L'Agenzia è un organismo comunitario dotato di personalità giuridica. Ha un consiglio di amministrazione che è composto da un rappresentante di ogni Stato membro e da due rappresentanti della Commissione.

Norvegia, Islanda e Svizzera, paesi associati all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen, prendono parte alle attività dell'Agenzia, ciascuno con un rappresentante al consiglio di amministrazione. Regno Unito e Irlanda partecipano ma non votano.

L'Agenzia è diretta dal suo direttore esecutivo che è completamente indipendente nell'espletamento delle sue funzioni. Per raggiungere le sue finalità, l'Agenzia può cooperare con Europol, con le autorità competenti dei paesi terzi e con le organizzazioni internazionali specializzate in questo settore. Le entrate dell'Agenzia provengono da una sovvenzione comunitaria – che per il 2005 è stata di 6,2 milioni di euro – da un contributo dei paesi associati all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen, dai compensi per i servizi forniti e dai contributi volontari degli Stati membri.

Il regolamento finanziario applicabile all'Agenzia è adottato dal consiglio di amministrazione, previa consultazione della Commissione.

Entro tre anni dalla data in cui l'Agenzia ha assunto le proprie funzioni e successivamente ogni cinque anni, il consiglio di amministrazione ordina una valutazione esterna indipendente sull'attuazione del regolamento.

L'Agenzia ha assunto le proprie funzioni con decorrenza dal 1º maggio 2005, ma è diventata operativa solo dal 3 ottobre 2005.

La politica comunitaria nel settore delle frontiere esterne dell'Unione europea è finalizzata ad una gestione integrata che garantisca un livello elevato e uniforme di controllo delle persone e di sorveglianza, come prerequisito fondamentale per la creazione di uno spazio di libertà, sicurezza e giustizia.

Poiché gli Stati membri sono responsabili dell'attuazione, a livello operativo, di tali norme comuni, la politica comunitaria trarrebbe inevitabilmente vantaggio da un migliore coordinamento delle attività svolte dagli Stati membri in relazione al controllo e alla sorveglianza delle frontiere esterne.

Il piano per la gestione delle frontiere esterne degli Stati membri dell'Unione europea, concordato dal Consiglio il 13 giugno 2002, appoggiava la creazione di un organo comune di esperti in materia di frontiere esterne ai fini della gestione integrata delle frontiere esterne, organo che tuttavia presentava limiti strutturali per quanto riguarda il coordinamento della cooperazione operativa. L'istituzione dell'Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne, cui viene attribuita questa funzione di coordinamento, costituisce un passo avanti nella realizzazione della cooperazione operativa tra Stati membri.

Il programma dell'Aja adottato il 4 e 5 novembre 2004, ha previsto una serie di misure e di impegni al fine di migliorare la gestione della migrazione, aspetto strettamente connesso al controllo delle frontiere esterne, e tra le priorità d'azione individuate dalla Commissione per

rispondere alle sfide dell'immigrazione, dopo la riunione informale dei Capi di Stato e di Governo dell'Unione europea del 27 ottobre 2005 ad Hampton Court, sono attribuite all'Agenzia una serie di azioni a breve termine:

messa in opera, con la massima urgenza e a titolo prioritario, delle misure per la gestione delle frontiere, previste dal programma di lavoro del 2006, per combattere l'immigrazione clandestina nella regione del Mediterraneo, mediante progetti pilota e operazioni comuni;

presentazione al Consiglio, entro maggio 2006, di una relazione sull'analisi dei rischi in Africa;

preparazione nel 2006 di uno studio sulle possibilità di rafforzare il controllo e la sorveglianza del Mar Mediterraneo. Nello studio sarà valutata la fattibilità di una rete di pattuglie costiere del Mediterraneo.

Al fine di promuovere la realizzazione tempestiva della rete di pattuglie costiere, l'Agenzia darà vita a un progetto pilota per l'organizzazione e la gestione corrente di una rete di punti di contatto nazionali negli Stati membri per il controllo e la sorveglianza delle frontiere marittime esterne nel Mediterraneo. Parallelamente, l'Agenzia organizzerà insieme agli Stati membri alcuni progetti pilota finalizzati a migliorare il lavoro delle pattuglie costiere che controllano le frontiere marittime nell'Unione europea. Se l'esperienza si mostrerà positiva la rete potrebbe costituire la base per una struttura più permanente sotto il controllo dell'Agenzia che promuoverebbe la cooperazione tra le due sponde, quella orientale e quella occidentale, del Mar Mediterraneo. L'Unione europea dovrà esaminare la fattibilità tecnica della creazione di un sistema di sorveglianza che possa coprire tutto il Mar Mediterraneo e che fornisca gli strumenti necessari per individuare i casi di immigrazione clandestina e salvare vite umane dall'annegamento, in maniera tempestiva ed efficace.

2. Biometria e sistemi d'informazione.

2.1 Misure previste.

stabilire un insieme di misure per assicurare che i documenti di identità e i visti/permessi di soggiorno siano autentici e i loro proprietari corrispondano alle persone in questi indicate. Armonizzare a questo fine gli identificatori biometrici che saranno introdotti nei documenti (anche per i cittadini dell'Unione) e nei sistemi informativi dell'Unione e assicurare l'interoperabilità tra SIS II, VIS ed EURODAC;

assicurare l'attuazione del VIS entro i tempi stabiliti e l'inserimento nel sistema di dati alfanumerici e fotografie al più tardi entro il 2006, e dei dati biometrici al più tardi entro il 2007.

