GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati (GEPD) sulla

— proposta di decisione del Consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II) (COM(2005)230 defin.);

— proposta di regolamento del Parlamento europeo e del Consiglio sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (COM(2005)236 defin.) e

— proposta di regolamento del Parlamento europeo e del Consiglio 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 defin.)

(2006/C 91/11)

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, ricevuta il 17 giugno 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. Cronistoria

Il sistema d'informazione Schengen (SIS) è un sistema informatico europeo su vasta scala creato come misura volta a compensare la soppressione dei controlli alle frontiere interne dello spazio Schengen. Il SIS consente alle autorità competenti degli Stati membri di scambiare informazioni che sono utilizzate per il controllo delle persone e degli oggetti alle frontiere esterne o all'interno del territorio, nonché per il rilascio di visti e di permessi di soggiorno.

La convenzione Schengen, entrata in vigore nel 1995, è un accordo intergovernativo. Il SIS, come parte della convenzione Schengen, è stato successivamente integrato nel quadro dell'UE dal trattato di Amsterdam.

Un nuovo sistema d'informazione Schengen di seconda generazione (SIS II) sostituirà il sistema attuale, in modo da consentire di estendere lo spazio Schengen ai nuovi Stati membri dell'UE. Esso introdurrà anche nuove funzionalità nel sistema. Le disposizioni Schengen, elaborate in forma di quadro intergovernativo, saranno interamente trasformate in strumenti giuridici europei classici.

Il 1º giugno 2005 la Commissione europea ha presentato tre proposte per l'istituzione del SIS II. Si tratta delle proposte seguenti:

— la proposta di regolamento fondata sul titolo IV del trattato CE (visti, asilo, immigrazione e altre politiche connesse con la libera circolazione delle persone), che disciplinerà gli aspetti del SIS II del primo pilastro (immigrazione), (di seguito «la proposta di regolamento»);

— la proposta di decisione fondata sul titolo VI del trattato UE (cooperazione di polizia e giudiziaria in materia penale), che disciplinerà il ricorso al SIS ai fini del terzo pilastro, (di seguito «la proposta di decisione»);

— la proposta di regolamento fondata sul titolo V (trasporti) concernente in modo specifico l'accesso delle autorità incaricate del rilascio delle carte di circolazione ai dati del SIS; la proposta sarà esaminata separatamente (cfr. infra punto 4.6.).

Va osservato in questo contesto che la Commissione presenterà nei prossimi mesi una comunicazione relativa all'interoperabilità e alle sinergie potenziate tra i sistemi d'informazione dell'UE (SIS, VIS, Eurodac).

Il SIS II consta di una banca dati centrale, il «sistema centrale d'informazione Schengen» (CS-SIS) di cui la Commissione assicurerà la gestione operativa, collegata ai punti di accesso nazionali definiti da ciascuno Stato membro (NI-SIS). Le autorità SIRENE garantiscono lo scambio di tutte le informazioni supplementari (informazioni connesse con segnalazioni introdotte nel SIS II ma non stoccate nello stesso).

Gli Stati membri alimenteranno il SIS II con dati relativi a persone ricercate per essere arrestate, prese in consegna o estradate, a persone ricercate nel contesto di procedimenti giudiziari, a persone da porre sotto sorveglianza o sotto controllo specifico, a persone alle quali deve essere rifiutato l'ingresso alla frontiera esterna e a oggetti perduti o rubati. Le «segnalazioni», insieme di dati inseriti nel SIS, consentono alle autorità competenti di identificare una persona o un oggetto.

Il SIS II presenta nuove caratteristiche: accesso più esteso al SIS (Europol, Eurojust, pubblici ministeri nazionali, autorità che rilasciano le carte di circolazione), interconnessione delle segnalazioni, aggiunta di nuove categorie di dati, inclusi i dati biometrici (impronte digitali e fotografie), nonché una piattaforma comune con il sistema d'informazione visti. Tali aggiunte sono state per anni oggetto di discussioni circa un presunto cambiamento delle finalità del SIS, da sistema di controllo a sistema d'informazione e d'indagine

1.2. **Valutazione generale delle proposte**

1. Il GEPD nota con soddisfazione di essere stato consultato in base all'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001. Tuttavia, dato il carattere obbligatorio della disposizione in questione, il presente parere dovrebbe essere menzionato nel preambolo dei testi.

