavia notare che la proposta sopra menzionata è finora solo una proposta e che l'inclusione della condizione di non costituire una minaccia alla salute pubblica nel regolamento VIS è subordinata all'adozione del Codice comunitario.

— Inoltre, se fosse adottato, questo motivo di rifiuto dell'ingresso dovrebbe essere interpretato in maniera restrittiva. Infatti la proposta relativa al Codice comunitario si basa a sua volta sulla già citata direttiva 2004/38/CE.

Il GEPD raccomanda pertanto di inserire nel testo della proposta un riferimento all'articolo 29 della direttiva 2004/38/CE per garantire che la «minaccia alla salute pubblica» sia intesa nel senso di tale disposizione. In ogni caso, considerata la sensibilità dei dati, questi dovrebbero essere trattati solo se la minaccia alla salute pubblica fosse reale, attuale e sufficientemente grave.

3.5.2 *Dati su altri membri di un gruppo*

L'articolo 2, punto 7 definisce i termini «membri del gruppo» come «gli altri richiedenti con i quali il richiedente viaggia, compresi il coniuge e i figli che lo accompagnano». Il commento sugli articoli precisa che le definizioni figuranti nell'articolo 2 della proposta si riferiscono al trattato o all'acquis di Schengen sulla politica in materia di visti, tranne alcuni termini, compresi «membri del gruppo», che sono definiti specificamente ai fini del regolamento in esame. Si può pertanto desumere che questa definizione non fa riferimento alla definizione di «visto collettivo» figurante al punto 2.1.4 dell'Istruzione consolare comune. Il commento sugli articoli menziona «i richiedenti che viaggiano in gruppo con altri richiedenti, ad esempio nell'ambito di un accordo ADS, o insieme con familiari».

Il GEPD sottolinea che nel regolamento dovrebbe figurare una definizione precisa e completa di «membri del gruppo». Non può che osservare che nella proposta attuale la definizione è troppo vaga, in mancanza di un riferimento preciso al trattato o all'acquis di Schengen. In base alla suddetta formulazione della definizione, «membri del gruppo» potrebbe includere colleghi, altri clienti della stessa agenzia di viaggio che partecipano a un viaggio organizzato, ecc. Le conseguenze sono in

effetti assai importanti: ai sensi dell'articolo 5 del progetto di regolamento, il fascicolo «domanda» per ciascun richiedente è collegato ai fascicoli «domanda» degli altri membri del gruppo.

3.6 **Conservazione dei dati**

L'articolo 20 del progetto di regolamento contempla per ciascun fascicolo un periodo di conservazione di cinque anni. Si tratta di una scelta politica affinché il legislatore comunitario preveda un limite di tempo ragionevole.

Non esiste alcuna prova — segnatamente non alla luce dei motivi addotti nel commento relativo agli articoli — da cui si evince che la scelta politica effettuata in tale proposta sia irragionevole o abbia conseguenze inaccettabili, a condizione che siano messi in atto tutti gli opportuni meccanismi correttivi. Questo significa che la rettifica o la cancellazione dei dati deve essere garantita quando i dati non sono più esatti e in particolare quando una persona ha ottenuto la nazionalità di uno Stato membro o ha acquisito uno status che non richiede il suo inserimento nel sistema.

Inoltre, quando sono ancora presenti nel sistema, i dati non possono in alcun modo pregiudicare una nuova decisione. Alcuni motivi del respingimento (in particolare segnalazione del richiedente ai fini del rifiuto dell'ingresso, minaccia alla salute pubblica) hanno una validità limitata nel tempo. Il fatto che abbiano costituito validi motivi di rifiuto dell'ingresso in un dato momento non dovrebbe influenzare una nuova decisione. La situazione deve essere interamente riesaminata per ciasuna nuova domanda di visto e questo dovrebbe essere, se del caso, reso esplicito nel regolamento.