2.2 Legislazione in preparazione.

2.2.1 SIS II.

Il sistema di informazione Schengen (SIS) è un database comune europeo creato come misura compensativa in seguito all'abolizione dei controlli alle frontiere interne dell'aerea Schengen. Il sistema offre il supporto tecnico per effettuare i controlli alle frontiere e gli altri controlli di polizia e doganali, contribuendo ad attuare le disposizioni sulla libera circolazione delle persone e sulla cooperazione giudiziaria e di polizia in sede penale.

Il SIS è stato sviluppato secondo una configurazione hit/no-hit: tramite una procedura automatizzata di interrogazione, il sistema indica se una determinata persona o bene sono oggetto di una segnalazione e, in caso affermativo, le misure da adottare immediatamente. La configurazione attuale del sistema prevede che il SIS tratti esclusivamente i dati necessari a tal fine e che ogni ulteriore informazione supplementare debba essere ottenuta attraverso gli uffici SIRENE.

Attualmente, ogni Paese consulta e alimenta le informazioni inserite nel database centrale Schengen per il tramite del sistema Schengen nazionale, inoltre i sistemi nazionali non possono scambiare direttamente i dati, possono farlo soltanto tramite il sistema centrale.

Il SIS è una banca dati a carattere operativo: non può esistere una segnalazione nel SIS senza che questa sia presente nella banca dati SIS nazionale e d'altra parte non appena un dato viene revocato dalla banca dati nazionale, questo scompare anche da quella centrale.

Per quanto riguarda la situazione italiana, attualmente le forze di polizia (Carabinieri, Polizia di Stato, Guardia di Finanza, Polizia forestale e Polizia penitenziaria) nel momento in cui sono in possesso di un dato utile possono inserirlo immediatamente oltre che nel CED (Centro Elaborazione Dati, supporto informatico per l'attività operativa e investigativa delle forze di polizia) anche nella sezione nazionale della banca dati Schengen.

Il SIS di seconda generazione nasce dall'esigenza pratica di predisporre un sistema in grado di integrare i nuovi Stati membri nell'area Schengen, ma anche dalla volontà di disporre di uno strumento efficace e flessibile per attuare le politiche necessarie a istituire uno spazio di libertà, sicurezza e giustizia. Nella Comunicazione della Commissione al Consiglio e al Parlamento europeo « Sviluppo del Sistema di informazione Schengen II e possibili sinergie con un futuro Sistema di informazione visti », 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 ». L'introduzione di nuove funzionalità è stata sempre ritenuta prioritaria dalla Commissione che ha altresì considerato possibile che in un futuro prossimo il SIS diventi, oltre a un sistema d'informazione, anche un sistema d'indagine.

Il SIS II, elaborato come struttura intergovernativa, sarà trasformato in un classico strumento legislativo europeo entro giugno 2006. Entro dicembre 2006 gli Stati membri dovranno aver predisposto le basi tecniche per garantire l'adeguamento dell'interfaccia nazionale e nel marzo 2007 è infine prevista la messa in funzione e l'allaccio su base europea.

Base giuridica.

Il quadro giuridico di riferimento riveste particolare importanza poiché definisce e specifica le finalità del sistema.

Il protocollo allegato al Trattato di Amsterdam ha integrato l'*acquis* di Schengen, e di conseguenza anche il SIS, nell'ambito dell'Unione europea.

Il Consiglio, con la decisione 1999/436/CE, ha individuato nei trattati la base giuridica per ciascuna delle disposizioni o decisioni che costituiscono l'*acquis* di Schengen, senza tuttavia giungere a una decisione univoca per le disposizioni relative al SIS. Di conseguenza, le disposizioni relative al SIS in materia di cooperazione di polizia e giudiziaria in materia penale sono considerate atti fondati sul titolo VI del Trattato UE mentre le disposizioni relative al SIS in materia di visti, immigrazione e libera circolazione delle persone si basano sul titolo IV del Trattato CE.

Il 1º giugno 2005 la Commissione europea ha presentato tre proposte relative al SIS II:

1) una proposta di regolamento sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione-SIS II (COM(2005) 236) definitivo), che contiene le disposizioni che stabiliscono quali autorità hanno accesso al SIS II in materia di frontiere esterne, visti, asilo e immigrazione e la definizione delle norme che incidono sulla politica dei controlli alle frontiere esterne, con particolare riguardo alle segnalazioni possibili;

2) una proposta di regolamento sull'accesso al sistema d'informazione Schengen di seconda generazione-SIS II dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (COM(2005)237 definitivo);

3) una proposta di decisione sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione-SIS II (COM(2005) 230 definitivo) in materia di cooperazione operativa tra le autorità competenti degli Stati membri per la prevenzione e l'individuazione dei reati e che disciplina la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle informazioni pertinenti. La proposta contiene pertanto disposizioni in materia tese ad agevolare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione al procedimento penale e all'esecuzione delle decisioni penali.

Struttura.

Il SIS II consiste di un database centrale denominato Sistema centrale d'informazione Schengen (C-SIS) per il quale la Commissione assicurerà la connessione a punti d'accesso nazionali definiti da ogni Stato membro (N-SIS). Le autorità SIRENE assicureranno lo scambio di tutte le informazioni supplementari (informazioni connesse alle segnalazioni SIS II ma non immagazzinate nel SIS II).