2. Il GEPD si compiace delle proposte in esame per varie ragioni. La trasformazione di una struttura intergovernativa in strumenti di diritto europeo comporta varie conseguenze positive: il valore giuridico delle disposizioni che disciplinano il SIS II sarà precisato, la Corte di giustizia sarà competente a interpretare lo strumento giuridico del primo pilastro, il Parlamento europeo sarà almeno parzialmente coinvolto (anche se un pò tardivamente) nel processo.

3. Inoltre, per quanto riguarda il merito, le proposte contengono una parte notevole dedicata alla protezione dei dati, e comportano veri miglioramenti rispetto alla situazione attuale. In particolare si possono citare le misure a favore delle vittime di un'usurpazione di identità, l'estensione del regolamento n. 45/2001 alle operazioni di trattamento dati realizzate dalla Commissione nel contesto del titolo VI, una migliore definizione dei motivi che giustificano l'introduzione di segnalazioni di persone ai fini della non ammissione.

4. È inoltre evidente la grande attenzione dedicata alla redazione delle proposte; esse sono complesse, ma ciò rispecchia l'inerente complessità del sistema che disciplinano. La maggior parte delle osservazioni formulate nel presente parere è volta a chiarire o a completare le disposizioni, senza configurare la necessità di un rimaneggiamento generale.

Nonostante l'apprezzamento complessivo positivo, si possono tuttavia formulare alcune riserve, in particolare sugli elementi indicati in appresso:

1. È spesso difficile conoscere le intenzioni sottese al testo e che non sia stata elaborata una motivazione è davvero deplorabile. Visto il carattere assai complesso di questi documenti la motivazione sarebbe stata indispensabile. Senza il suo supporto in alcuni casi al lettore resta soltanto lo spazio per ipotesi.

2. Inoltre non si può che deplorare l'assenza di uno studio di valutazione di impatto. L'esistenza della prima versione del sistema non giustifica tale omissione, poiché vi sono notevoli differenze tra le due versioni. Si sarebbe dovuto riflettere meglio, tra l'altro, sulle conseguenze dell'inserimento di dati biometrici.

3. Il quadro giuridico della protezione dei dati è molto complesso e si basa sull'applicazione combinata della lex generalis e della lex specialis. Occorrerebbe garantire che, anche quando si elabora una normativa specifica, l'esistente quadro giuridico della protezione dei dati di cui alla direttiva 95/46/CE e al regolamento n. 45/2001 rimanga pienamente applicabile. L'applicazione combinata di vari strumenti giuridici non dovrebbe comportare discrepanze tra i regimi nazionali su aspetti fondamentali, né un indebolimento dell'attuale livello di protezione dei dati.

4. L'estensione dell'accesso a molte nuove autorità che non perseguono l'obiettivo originario di «controllo di persone e oggetti» dovrebbe comportare salvaguardie più rigorose.

5. Le proposte sono in gran parte fondate su altri strumenti giuridici ancora in fase di elaborazione (o addirittura non ancora proposti). Il GEPD, pur comprendendo le difficoltà di legiferare in una situazione complessa e in costante evoluzione, ritiene inaccettabile la situazione per le conseguenze sulle persone interessate e l'incertezza giuridica che crea.

6. La ripartizione delle competenze tra Stati membri e Commissione si presta a qualche confusione. L'assoluta chiarezza al riguardo è non solo necessaria per il buon funzionamento del sistema ma costituisce altresì un requisito essenziale per garantire un controllo generale dello stesso.

1.3. **Struttura del parere**

Il parere è strutturato come segue: innanzi tutto chiarisce il quadro giuridico applicabile al SIS II. definisce poi le finalità del SIS II e gli elementi che presentano significative differenze rispetto all'attuale sistema. Il punto 5 contiene osservazioni sui ruoli rispettivi della Commissione e degli Stati membri per quanto riguarda il funzionamento del SIS II. Il punto 6 riguarda i diritti delle persone interessate dai dati, mentre il punto 7 tratta del controllo, a livello nazionale e di GEPD, nonché della cooperazione tra le autorità di controllo. Il punto 8 presenta alcune osservazioni e possibili modifiche in materia di sicurezza; i punti 9 e 10 riguardano rispettivamente la comitatologia e l'interoperabilità. Infine nel sommario delle conclusioni figurano le principali conclusioni per ciascun punto.