3.7. **Accesso e uso dei dati**

3.7.1 *Osservazioni preliminari*

Come osservazione preliminare, il garante europeo della protezione dei dati (GEPD) prende atto dell'attenzione ovviamente prestata al sistema normativo di accesso e di uso dei dati VIS. Ciascuna autorità ha accesso a differenti dati per scopi diversi. Si tratta di un approccio adeguato che il GEPD può solo incoraggiare. Le seguenti osservazioni sono volte ad applicare questo approccio nella misura più ampia possibile.

3.7.2 *Controlli sui visti alle frontiere esterne nonché all'interno del territorio*

Nel caso di controlli sui visti alle frontiere esterne, l'articolo 16 della proposta di regolamento cita chiaramente i due precisi obiettivi:

— «verificare l'identità della persona», il che significa secondo la definizione data, una comparazione faccia a faccia (one to one comparison);

— «verificare l'autenticità del visto». Come proposto dalle norme dell'ICAO, il microchip del visto potrebbe utilizzare un sistema di certificazione a chiave pubblica/privata ((Public Key Infrastructure) al fine di effettuare tale processo di autenticazione.

Questi due obiettivi possono essere opportunamente raggiunti con l'esclusivo accesso al microchip protetto da parte delle autorità competenti ad effettuare i controlli sui visti. Un accesso alla base di dati centrale del VIS sarebbe pertanto eccessivo nel caso specifico. Quest'ultima opzione comporterebbe più autorità collegate al VIS, il che potrebbe far aumentare il rischio di un uso improprio. Potrebbe inoltre risultare un'opzione più costosa in quanto aumenteranno in misura considerevole il numero di accessi protetti e controllati al VIS nonché l'esigenza di formazione specifica connessa a tali accessi.

Permangono inoltre dubbi sull'adeguatezza dell'accesso ai dati come previsto all'articolo 16, paragrafo 2. Infatti, il paragrafo 2, lettera a) stabilisce che se, da una prima interrogazione emerge che i dati relativi al richiedente sono registrati nel VIS (come dovrebbe avvenire in linea di massima), l'autorità competente può consultare altri dati, sempre allo scopo di verificare l'identità. Questi dati riguardano tutte le informazioni relative alla domanda, le fotografie, le impronte digitali, nonché qualunque visto precedentemente rilasciato, annullato, revocato o prorogato.

Qualora la verifica dell'identità vada a buon fine, non è affatto chiaro per quale motivo il resto di tali dati sia ancora necessario. Questi dovrebbero in effetti solo essere resi accessibili, a condizioni restrittive, in caso di fallimento delle procedure di verifica. In tal caso, i dati citati all'articolo 16, paragrafo 2 contribuirebbero appositamente a una procedura di ripiego volta a stabilire l'identità della persona. Tali dati non dovrebbero pertanto essere accessibili a tutto il personale addetto ai controlli di frontiera, ma in modo più restrittivo solo ai funzionari incaricati di casi problematici.

Infine, la definizione delle autorità che hanno accesso dovrebbe essere più precisa. In particolare, non è chiaro chi siano «le autorità competenti ad effettuare controlli nell'ambito del territorio degli Stati membri». Il GEPD ritiene che si tratti delle autorità competenti ad effettuare controlli *sui visti*, e che l'articolo 16 debba essere modificato in tal senso.

3.7.3 *Uso dei dati ai fini dell'identificazione e del rimpatrio di immigrati clandestini, e delle procedure di asilo*

Nei casi descritti agli articoli 17, 18 e 19 (rimpatrio di immigrati clandestini e procedura di asilo), il VIS è utilizzato ai fini dell'identificazione. Tra i dati che possono essere utilizzati ai fini dell'identificazione vi sono le fotografie. Tuttavia, allo stato attuale della tecnologia connessa al riconoscimento facciale automatico per tali sistemi informatici su vasta scala, le fotografie non possono essere utilizzate per l'identificazione (uno fra molti, «one -to-many»); queste non possono garantire un risultato affidabile. Non devono pertanto essere considerate dati idonei ai fini dell'identificazione.