Gli Stati membri forniranno al SIS II i dati relativi a:

persone ricercate in vista dell'arresto, della consegna o dell'estradizione;

persone ricercate nell'ambito di procedimenti giudiziari;

persone poste sotto sorveglianza o soggette a determinati controlli;

cittadini di paesi terzi ai fini della non ammissione;

dati relativi a oggetti a fini di sequestro o di prova.

La Commissione è responsabile della gestione operativa del SIS II, ovvero della manutenzione e degli sviluppi tecnici necessari per un buon funzionamento del sistema.

Nuove caratteristiche.

Il SIS II sviluppa nuove caratteristiche. Fra queste:

accesso allargato a Europol, Eurojust, ai servizi competenti negli Stati membri per il rilascio delle carte di circolazione, nonché alle autorità nazionali competenti per l'esame delle domande di asilo e a quelle competenti per il riconoscimento e la revoca dello status di rifugiato e infine alle autorità competenti per eseguire una decisione di rimpatrio o un provvedimento di allontanamento;

connessioni fra segnalazioni, ovvero, al momento della loro introduzione gli Stati membri, secondo il loro diritto interno, potranno creare connessioni fra due o più segnalazioni;

dati biometrici quali impronte digitali e fotografie;

l'interoperabilità fra sistemi d'informazione (SIS II, VIS ed Eurodac);

maggiori garanzie contro il reato dell'usurpazione dell'identità.

Parere del Garante europeo per la protezione dei dati.

Il parere prende in esame le proposte concernenti il SIS II analizzando quali possibili modifiche esse comportino rispetto alla natura del sistema.

Il Garante valuta che la trasformazione di uno strumento intergovernativo in norma europea possa generare conseguenze positive quali l'approfondimento della valutazione legislativa delle regole governanti il SIS e il coinvolgimento, finora modesto, del Parlamento europeo nel processo legislativo. Infine, in tal modo la Corte di

Giustizia diverrà competente per l'interpretazione delle questioni connesse agli strumenti riferiti al primo pilastro.

Il Garante ritiene inoltre che la parte dedicata alla protezione dei dati migliori di molto la situazione odierna, in particolare saluta con soddisfazione la misura in favore delle vittime dell'usurpazione dell'identità, l'estensione del Regolamento 45/2001 alle attività di trattamento dati della Commissione relativamente al Titolo IV e la migliore definizione degli obiettivi e condizioni delle segnalazioni ai fini della non ammissione.

Al di là dell'apprezzamento d'insieme vengono però espresse riserve di non poco rilievo, prima fra tutte quella riferita alle diverse basi giuridiche. Il Garante sottolinea che l'uso combinato di strumenti legislativi diversi rende difficile garantire un'applicazione uniforme a fronte di normative nazionali in materia non omogenee, sottolineando il rischio di difformità su aspetti anche fondamentali. In tal senso ribadisce che l'applicazione di diversi strumenti legislativi, inevitabile nella struttura normativa europea, non debba avere come conseguenza differenti livelli di protezione dei dati a seconda della loro tipologia. Considerata la complessità proposta, in grado di generare confusione nell'applicazione pratica (incertezze nell'attribuzione di competenze fra Stati membri e Commissione), il Garante ritiene utile lo sviluppo di un vademecum contenente il catalogo di tutte le norme esistenti in relazione al SIS II e alla loro applicabilità gerarchica e di un memorandum esplicativo in grado di chiarire i punti diversamente interpretabili. Il Garante sottolinea che la chiarezza, oltre ad essere un elemento fondamentale per il buon funzionamento del sistema, è anche un requisito base per assicurarne un controllo completo ed efficace.

A tal fine ritiene utile riflettere sulla possibilità di verificare e valutare l'impatto sulla privacy del SIS II, considerando ininfluente il fatto che la prima versione del sistema sia già in funzione, vista la diversità fra la prima e la seconda versione e l'introduzione di nuove categorie di dati quali quelli biometrici.

Il Garante rileva inoltre che le proposte definiscono la segnalazione (*alert*) come un insieme di dati che permette alle autorità nazionali competenti di identificare un individuo o un oggetto in vista di una linea di condotta specifica da seguire. In tal senso il SIS II ha ancora la struttura di un sistema hit-no hit, in cui ogni segnalazione è inserita per uno scopo specifico e a cui le autorità nazionali competenti hanno accesso in quanto motivate da un'azione specifica. Alcune categorie di accessi previsti dalle proposte non sembrano però seguire tale logica in quanto forniscono alle autorità informazioni utilizzabili senza però dare loro la possibilità di intraprendere azioni specifiche. È quanto il Garante lamenta rispetto all'accesso all'insieme dei dati sull'immigrazione da parte delle autorità nazionali competenti in materia di asilo e di status di rifugiato. Tale situazione sembra ripresentarsi per l'accesso di Europol alle segnalazioni sull'estradizione, la sorveglianza discreta e gli oggetti rubati e con l'accesso da parte di Eurojust all'insieme di dati sull'estradizione. Il Garante sottolinea che in tal modo le finalità previste del sistema passano da informative a investigative senza che tale passaggio sia stato accompagnato da un adeguato livello di protezione e riflessione.

Il Garante ribadisce infine che ulteriori accessi dovrebbero essere concessi solo in presenza di validi motivi e limitati sia rispetto alle categorie di dati accessibili che ai soggetti autorizzati.

Parere dell' Autorità di Controllo Comune Schengen (ACC) sulle basi giuridiche proposte per il SIS II.