2. QUADRO GIURIDICO PERTINENTE

2.1. **Quadro giuridico pertinente in materia di protezione dei dati del SIS II**

Le proposte fanno riferimento alla direttiva 95/46/CE, alla convenzione n. 108 del Consiglio d'Europa e al regolamento n. 45/2001 come quadro giuridico della protezione dei dati. Sono tuttavia pertinenti anche altri strumenti.

Per chiarire il contesto in questione e rammentare i principali punti su cui si fonda il presente parere è utile tener conto di quanto segue.

— 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, è 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.

— 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. 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.

— A norma dell'articolo 6, paragrafo 2 del trattato UE l'Unione rispetta i diritti fondamentali quali sono garantiti dalla CEDU.

I tre testi esplicitamente applicabili alle proposte relative al SIS II sono i seguenti:

— la convenzione n. 108 del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (di seguito *«convenzione 108»*), che ha enunciato principi fondamentali in materia di protezione delle persone rispetto al trattamento di dati di carattere personale. Tutti gli Stati membri hanno ratificato la convenzione 108 che si applica altresì alle attività dei settori di polizia e giudiziario. La convenzione 108 è attualmente il regime di protezione dei dati applicabile alla convenzione SIS, insieme alla raccomandazione n. (87) 15 del 17 settembre 1987 del Comitato dei ministri del Consiglio d'Europa che disciplina il ricorso ai dati di carattere personale nel settore della polizia;

— 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 (GU L 281 del 23.11.1995, pag. 31), denominata in seguito *«direttiva 95/46/CE»*. Va osservato che nella maggior parte degli Stati membri la legislazione nazionale che attua la direttiva contempla anche le operazioni di trattamento dei dati realizzate nel settore di polizia e giudiziario;

— 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 (GU L 8 del 12.1.2001, pag. 1), denominato di seguito *«regolamento 45/2001»*.

L'interpretazione della direttiva 95/46/CE e del regolamento 45/2001 dipende in parte dalla pertinente giurisprudenza della Corte europea dei diritti dell'uomo conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del 1950. 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].

[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.

Il 4 ottobre 2005 la Commissione ha presentato una proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale [1] (in seguito *«progetto di decisione quadro»*). Tale decisione quadro è volta a sostituire la convenzione 108 in quanto testo di riferimento per il progetto di decisione relativa al SIS II, che potrebbe avere ripercussioni sul regime di protezione dei dati in questo contesto (cfr. infra punto 2.2.5).

2.2. **Regime giuridico di protezione dei dati del SIS II**

2.2.1. *Osservazioni di carattere generale*

La base giuridica necessaria per disciplinare il SIS II consta di strumenti separati; tuttavia, come affermato nei considerando, ciò «non intacca il principio secondo il quale il SIS II è un sistema unico d'informazione e in quanto tale deve operare. È pertanto necessario che alcune disposizioni di tali strumenti siano identiche».

La struttura dei due documenti è fondamentalmente la stessa, con i capitoli I, II e III quasi identici nei due testi. Il fatto che il SIS II debba essere considerato come sistema d'informazione unico dotato di due basi giuridiche differenti si riflette anche nel regime, piuttosto complesso, di protezione dei dati.

Il regime di protezione dei dati è in parte determinato, nelle proposte stesse, come *«lex specialis»* completata da una diversa legislazione di riferimento (*«lex generalis»*) per ciascun settore (Commissione, Stati membri nel contesto del primo pilastro e Stati membri nel contesto del terzo pilastro).

Tenuto conto di questa struttura si presenta il quesito di come trattare le norme particolari rispetto alla norma generale. Nella fattispecie il GEPD considera la norma particolare come un'applicazione della norma generale. Di conseguenza la *lex specialis* deve essere sempre conforme alla *lex generalis*; essa elabora (precisandola o completandola) la *lex generalis* ma non è concepita come eccezione riguardo a quest'ultima.

Quanto al quesito circa quale sia la norma da applicare in casi specifici, il principio è che la *lex specialis* si applichi in via prioritaria; ma ogniqualvolta questa non si pronunci o non sia chiara, si deve fare riferimento alla *lex generalis*.

In questa struttura si configurano tre diverse combinazioni tra *lex generali* e *lex specialis*, come sintetizzato in appresso.