Pertanto, il GEPD suggerisce caldamente che le «fotografie» siano eliminate dalla prima parte di questi articoli e che siano mantenute nella seconda parte (le fotografie possono essere utilizzate quale strumento di verifica dell'identità di qualcuno, ma non per identificare in una base di dati su vasta scala).

Un'altra ipotesi sarebbe quella di modificare l'articolo 36 nel senso che le funzionalità di trattamento delle fotografie ai fini dell'identificazione saranno attuate solo quando questa tecnologia sarà considerata affidabile (eventualmente previo parere del comitato tecnico).

3.7.4 *Pubblicazione delle autorità che hanno accesso*

L'articolo 4 del progetto di regolamento prevede la pubblicazione nella Gazzetta ufficiale dell'Unione europea delle autorità competenti designate in ciascuno Stato membro ad avere accesso al VIS. Tale pubblicazione dovrebbe essere fatta su base periodica (annuale), al fine di informare delle modifiche apportate alle situazioni nazionali. Il GEPD sottolinea l'importanza di questa pubblicazione quale indispensabile strumento di controllo, a livello europeo nonché a livello nazionale o locale.

3.8 **Responsabilità**

Si rammenta che il VIS sarà basato su un'architettura centralizzata con una base di dati centrale dove saranno archiviate tutte le informazioni sui visti e le interfacce nazionali ubicate negli Stati membri che consentono alle proprie autorità competenti di accedere al sistema centrale. Secondo i considerando nn. 14 e 15 del progetto di regolamento, la direttiva 95/46/CE si applica al trattamento dei dati personali da parte degli Stati membri in applicazione del regolamento, e il regolamento(CE) n. 45/2001 si applica alle attività della Commissione in relazione alla tutela dei dati personali. Come citato nei suddetti considerando in questo contesto, la proposta è volta a precisare taluni punti, fra cui, per quanto attiene alle responsabilità in materia di utilizzazione dei dati e al controllo della protezione dei dati.

Infatti, questi punti sembrerebbero collegarsi ad alcuni dettagli importanti senza i quali il sistema delle garanzie di cui alla direttiva 95/46/CE e al regolamento 45/2001 non si applicherebbe o non sarebbe pienamente coerente con la proposta. L'applicabilità del diritto nazionale in conformità della direttiva ipotizza di norma un responsabile del trattamento che è stabilito in quello Stato membro (articolo 4), mentre l'applicabilità del regolamento dipende dal trattamento dei dati personali da parte di un'istituzione o di un organo comunitario nell'esercizio di attività le quali rientrano tutte o in parte nel campo di applicazione del diritto comunitario (articolo 3).

A norma dell'articolo 23, paragrafo 2 del progetto di regolamento, i dati saranno «trattati dal VIS a nome degli Stati membri». A norma dell'articolo 23, paragrafo 3 gli Stati membri designano l'autorità che dev'essere considerata quale la propria autorità di controllo ai sensi dell'articolo 2, lettera d) della direttiva 95/46/CE. Questo sembra suggerire che, secondo il sistema della direttiva, la Commissione dovrebbe essere considerata l'incaricato del trattamento. Ciò è confermato dalla spiegazione degli articoli. ([1])

Questo linguaggio tende a sottovalutare il ruolo estremamente importante e fondamentale svolto dalla Commissione, sia nella fase di sviluppo del sistema che nel corso del suo normale funzionamento. È difficile collegare esattamente il ruolo della Commissione al concetto di responsabile del trattamento o di incaricato del trattamento; si tratta o di un incaricato del trattamento con poteri inconsueti (fra cui la progettazione del sistema) o di un responsabile del trattamento con restrizioni (in quanto i dati sono inseriti e utilizzati dagli Stati membri). La Commissione svolge effettivamente quello che deve essere riconosciuto quale ruolo ([2]) *sui generis* nel VIS.