L'ACC è un'autorità indipendente prevista dall'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen al fine di esercitare il controllo dell'unità di supporto tecnico del Sistema d'Informazione Schengen. Essa è composta da due rappresentanti di ciascuna autorità nazionale di controllo per la protezione dei dati ed è altresì competente ad analizzare le difficoltà di applicazione o di interpretazione che possono sorgere dall'utilizzazione del Sistema d'Informazione Schengen, a studiare i problemi che possono presentarsi nell'esercizio del controllo indipendente effettuato dalle autorità di controllo nazionali delle Parti contraenti ovvero nell'esercizio del diritto di accesso al Sistema, nonché ad elaborare proposte armonizzate allo scopo di trovare soluzioni comuni ai problemi esistenti. Il controllo è esercitato conformemente alle disposizioni della Convenzione Schengen e della Convenzione 108 del Consiglio d'Europa.

L'ACC sottolinea come le proposte non indichino chiaramente un responsabile del trattamento dati per il SIS II; esse infatti si limitano a definire la Commissione come responsabile della gestione operativa del sistema. Rileva dunque, che, poiché i dati trattati dal SIS II ricadono nel primo e terzo pilastro, in linea teorica, è possibile individuare come responsabili del trattamento dati sia la Commissione che le autorità competenti degli Stati membri, ma lamenta che la base giuridica non chiarisca sufficientemente la ripartizione di responsabilità e competenze.

La convenzione Schengen ha previsto un sistema di controllo e di protezione dei dati distinguendo tra un controllo nazionale e un controllo dell'unità centrale SIS da parte dell'Autorità comune di controllo. Nella base giuridica proposta per il SIS II, trattamento e controllo a livello nazionale rimangono identici a quanto proposto per il SIS, mentre per quanto riguarda il controllo dell'architettura tecnica del SIS II le proposte prevedono che il Garante europeo per la protezione dei dati controlli che le attività di trattamento dati effettuate dalla Commissione siano conformi con quanto disposto dalle proposte di decisone e di regolamento. L'ACC giudica tale approccio riduttivo poiché disconosce l'importanza di un controllo comune esercitato in maniera condivisa dalle autorità nazionali competenti attraverso l'Autorità di controllo comune, alla quale in ultimo non viene riconosciuto lo stesso ruolo attribuito dalla Convenzione Schengen. Tale ruolo viene sostituito con la previsione di una generica reciproca cooperazione che il Garante europeo è tenuto a sollecitare convocando almeno una volta l'anno una riunione comune delle autorità nazionali preposte.

L'ACC rileva inoltre come il requisito di configurare un sistema flessibile di natura indefinita possa condurre a una « deriva funzio-

nale », nel senso che le richieste provenienti da un'ampia gamma di organismi ed enti possono dare luogo a una situazione per cui le informazioni detenute nel sistema vengano utilizzate per scopi diversi da quelli inizialmente previsti. In tal senso l'ACC ritiene che prima di rendere operativa la previsione che il SIS II consenta la « interconnessione » delle segnalazioni presenti nel sistema, sia necessario prevedere il quadro giuridico di riferimento poiché proprio l'interconnessione delle segnalazioni potrebbe permettere agli utenti di accedere a informazioni per le quali non sono abilitati. Pertanto, l'ACC sottolinea come urgente la necessità di prevedere garanzie atte ad assicurare che l'interconnessione di segnalazioni non modifichi i diritti di accesso in essere rispetto alle singole categorie di segnalazioni.

L'ACC inoltre ribadisce che vi può essere la possibilità che il SIS II, incorporando nuove categorie di dati, duplichi sistemi di informazione già esistenti in ambito UE. In tal senso ritiene indispensabile 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. A tale proposito, l'ACC ricorda che l'articolo 94 della Convenzione Schengen prevede che « la Parte contraente che fornisce la segnalazione verifica se l'importanza del caso giustifica il suo inserimento nel Sistema d'Informazione Schengen », e auspica che tale previsione venga inserita nelle norme regolanti il SIS II.

2.2.2 VIS

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.

Nel giugno 2004 una decisione del Consiglio ha avviato il processo istitutivo del sistema d'informazione visti fornendo la base giuridica per la sua iscrizione nel bilancio dell'UE, comprese le misure preparatorie necessarie per l'introduzione degli elementi biometrici nella banca dati, definendo l'architettura del VIS e conferendo alla Commissione il mandato di sviluppare il sistema VIS a livello tecnico, assistita dal comitato SIS II (istituito dall'articolo 5, paragrafo 1 del regolamento (CE) n. 2424/2001 sullo sviluppo del Sistema d'informazione Schengen di seconda generazione – SIS II), mentre le interfacce nazionali saranno adattate o sviluppate dagli Stati membri.

Nel febbraio 2005 il Parlamento europeo e il Consiglio hanno presentato una proposta di regolamento concernente il VIS e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata. La proposta definisce lo scopo, le funzionalità e le competenze del VIS e conferisce alla Commissione il mandato di istituire e gestire la banca dati nonché di stabilire le procedure e le condizioni per lo scambio dei dati fra gli Stati membri. I dati che dovranno essere inseriti nel VIS comprendono dati alfanumerici e fotografie, ma anche le impronte digitali dei richiedenti al fine di garantire l'esattezza della verifica e dell'individuazione.

La proposta tiene conto degli orientamenti per lo sviluppo del VIS adottati dal Consiglio il 19 febbraio 2004 nonché dei risultati di una

valutazione approfondita di impatto affidata alla Commissione, che ha stimato che l'inserimento dei dati biometrici nella banca dati sia attualmente la soluzione più idonea per migliorare la politica comune in materia di visti.