2.2.2. *Regime applicabile per la Commissione*

Quando è coinvolta la Commissione, si applica il regolamento 45/2001, anche per quanto attiene al ruolo del GEPD, che le attività siano svolte nell'ambito del primo pilastro (proposta di regolamento) o del terzo pilastro (proposta di decisione). Il considerando 21 della proposta di decisione afferma che «Il regolamento (CE) n. 45/2001 (....) disciplina il trattamento di dati personali effettuato dalla Commissione nell'esercizio di attività che rientrano in tutto o in parte nel campo di applicazione del diritto comunitario. Parte del trattamento dei dati personali a cura del SIS II rientra nel campo di applicazione del diritto comunitario.»

Esistono motivi pratici al riguardo: sarebbe infatti estremamente difficile, per quanto concerne la Commissione, stabilire se i dati sono trattati nel quadro di attività che rientrano nel primo o nel terzo pilastro.

Inoltre applicare un unico strumento giuridico a tutte le attività della Commissione nel contesto del SIS II non solo appare più logico da un punto di vista pratico, ma migliora anche la coerenza (garantendo, come afferma il considerando 21 della proposta di decisione, un'applicazione «coerente e omogenea delle norme relative alla tutela delle libertà e dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali»). Il GEPD accoglie pertanto con favore il riconoscimento da parte della Commissione che il regolamento 45/2001 si applica a tutte le attività di trattamento dei dati della Commissione nel contesto del SIS II.

2.2.3. *Regime applicabile per gli Stati membri*

La situazione per quanto concerne gli Stati membri è più complessa. Il trattamento dei dati di carattere personale in applicazione della proposta di regolamento è disciplinato sia da quest'ultimo che dalla direttiva 95/46/CE. Nel considerando 14 della proposta di regolamento si afferma molto chiaramente che la direttiva deve essere considerata come *lex generalis*, mentre il regolamento SIS II sarà la *lex specialis*. Ciò comporta varie conseguenze che saranno descritte in appresso.

Quanto alla proposta di decisione, lo strumento giuridico di riferimento in materia di protezione dei dati (*lex generalis*) è la convenzione 108, il che può far insorgere un'importante differenza in certi punti tra i regimi di protezione dei dati applicabili nel contesto del primo e del terzo pilastro.

2.2.4 *Impatto sul livello di protezione dei dati*

A titolo di commento generale sull'architettura prevista per la protezione dei dati, il GEPD sottolinea i seguenti elementi:

— l'applicazione della proposta di regolamento in quanto lex specialis della direttiva 95/46/CE (e analogamente quella della proposta di decisione come lex specialis della convenzione 108) non dovrebbe mai condurre a una diminuzione del livello di protezione dei dati garantito ai sensi della direttiva o della convenzione. Il GEPD farà raccomandazioni al riguardo (cfr. ad esempio il diritto di ricorso);

[1] (COM(2005) 475 defin.).

— analogamente, l'applicazione combinata di strumenti giuridici non può avere l'effetto di abbassare il livello della protezione dei dati garantito nel quadro dell'attuale convenzione Schengen (cfr. ad esempio le osservazioni formulate in appresso circa l'articolo 13 della direttiva 95/46/CE);

— l'applicazione di due strumenti diversi, benché necessaria a motivo del quadro giuridico europeo, non dovrebbe condurre a ingiustificate discrepanze nella protezione dei dati delle persone interessate in funzione del tipo di dati trattati. Ciò deve essere per quanto possibile evitato. Le raccomandazioni formulate in appresso saranno altresì volte a migliorare il più possibile la coerenza (cfr. ad esempio i poteri delle autorità di controllo nazionali);

— il quadro giuridico è così complesso che molto probabilmente ingenererà una certa confusione al momento dell'applicazione pratica. In alcuni casi è difficile distinguere come interagiscano la *lex generalis* e la *lex specialis*, e sarebbe utile chiarirlo nelle proposte. Inoltre, in questa situazione giuridica complessa è molto utile il suggerimento formulato dall'Autorità di controllo comune (ACC) Schengen nel suo parere sulla base giuridica proposta per il SIS II (27 settembre 2005) di elaborare un vademecum che enumeri tutti i diritti esistenti in relazione al SIS II e stabilisca una gerarchia chiara della legislazione applicabile.

In conclusione il presente parere cercherà di garantire un livello elevato di protezione dei dati, di coerenza e di chiarezza per far sì che le persone interessate abbiano la necessaria certezza del diritto.