Tale ruolo significativo dovrebbe essere riconosciuto tramite una descrizione completa dei compiti svolti dalla Commissione, piuttosto che mediante una formulazione che non corrisponde affatto alla realtà, in quanto troppo restrittiva, non modifica niente nel funzionamento del VIS e ingenera solo confusione. Questo è altresì importante in vista di un controllo coerente ed efficace del VIS (vedasi anche il punto 3.11). Il GEPD raccomanda pertanto di sopprimere l'articolo 23, paragrafo 2.

Il GEPD intende inoltre evidenziare l'estrema importanza di una descrizione completa dei compiti svolti dalla Commissione in relazione al VIS, qualora la Commissione intenda affidare i compiti di gestione a un altro organo. La scheda finanziaria allegata alla proposta cita la possibilità di trasferire detti compiti all'Agenzia per le frontiere esterne. In tale contesto, è basilare che la Commissione non lasci incertezze quanto alla portata delle sue competenze, affinché il suo successore conosca i limiti entro cui poter agire.

3.9 **Sicurezza**

La gestione e il rispetto di un livello di sicurezza ottimale per il VIS rappresenta un presupposto per garantire la prevista tutela dei dati personali archiviati nella base di dati. Al fine di ottenere tale livello soddisfacente in materia di tutela, devono essere messe in atto opportune garanzie per gestire i potenziali rischi connessi all'infrastruttura del sistema e alle persone coinvolte. Tale argomento viene attualmente discusso in vari punti della proposta e necessita di alcune migliorie.

Gli articoli 25 e 26 della proposta contengono varie misure per la sicurezza dei dati e precisano i tipi di abusi da evitare. Tali disposizioni potrebbero tuttavia essere utilmente integrate da misure volte a controllare e a riferire in maniera sistematica sull'efficienza delle misure di sicurezza già menzionate. Il GEPD raccomanda più specificamente di aggiungere a questi articoli disposizioni sulla verifica sistematica delle misure di sicurezza.

Questo si collega all'articolo 40 della proposta, che prevede il monitoraggio e la valutazione. Ciò non dovrebbe solo riguardare gli aspetti legati ai risultati, ai costi-benefici e alla qualità del servizio, ma anche il rispetto delle prescrizioni di legge, soprattutto nel settore della tutela dei dati. Il GEPD raccomanda pertanto che il campo di applicazione dell'articolo 40 sia esteso al monitoraggio e all'elaborazione di relazioni sulla legalità del trattamento.

Inoltre, a integrazione dell'articolo 24, paragrafo 4, lettera c) o dell'articolo 26, paragrafo 2, lettera e) per quanto concerne il personale debitamente autorizzato che ha accesso ai dati, va aggiunto che lo Stato membro dovrebbe garantire la disponibilità di precisi profili degli utenti (che dovrebbero essere tenuti a disposizione delle autorità nazionali di controllo). Oltre a detti profili degli utenti, gli Stati membri devono redigere e tenere costantemente aggiornato un elenco completo delle identità degli utenti. Lo stesso si applica alla Commissione: l'articolo 25, paragrafo 2, lettera b) dovrebbe pertanto essere integrato in tal senso.

([1]) Vedasi la pagina 37 della proposta.

([2]) Sebbene la definizione di responsabile del trattamento nella direttiva 95/46/CE e nel regolamento n. 45/2001 preveda anche la possibilità di più responsabili del trattamento con competenze differenti.

Queste misure di sicurezza sono integrate dal monitoraggio e da garanzie organizzative. L'articolo 28 della proposta descrive le condizioni e le finalità per cui devono essere tenuti registri di tutte le operazioni di trattamento dei dati. Tali registri non saranno solo archiviati per monitorare la tutela dei dati e per garantire la sicurezza degli stessi dati ma anche per effettuare verifiche periodiche del VIS. Le relazioni di verifica contribuiranno all'effettiva esecuzione dei compiti svolti dalle autorità di controllo che saranno in grado di individuare i punti più deboli e di concentrarsi sugli stessi durante la procedura di verifica.