Il VIS agevolerà i controlli alle frontiere esterne e all'interno degli Stati membri, l'applicazione del regolamento « Dublino » volto a determinare lo Stato membro competente per l'esame di una domanda d'asilo e l'individuazione e il rimpatrio degli immigranti illegali.

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 un'autorità centrale nazionale collegata all'interfaccia nazionale attraverso la quale le rispettive autorità competenti avranno accesso al CS-VIS.

La proposta prevede l'introduzione dei dati biometrici nel corso della procedura di presentazione della domanda e la registrazione dei medesimi nella base di dati centrale, dove saranno conservati per un periodo di cinque anni. La proposta elenca altresì le autorità competenti, diverse dalle autorità competenti per i visti, abilitate ad accedere al VIS (autorità competenti in materia di controlli alle frontiere esterne e all'interno del territorio degli Stati membri, autorità competenti in materia di immigrazione e autorità competenti in materia di asilo) e definisce i diritti di accesso loro attribuiti.

La proposta contiene una sezione dedicata alla protezione dei dati in cui sono definiti i ruoli delle autorità nazionali e del Garante europeo della protezione dei dati – GEPD.

A tale proposito, il Garante europeo della protezione dei dati, nel parere del 23 marzo del 2005 sulla proposta di regolamento, pur indicando che l'ulteriore sviluppo della politica comune in materia di visti richiede uno scambio efficace di dati pertinenti e che uno dei meccanismi capaci di assicurare una trasmissione fluida di informazioni possa essere individuato nel VIS, sottolinea che 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.

Rispetto all'introduzione di elementi biometrici, il GEPD riconosce i vantaggi legati al loro uso, sottolineandone tuttavia il notevole impatto e proponendo l'introduzione di salvaguardie rigorose circa il loro utilizzo, lamenta altresì come l'introduzione nel sistema delle impronte digitali, vista la poca chiarezza e difficoltà di lettura del dato, richieda ulteriori approfondimenti.

Il GEPD rileva inoltre che l'accesso sistematico da parte delle autorità di contrasto nazionali non appare conforme con le finalità dichiarate del sistema, che a suo parere andrebbero ulteriormente chiarite, anche relativamente alla prevista interoperabilità con altri sistemi, la quale, ribadisce il GEPD, non può essere attuata in violazione del principio di limitazione dello scopo.

Ulteriori rilievi sono contenuti nel parere sulla proposta di regolamento formulato dal Gruppo che riunisce i Garanti Europei, Gruppo

ex articolo 29, del 27 giugno 2005. Nel parere, i Garanti europei hanno a loro volta confermato l'apprezzamento per gli impegni che la Commissione ha assunto nei mesi scorsi nel dialogo diretto tenuto con le autorità di protezione dei dati, evidenziando però i rischi che potrebbero derivare dall'inserimento di una grande quantità di dati personali, anche di nuova generazione come quelli biometrici, in un database centralizzato che prevede uno scambio di dati su larga scala e che può riguardare un enorme numero di persone. I Garanti, pertanto, chiedono che vengano svolti alcuni approfondimenti, e che vengano in particolare specificate chiaramente ed esaustivamente le finalità del trattamento dei dati contenuti nel VIS in rapporto alla politica comune dei visti che ne costituisce il fondamento giuridico; che siano stabiliti tempi di conservazione limitati e proporzionati (attualmente previsti in cinque anni); che siano definite con precisione le autorità abilitate a introdurre dati nel VIS così come a modificarli e cancellarli, anche su richiesta dell'interessato; che vengano individuati gli organismi che possono accedere al sistema (in particolare con riguardo alle previste interconnessioni con il sistema informativo SIS II) e che vengano meglio definite le funzioni di controllo e supervisione da parte delle Autorità di protezione dei dati personali.

2.2.3 Proposta di decisione quadro del Consiglio sullo scambio di informazioni in virtù del principio di disponibilità.

Conformemente al programma dell'Aia, la proposta intende migliorare lo scambio di informazioni fra gli Stati membri ai fini delle attività di contrasto, eliminando l'incertezza dei meccanismi di scambio tradizionali, basati sull'applicazione del diritto dello Stato membro richiesto, e combinando reciproco riconoscimento e accesso equivalente alle informazioni necessarie ai fini della prevenzione, dell'individuazione e dell'investigazione dei reati prima che inizi il procedimento giudiziario. Alle autorità competenti degli Stati membri e ai funzionari di Europol verrà pertanto garantito l'accesso diretto on line alle informazioni disponibili e ai dati di indice per le informazioni non accessibili direttamente on line. La proposta privilegia i canali diretti e prevede l'obbligo della risposta.

I tipi di informazioni ai sensi della decisione, includono i profili del DNA, le impronte digitali, la balistica, le informazioni sull'immatricolazione dei veicoli, e ulteriori dati contenuti anche nei registri civili.

Nella relazione presentata dalla Commissione, tra le disposizioni vigenti nel settore della proposta, viene inserito l'accordo di Prüm e vengono inoltre indicate le similitudini tra questo e la proposta di decisione.

2.2.4 Proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.

La proposta di decisione disciplina lo scambio dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia

penale, in conformità del principio di disponibilità delle informazioni garantito dal programma dell'Aia, rafforzando la fiducia reciproca delle autorità competenti e garantendo che le informazioni siano protette in modo da escludere qualsiasi intralcio alla cooperazione pur nel pieno rispetto dei diritti fondamentali dell'individuo. L'introduzione del principio di disponibilità è pertanto subordinato all'introduzione di un nuovo strumento giuridico per la protezione dei dati nell'ambito del terzo pilastro.

La proposta definisce il procedimento per l'adozione delle misure necessarie per valutare il livello della protezione dei dati in un Paese terzo od organismo internazionale, introducendo norme comuni sulla riservatezza e sicurezza del trattamento, sulla responsabilità e le sanzioni anche penali per le violazioni particolarmente gravi e intenzionali nonché sui ricorsi giurisdizionali. Vengono altresì sollecitate autorità nazionali di controllo forti ed efficienti in grado di contribuire alla trasparenza dei trattamenti effettuati.

2.3 Legislazione.

2.3.1 Direttiva del Consiglio 2004/82/CE del 29 aprile 2004 concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

La Direttiva del Consiglio 2004/82/CE del 29 aprile 2004 concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate impone ai vettori obblighi complementari a quelli stabiliti a norma dell'articolo 26 della convenzione di Schengen(2), integrati a

---

(2) Riportiamo di seguito l'articolo 26 della Convenzione di Schengen:

1. Fatti salvi gli obblighi derivanti dalla loro adesione alla Convenzione di Ginevra del 28 luglio 1951 relativa allo status dei rifugiati, quale emendata dal Protocollo di New York del 31 gennaio 1967, le Parti contraenti si impegnano ad introdurre nelle rispettive legislazioni nazionali le seguenti regole:

a) se ad uno straniero viene rifiutato l'ingresso nel territorio di una Parte contraente, il vettore che lo ha condotto alla frontiera esterna per via aerea, marittima o terrestre è tenuto a prenderlo immediatamente a proprio carico. A richiesta delle autorità di sorveglianza della frontiera, egli deve ricondurre lo straniero nel Paese terzo dal quale è stato trasportato, nel Paese terzo che ha rilasciato il documento di viaggio in suo possesso durante il viaggio o in qualsiasi altro Paese terzo in cui sia garantita la sua ammissione;

b) il vettore è tenuto ad adottare ogni misura necessaria per accertarsi che lo straniero trasportato per via aerea o marittima sia in possesso dei documenti di viaggio richiesti per l'ingresso nei territori delle Parti contraenti.

2. Fatti salvi gli obblighi derivanti dalla loro adesione alla Convenzione di Ginevra del 28 luglio 1951 relativa allo status dei rifugiati, quale emendata dal Protocollo di New York del 31 gennaio 1967, e nel rispetto del proprio diritto costituzionale, le Parti contraenti si impegnano ad istituire sanzioni nei confronti dei vettori che trasportano per via aerea o marittima, da un Paese terzo verso il loro territorio, stranieri che non sono in possesso dei documenti di viaggio richiesti.

3. Le disposizioni del paragrafo 1, lettera *b)* e del paragrafo 2 si applicano ai vettori di gruppi che effettuano collegamenti stradali internazionali con autopullman, ad eccezione del traffico frontaliero.

sua volta dalla direttiva 2001/51/CE del Consiglio. Gli obblighi previsti hanno l'obiettivo di controllare i flussi migratori e di combattere l'immigrazione clandestina, nonché di intensificare i controlli relativi alla lotta al terrorismo.

La direttiva naturalmente tiene conto delle disposizioni della direttiva 95/46/CE riguardante il trattamento dei dati personali e la libera circolazione degli stessi e definisce legittimo l'utilizzo dei dati dei passeggeri, trasmessi durante le procedure di controllo alle frontiere, anche come mezzi probatori in procedimenti derivanti dall'applicazione della normativa in materia di ingresso e immigrazione, da quella relativa alla tutela dell'ordine pubblico e della sicurezza nazionale, mentre introduce una previsione di sanzione in caso di uso dei dati in contrasto con tale obiettivi.

La direttiva prevede che i dati relativi alle persone trasportate(3) debbano essere trasmessi anticipatamente dai vettori alle competenti autorità nazionali.

Nel caso di mancata o incompleta trasmissione, gli Stati membri possono adottare nei confronti dei vettori inadempienti sanzioni dissuasive, effettive e proporzionate.

Il meccanismo previsto è molto semplice: i vettori trasmettono in via elettronica i dati personali dei passeggeri che oltrepassano una frontiera esterna dell'Unione alle autorità incaricate dallo Stato membro di effettuare i controlli delle persone alle frontiere esterne. Queste salvano i dati ricevuti in un file provvisorio che, a meno che i dati non siano necessari per l'esercizio di funzioni regolamentari previste, sarà cancellato entro 24 ore.

Gli Stati membri sono inoltre vincolati ad adottare tutte le misure necessarie per costringere i vettori a informare i passeggeri di quanto avviene dei loro dati.

L'articolo 7 stabilisce che gli Stati membri adottino tutte le misure necessarie per conformarsi alla direttiva entro il 5 settembre 2006.

2.4 Accordi.

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

Dal 5 marzo 2003, per motivi di sicurezza e di protezione del loro territorio, le Autorità Statunitensi richiedono ai vettori che operano voli da, per, o attraverso gli Stati Uniti d'America, di fornire, all'Ufficio Statunitense delle dogane e della protezione delle frontiere (United

---

(3) Le informazioni indicate sono: numero e tipo di documento di viaggio; cittadinanza; nome completo e data di nascita; valico di frontiera di ingresso nel territorio degli Stati membri; numero del trasporto; ora di partenza e di arrivo del mezzo di trasporto; numero complessivo di passeggeri trasportato; primo punto di imbarco.