3.10 **Diritti delle persone interessate**

3.10.1 *Informazione delle persone interessate*

È della massima importanza fornire informazioni alle persone interessate per effettuare un trattamento leale. Rappresenta una garanzia indispensabile per i diritti della persona. L'articolo 30 della proposta segue essenzialmente l'articolo 10 della direttiva 95/46/CE per tale finalità.

Questa disposizione potrebbe, tuttavia, trarre vantaggio da alcune modifiche onde conformarsi meglio all'ambito del VIS. La direttiva prevede infatti che siano fornite alcune informazioni, ma autorizza, se del caso, ulteriori informazioni da dare. ([1]) L'articolo 30 dovrebbe pertanto essere modificato al fine di includervi i seguenti punti:

— le persone interessate dovrebbero essere altresì informate circa il periodo di conservazione che si applica ai loro dati;

— l'articolo 30, paragrafo 1, lettera e) riguarda «il diritto di accesso e di eventuale rettifica dei dati.» Sarebbe più preciso citare il «diritto di accesso e di eventuale *richiesta di* rettifica *o di cancellazione* dei dati». Al riguardo, le persone interessate dovrebbero essere informate della possibilità di chiedere consulenza o assistenza alle competenti autorità di controllo;

— infine, l'articolo 30, paragrafo 1, lettera a) cita le informazioni sull'identità del responsabile del trattamento o del suo rappresentante, qualora ve ne siano. Dato che il responsabile del trattamento è sempre stabilito nel territorio dell'Unione europea, non sussiste la necessità di prevedere quest'ultima possibilità.

3.10.2 *Diritto di accedere, rettificare e cancellare i dati*

L'articolo 31, paragrafo 1, ultima frase recita: «Tale accesso ai dati può essere accordato soltanto da uno Stato membro». Si può ipotizzare che questo significhi che l'accesso ai dati (o la loro comunicazione) non possa essere accordato dall'unità centrale, ma soltanto da uno Stato membro. Il GEPD raccomanda che sia reso esplicito che detta comunicazione può essere richiesta in qualsiasi Stato membro.

In aggiunta, la redazione di questa disposizione sembra implicare altresì che l'accesso non potrà essere rifiutato e che sarà dato senza l'autorizzazione dello Stato membro competente. Questo spiegherebbe perché le autorità nazionali debbono cooperare per applicare i diritti sanciti all'articolo 31, paragrafi 2, 3 e 4 ma non all'articolo 31, paragrafo 1 ([2]).

3.10.3 *Assistenza da parte delle autorità di controllo*

L'articolo 33, paragrafo 2 stabilisce che l'obbligo delle autorità di controllo nazionali di fornire assistenza e consulenza alla persona interessata sussista per tutta la durata del procedimento (dinanzi a un giudice). Il significato di questo paragrafo non è chiaro. Le autorità di controllo nazionali hanno differenti atteggiamenti verso il loro ruolo nel corso dei procedimenti giurisdizionali. Sembra come se le stesse autorità debbano svolgere il ruolo del procuratore legale del ricorrente dinanzi al giudice, il che non è possibile in molti paesi.

([1]) Esso cita: «*ulteriori informazioni (...) nella misura in cui, in considerazione delle specifiche circostanze in cui i dati vengono raccolti, tali informazioni siano necessarie per effettuare un trattamento leale nei confronti della persona interessata*».

([2]) Di conseguenza, l'articolo 31, paragrafo 3 relativo alla cooperazione fra le autorità nazionali nell'esercizio del diritto di rettificare o cancellare potrebbe essere modificato in tal senso, per maggiore chiarezza: qualora la richiesta *citata all'articolo 31, paragrafo 2*. Le richieste di cui all'articolo 31, paragrafo 1 (accesso) non implicano la cooperazione fra le autorità.

3.11 **Controllo**

La proposta ripartisce il compito di controllo fra le autorità di controllo nazionali e il GEPD. Questo è coerente con l'approccio della proposta al diritto applicabile e alle responsabilità per il funzionamento e l'uso del VIS e con l'esigenza di un controllo effettivo. Il GEPD accoglie pertanto favorevolmente tale approccio agli articoli 34 e 35.