States Bureau of Customs and Border Protection – US CBP), l'accesso elettronico ai dati relativi ai passeggeri.

I vettori che non adempiono a tali richieste possono incorrere in pesanti sanzioni e addirittura perdere il diritto di atterrare negli Stati Uniti d'America.

Il trasferimento dei dati dei passeggeri alle Autorità Statunitensi è dunque una condizione per operare servizi di trasporto aereo da, per o attraverso il territorio USA.

L'11 maggio 2004 la Comunità Europea e gli Stati Uniti d'America hanno siglato un accordo 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 d'America, poi approvato con la Decisione 2004/496/CE del 17 maggio 2004.

Precedentemente, in base agli specifici impegni assunti dagli Stati Uniti d'America con tale accordo circa il livello di protezione assicurato dalle Autorità Statunitensi ai dati contenuti nelle prenotazioni provenienti dall'Unione Europea, la Commissione Europea, con Decisione 2004/535/CE del 14 maggio 2004, aveva stabilito che tale Stato soddisfa i requisiti di protezione dei dati personali richiesti dalla normativa europea in tema di privacy – Direttiva 95/46/CE del 24 ottobre 1995 – per potere effettuare il loro trasferimento verso un Paese extra Ue come gli Stati Uniti d'America.

L'accordo prevede che lo US CBP abbia accesso ai PNR (Passenger Name Record, ovvero ai dati del cliente registrati all'atto della prenotazione di un viaggio aereo) riguardanti i voli operati da, per o attraverso gli Stati Uniti d'America.

I PNR sono file elettronici creati nei sistemi informatici usati dai vettori per ogni itinerario prenotato dal passeggero. Essi contengono informazioni di varia natura (nome del passeggero, contatto telefonico dello stesso, data del volo, origine e destinazione, numero del posto a bordo, numero dei bagagli, indicazione dell'agenzia di viaggio eventualmente coinvolta, forma di pagamento e ogni ulteriore informazione fornita dal passeggero in fase di prenotazione). I dati sono intercettati dallo US CBP all'interno dei sistemi di prenotazione fino a 48 ore prima della partenza del volo e utilizzati per operare controlli dei passeggeri prima del loro arrivo sul territorio USA, con lo scopo di facilitare l'ingresso della maggior parte dei viaggiatori, focalizzando le risorse dello US CBP stesso solo su quel numero ristretto di passeggeri che potrebbe costituire un rischio reale per la sicurezza.

Lo US CBP, che è parte del ministero della Sicurezza interna, Department of Homeland Security, ha accesso ai dati per finalità di prevenzione e lotta contro il terrorismo e gli atti criminali gravi.

Secondo quanto previsto dalla legislazione statunitense, lo US CBP può trasmettere ad altre autorità i dati in suo possesso se questi vengono utilizzati per finalità connesse alla lotta al terrorismo o in osservanza di obblighi di legge ma, comunque, solo dopo una valutazione caso per caso.

Tali dati possono inoltre essere resi disponibili, quando necessario, per la protezione dell'interesse vitale dei passeggeri o di terze persone

(in particolare nei casi di importanti rischi sanitari) o nell'ambito di procedimenti penali.

I dati sono conservati per 7 anni, ma, nei casi in cui in tale periodo venga effettuato un accesso manuale agli stessi, essi possono essere conservati per ulteriori 8 anni.

Le Autorità Statunitensi si sono impegnate a consegnare ai passeggeri che ne facciano richiesta una copia dei dati intercettati nel PNR e contenuti nei loro database. I passeggeri possono altresì richiedere la rettifica dei loro dati ed ottenerla laddove lo US CBP o la Transport Security Agency (TSA) la considerino giustificata e adeguatamente argomentata.

Una decisione negativa potrà, peraltro, formare oggetto di impugnativa giudiziale.

Opposizione del Parlamento europeo alla conclusione dell'Accordo.

Il Parlamento europeo il 27 luglio 2004 ha proposto dinanzi alla Corte di Giustizia delle Comunità europee (Causa C-317/04) un ricorso contro il Consiglio dell'Unione europea. Il Parlamento ha chiesto che la Corte annulli la decisione del Consiglio del 17 maggio 2004 (2004/496/CE), poiché ritiene che l'articolo 95 CE non giustifichi la competenza della Comunità a concludere l'accordo, in quanto esso riguarda il trattamento di dati esclusi dall'ambito di applicazione della direttiva 95/46 sulla tutela dei dati personali e che dunque l'accordo implicherebbe la modifica di tale direttiva.

Il Parlamento sostiene che l'accordo è stato concluso in violazione dei diritti fondamentali, in particolare in violazione dell'articolo 8 della Convenzione europea sulla salvaguardia dei diritti dell'uomo, costituendo un'ingerenza nella vita privata dei singoli e che esso altresì non terrebbe conto del principio di proporzionalità poiché prevede il trasferimento di una quantità eccessiva di dati dei passeggeri, conservati troppo a lungo dalle autorità statunitensi. Infine, il Parlamento ritiene che la procedura che ha portato alla firma dell'accordo non sia stata trasparente e conforme al diritto e alla procedura attraverso le quali il Parlamento europeo da il proprio consenso agli accordi internazionali.

La Corte con un ordinanza del 17 marzo 2005 ha provveduto che il Garante europeo della protezione dei dati sia ammesso a intervenire nel procedimento C-317/04 a sostegno delle conclusioni del Parlamento europeo e si è riservato di stabilire un termine affinché quest'ultimo possa esporre le proprie argomentazioni.

L'11 novembre 2005, l'avvocato generale Philippe Léger ha proposto alla Corte di giustizia europea di annullare, per mancanza di una base giuridica adeguata, la decisione della Commissione del 14 maggio 2004 e quella del Consiglio del 17 maggio. La Corte si pronuncerà sul merito del caso nella primavera 2006.

2.5 Accordi in preparazione.

2.5.1 Proposta di decisione del Consiglio relativa alla conclusione di un accordo tra la Comunità europea e il governo del Canada sul trattamento di informazioni anticipate sui passeggeri (API) e dei dati delle pratiche dei passeggeri (PNR).

Sulla proposta presentata il 19 maggio 2005, il Parlamento europeo si è pronunciato con la risoluzione A6-0226/2005 con la quale respinge la conclusione dell'accordo.

Tale posizione, motivata con l'opportunità di attendere la sentenza della Corte di giustizia delle Comunità europee in merito all'accordo USA/CE, riconosce tuttavia che il negoziato con le autorità canadesi rappresenta un equilibrio accettabile tra le esigenze di libertà e quelle di sicurezza del Paese terzo. Il Parlamento ribadisce comunque di essere stato consultato all'ultimo momento e senza essere in possesso di tutte le informazioni necessarie.

3. Politica in materia di visti.

La politica in materia di visti si lega strettamente alle questioni connesse con l'ingresso degli stranieri nel territorio comunitario e quindi in linea generale alle politiche relative all'immigrazione.

Le misure previste sono state adottate in base al Titolo VI TUE, all'*acquis* di Schengen e al Titolo IV CE. Risulta pertanto di estrema difficoltà fornire un quadro esauriente delle misure adottate in tale settore.

Limitandoci alla normativa discendente dall'*acquis* di Schengen, da sottolineare che essa ha introdotto il limite fondamentale, sia per la concessione dei visti che dei permessi di soggiorno, della segnalazione ai fini della non ammissione: decisione fondata sulla circostanza che la presenza dello straniero nel territorio nazionale di uno Stato possa costituire una minaccia per l'ordine e la sicurezza pubblica. La segnalazione viene introdotta nel SIS e anche le altre parti contraenti si allineano sulla posizione dello Stato che ha fornito la segnalazione e ne possono derogare soltanto in presenza di seri motivi.

La politica in materia di visti è costituita dal Regolamento (CE) n. 539/2001 del Consiglio, del 15 marzo 2001, che adotta l'elenco dei paesi terzi i cui cittadini devono essere in possesso del visto all'atto dell'attraversamento delle frontiere esterne e l'elenco dei paesi terzi i cui cittadini sono esenti da tale obbligo, la cui ultima modifica risale al giugno del 2005.

L'ingresso ai fini di immigrazione, legato al permesso di soggiorno, è invece disciplinato dal Regolamento (CE) n. 1030/2002 del Consiglio, del 13 giugno 2002, che istituisce un modello uniforme per i permessi di soggiorno rilasciati ai cittadini di paesi terzi e per il quale è stato avviato un processo di modifica nel 2003 che prevede l'introduzione

di identificatori biometrici nei visti e nei permessi di soggiorno, in modo da creare un legame più sicuro tra questi e i loro titolari.

Il Regolamento (CE) n. 2252/2004 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, fissa le caratteristiche tecniche e di interoperabilità dei nuovi passaporti e documenti di viaggio dei cittadini europei. Le disposizioni del regolamento si applicano alle nuove emissioni di passaporti e documenti di viaggio, ma non alle carte di identità rilasciate dagli Stati membri ai loro cittadini, o ai passaporti e ai documenti di viaggio temporanei di validità pari o inferiore a 12 mesi.

Accanto ai regolamenti, esistono poi norme circa le migliori prassi da applicare nella concessione dei documenti necessari alla libera circolazione dei cittadini dei paesi terzi, quali quelle relative alla cooperazione consolare in materia di visti (Istruzione Consolare Comune).

Il Catalogo Schengen: raccomandazioni e migliori pratiche, si presenta invece come uno strumento di lavoro esplicativo finalizzato ad approfondire e precisare l'*acquis,* indicando come dovrebbe essere applicato correttamente nei vari settori (*acquis* di Schengen integrato nell'Unione europea; frontiere esterne, allontanamento e riammissione; Sistema d'Informazione Schengen, Sirene; rilascio dei visti; cooperazione di polizia).

3.1 Misure previste.

istituire, a lungo termine, uffici comuni per il rilascio dei visti nell'ambito della discussione sulla creazione del Servizio Europeo di Relazioni esterne. A tal fine favorire le iniziative dei singoli stati membri, che su base volontaria cooperano mettendo in comune personale e mezzi e per il rilascio dei visti;

modificare le istruzioni consolari comuni e istituire centri comuni di trattamento delle richieste di visto entro il primo semestre del 2006;

elaborare norme minime per le carte d'identità nazionali e inserire dal 2006 in poi gli integratori biometrici nei documenti di viaggio, nei visti, nei permessi di soggiorno e nei passaporti dei cittadini europei;

intensificare gli sforzi per il rilascio semplificato dei visti di breve durata ai cittadini dei paesi terzi, ove possibile e su base di reciprocità, quale elemento di un reale partenariato nelle relazioni esterne e nel contesto della politica di riammissione;

garantire prima possibile ai cittadini Ue l'esenzione dei visti per i viaggi nei paesi terzi figuranti nell'elenco positivo.