Le autorità di controllo nazionali verificano la legalità del trattamento dei dati personali da parte degli Stati membri, *compresa la trasmissione da e verso il VIS*. Il GEPD controlla le attività della Commissione (...) *verificando altresì che i dati personali siano trasmessi legalmente tra le interfacce nazionali e il sistema centrale di informazioni visti*. Questo potrebbe tradursi in sovrapposizioni, in quanto sia l'autorità di controllo nazionale che il GEPD sono contemporaneamente responsabili del controllo della legalità della trasmissione dei dati tra le interfacce nazionali e il sistema centrale di informazioni visti.

Il GEPD suggerisce pertanto di modificare l'articolo 34 e precisare che le autorità di controllo nazionali verificano la legalità del trattamento dei dati personali da parte dello Stato membro, compresa la loro trasmissione da e verso l'interfaccia nazionale del VIS.

Per quanto concerne il controllo del VIS, è altresì importante sottolineare che le attività di controllo da parte delle autorità di controllo nazionali e del GEPD dovrebbero essere coordinate in una certa misura, al fine di garantire un livello sufficiente di coerenza e di efficacia globale. Infatti, sussiste l'esigenza di un'attuazione armonizzata del regolamento e di cooperazione verso un approccio generale dei problemi comuni. Inoltre, in materia di sicurezza, si può aggiungere che il livello di sicurezza del VIS sarà definito sostanzialmente dal livello di sicurezza dell'anello più debole. A tale riguardo anche la cooperazione fra il GEPD e le autorità nazionali deve essere strutturata e migliorata. L'articolo 35 dovrebbe pertanto contenere una disposizione in tal senso secondo cui il GEPD convoca, almeno una volta l'anno, una riunione con tutte le autorità di controllo nazionali.

3.12 **Attuazione**

L'articolo 36, paragrafo 2 della proposta prevede che: «*Le misure necessarie all'esecuzione tecnica delle funzionalità di cui al paragrafo 1 sono adottate conformemente alla procedura prevista all'articolo 39, paragrafo 2*.» L'articolo 39 fa riferimento ad un comitato che assiste la Commissione istituito nel dicembre 2001 ([1]) ed utilizzato in vari strumenti.

L'esecuzione tecnica delle funzionalità del VIS (le interazioni con le autorità competenti e il modello uniforme per i visti) presenta una serie di potenziali impatti critici sulla protezione dei dati. Per esempio, la scelta di inserire o meno un microchip nei visti che avrà un impatto sul modo in cui la banca dati centrale sarà utilizzata, nonché il formato del modello utilizzato per scambiare i dati biometrici che guiderà e delineerà la relativa politica in materia di protezione dei dati ([2]).

Questa selezione di tecnologie avrà un impatto determinante sulla corretta attuazione dei principi di scopo e proporzionalità e dovrebbe di conseguenza essere controllata. Pertanto le scelte tecnologiche con un impatto significativo sulla protezione dei dati dovrebbero essere fatte di preferenza tramite regolamento, in conformità della procedura di codecisione. Soltanto allora può essere esercitato il necessario controllo politico. In tutti gli altri casi con un impatto sulla protezione dei dati il GEPD dovrebbe avere la possibilità di esprimere suggerimenti riguardo alle scelte fatte da questo comitato.

3.13 **Interoperabilità**

L'interoperabilità è un presupposto fondamentale e vitale per l'efficienza dei sistemi informatici su vasta scala come il VIS. Offre la possibilità di ridurre il costo globale in maniera consistente e di evitare ridondanze naturali di elementi eterogenei. L'interoperabilità può inoltre contribuire all'obiettivo di una politica comune in materia di visti tramite l'attuazione della stessa procedura per tutti gli elementi costitutivi di questa politica. Tuttavia è fondamentale distinguere tra due livelli di interoperabilità:

— l'interoperabilità tra gli Stati membri dell'UE è fortemente auspicabile; effettivamente le domande di visto inviate dalle autorità di uno Stato membro devono essere interoperabili con quelle inviate dalle autorità di qualsiasi altro Stato membro;

([1]) Regolamento n. 2424/2001 del Consiglio del 6 dicembre 2001 sullo sviluppo del Sistema d'informazione Schengen di seconda generazione (SIS II).

([2]) La proposta di regolamento del Consiglio che modifica il regolamento (CE) n. 1683/95 (modello uniforme per i visti) del settembre 2003 includeva anche un articolo simile.

— l'interoperabilità tra sistemi creati per scopi differenti o con sistemi di paesi terzi è molto più discutibile.

Tra le salvaguardie disponibili utilizzate per limitare la finalità del sistema ed impedire la «funzione di scorrimento» (function creep), l'utilizzo di standard tecnologici differenti può contribuire a questa limitazione. Inoltre, qualsiasi forma di interazione tra due sistemi diversi dovrebbe essere attentamente documentata. L'interoperabilità non dovrebbe mai portare ad una situazione in cui un'autorità, non autorizzata all'accesso o all'utilizzo di taluni dati, possa ottenere tale accesso tramite un altro sistema di informazione.

In questo contesto il GEPD desidera fare riferimento alla dichiarazione del Consiglio del

25 marzo 2004 sulla lotta al terrorismo, in cui si chiede alla Commissione di presentare proposte per migliorare l'interoperabilità e le sinergie fra i sistemi d'informazione (SIS II, VIS ed Eurodac).

Egli desidera inoltre fare riferimento alla discussione in corso relativa all'organo a cui potrebbe essere affidata in futuro la gestione dei diversi sistemi su vasta scala (cfr. anche il punto 3.8 del presente parere). Il GEPD sottolinea nuovamente che l'interoperabilità dei sistemi non può essere attuata in violazione del principio di limitazione dello scopo e che dovrebbe essergli presentata qualsiasi proposta in materia.

4. **CONCLUSIONI**

4.1 **Punti generali**

1. Il GEPD riconosce che l'ulteriore sviluppo di una politica comune in materia di visti necessita di uno scambio efficiente dei dati pertinenti. Uno dei meccanismi che possono assicurare un regolare flusso di informazioni è il VIS. Il GEPD ha preso accuratamente atto delle prove presentate nella VIE. Sebbene queste prove non siano del tutto decisive, sembrano esserci ragioni sufficienti per giustificare l'istituzione del VIS con lo scopo di migliorare la politica comune in materia di visti.

   Comunque questo nuovo strumento dovrebbe essere limitato alla raccolta e allo scambio dei dati, nella misura in cui siano necessari allo sviluppo di una politica comune in materia di visti e proporzionati a tale obiettivo.

2. L'istituzione del VIS può avere conseguenze positive per altri interessi pubblici legittimi, pur tuttavia ciò non altera lo scopo del VIS. Pertanto tutti gli elementi del VIS devono essere strumenti necessari e proporzionati per raggiungere l'obiettivo sopra citato.

   Inoltre:

   — l'accesso sistematico da parte delle autorità di contrasto non sarebbe conforme con questo scopo;

   — il GEPD raccomanda che tale distinzione tra «scopo» e «benefici» sia resa più esplicita nel testo dell'articolo 1, paragrafo 2;

   — l'interoperabilità con altri sistemi non può essere attuata in violazione del principio di limitazione dello scopo.

3. Il GEPD riconosce i vantaggi dell'utilizzo dei dati biometrici ma sottolinea il notevole impatto dell'utilizzo di tali dati e propone l'inserimento di salvaguardie rigorose per l'utilizzo dei dati biometrici. Inoltre l'imperfezione tecnica delle impronte digitali richiede che siano sviluppate e inserite nella proposta procedure di ripiego.

4. Il presente parere dovrebbe essere menzionato nel preambolo del regolamento prima dei considerando («Visto il parere....»).

4.2 **Altri punti**

5. Riguardo ai motivi di rifiuto del visto: dovrebbe essere incluso nel testo della proposta un riferimento all'articolo 29 della direttiva 2004/58/CE per assicurare che «minaccia all'ordine pubblico sia compreso alla luce di quella disposizione».

6. I dati sui membri di un gruppo hanno un significato speciale nella proposta: pertanto dovrebbe essere prevista una definizione precisa e completa di «membri del gruppo.»

7. Non ci sono prove che la scelta politica che è stata fatta in questa proposta sul periodo di conservazione dei dati sia irragionevole o avrebbe conseguenze inaccettabili, a patto che siano attivati tutti i meccanismi di correzione opportuni.

   Inoltre la proposta dovrebbe indicare esplicitamente che i dati personali devono essere completamente riesaminati ad ogni nuova domanda di visto.

8. Riguardo al controllo dei visti alle frontiere esterne: l'articolo 16 della proposta dovrebbe essere modificato poiché un accesso esclusivo alla banca di dati centrale del VIS sarebbe sproporzionato in tali casi. È sufficiente un unico accesso da parte delle autorità competenti a svolgere il controllo dei visti al microchip protetto.

   Inoltre se l'identità è stata verificata, non è affatto chiaro per qual ragione la parte restante di questi dati sia ancora necessaria.

9. Riguardo all'utilizzo dei dati per l'identificazione e il rimpatrio di immigrati clandestini e per le procedure di asilo: «fotografie» dovrebbe essere rimosso dalla prima parte degli articoli 17, 18 e 19 e mantenuto nella seconda parte.

10. Riguardo alle responsabilità della Commissione e degli Stati membri: l'articolo 23, paragrafo 2, dovrebbe essere soppresso.

11. Dovrebbero essere aggiunte alla proposta disposizioni sull'(auto)verifica sistematica delle misure di sicurezza. Il campo di applicazione dell'articolo 40 deve essere esteso a monitorare e relazionare sulla liceità del trattamento dei dati. Inoltre:

   — un elenco completo delle identità degli utenti deve essere redatto e tenuto costantemente aggiornato da parte degli Stati membri. Lo stesso si applica alla Commissione: l'articolo 25, paragrafo 2, lettera b), dovrebbe pertanto essere completato nello stesso senso;

   — l'articolo 28 della proposta descrive le condizioni e i fini per cui devono essere registrate tutte le operazioni di trattamento dei dati. Queste registrazioni sono conservate non soltanto per controllare la protezione dei dati e per garantire la sicurezza dei dati ma anche per effettuare una autoverifica regolare del VIS.

12. Riguardo ai diritti delle persone cui si riferiscono i dati:

   — l'articolo 30 dovrebbe essere modificato per assicurare che le persone interessate debbano anche essere informate del periodo di conservazione applicabile ai loro dati;

   — l'articolo 30, paragrafo 1, lettera e), dovrebbe menzionare il diritto di accesso e il diritto di richiesta di rettifica o di cancellazione dei dati;

   — l'articolo 31, paragrafo 1, deve specificare esplicitamente che talune comunicazioni possono essere richieste in qualsiasi Stato membro.

13. Riguardo al controllo:

— l'articolo 34 dovrebbe essere modificato per chiarire che le autorità di controllo nazionali verificano la legalità del trattamento dei dati personali da parte dello Stato membro in questione, compresa la loro trasmissione da e verso l'interfaccia nazionale del VIS;

— l'articolo 35 dovrebbe pertanto contenere una disposizione che stabilisce che il GEPD convoca almeno una volta all'anno una riunione con tutte le autorità di controllo nazionali.

14. Riguardo all'attuazione:

— le scelte tecnologiche con un impatto significativo sulla protezione dei dati dovrebbero essere fatte di preferenza tramite regolamento, in conformità della procedura di codecisione;

— in altri casi, il GEPD dovrebbe avere la possibilità di esprimere suggerimenti riguardo alle scelte fatte dal comitato previsto dalla proposta.

Fatto a Bruxelles il 23 marzo 2005

Peter HUSTINX

Garante europeo della protezione dei dati