2.2.5. *Impatto del progetto di decisione quadro sulla protezione dei dati nell'ambito del terzo pilastro*

La decisione quadro sulla protezione dei dati personali nell'ambito del terzo pilastro [1] sostituirà la convenzione 108 come strumento di riferimento per la protezione dei dati nel progetto di decisione SIS II. Ciò non è affermato nella proposta ma è conseguente alla proposta di decisione quadro. L'articolo 34, paragrafo 2 stabilisce che «qualsiasi riferimento alla convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, del 28 gennaio 1981, deve essere considerato come un riferimento alla presente decisione quadro». Il GEPD formulerà un parere sul progetto di decisione quadro nelle prossime settimane e quindi nel presente parere non ne analizzerà il contenuto nei dettagli. Tuttavia, ogniqualvolta l'applicazione della decisione quadro può avere un impatto significativo sul regime di protezione dei dati del SIS II, ciò verrà indicato.

2.2.6. *Applicazione dell'articolo 13 della direttiva 95/46/CE e dell'articolo 9 della convenzione 108*

L'articolo 13 della direttiva 95/46/CE e l'articolo 9 della convenzione 108 prevedono che gli Stati membri possano adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti da tali strumenti qualora tale restrizione costituisca una misura necessaria alla salvaguardia di altri importanti interessi (ad esempio, sicurezza dello Stato, difesa, pubblica sicurezza) [2].

I considerando della proposta di regolamento e della proposta di decisione affermano che gli Stati membri potrebbero fare ricorso a tale possibilità quando attuano le proposte a livello nazionale. In tal caso dovrebbe essere rispettata una duplice condizione: l'applicazione dell'articolo 13 della direttiva 95/46/CE deve essere conforme all'articolo 8 della CEDU e non dovrebbe condurre a un indebolimento del presente regime di protezione dei dati.

Ciò è ancora più essenziale nel caso del SIS II poiché il sistema deve essere prevedibile. Dato che gli Stati membri condividono i loro dati deve esistere la possibilità di sapere con sufficiente certezza come saranno trattati a livello nazionale.

Sussiste in particolare un elemento di inquietudine al riguardo, ossia che le proposte conducano a una riduzione dell'attuale livello di protezione dei dati. L'articolo 102 della convenzione di Schengen prevede un sistema in cui il ricorso ai dati è strettamente disciplinato e limitato, anche nel diritto nazionale («qualsiasi utilizzazione dei dati non conforme ai paragrafi da 1 a 4 sarà considerata uno sviamento di finalità alla luce del diritto nazionale di ciascuna parte contraente»). Sia la direttiva 95/46/CE che la convenzione 108 prevedono tuttavia la possibilità di includere nel diritto nazionale eccezioni, tra l'altro, al principio di limitazione delle finalità del trattamento dei dati. In questo caso ci si allontanerebbe dal regime attuale della convenzione di Schengen, in cui la legislazione nazionale non può deviare dal principio centrale di limitazione delle finalità e dell'utilizzazione.

L'adozione della decisione quadro non cambierebbe questa osservazione: il problema vero è molto più mantenere un principio rigoroso di limitazione delle finalità del trattamento dei dati del SIS II piuttosto che fare in modo che tali dati siano trattati conformemente alla decisione quadro.

[1] Sostituirà anche il regime generale di protezione dei dati della convenzione Schengen (articoli da 126 a 130 della convenzione di Schengen). Questo regime non si applica al SIS.

[2] Uno Stato membro che ricorra a questa possibilità di limitare i diritti lo può fare soltanto nel rispetto dell'articolo 8 della CEDU, come indicato precedentemente.

Il GEPD suggerisce di introdurre nelle proposte relative al SIS II (ossia all'articolo 21 della proposta di regolamento e all'articolo 40 della proposta di decisione) una disposizione, avente lo stesso effetto dell'attuale articolo 102, paragrafo 4 della convenzione Schengen, che limiti per gli Stati membri la possibilità di autorizzare un'utilizzazione dei dati non prevista nei testi del SIS II. Un'altra possibilità sarebbe limitare esplicitamente nella proposta di decisione e nella proposta di regolamento la portata delle eccezioni previste ai sensi dell'articolo 13 della direttiva o dell'articolo 9 della convenzione, stabilendo ad esempio che gli Stati membri possono limitare solo i diritti di accesso e d'informazione, ma non i principi che riguardano la qualità dei dati.

3. **FINALITÀ**

Conformemente all'articolo 1 dei due documenti («istituzione e obiettivo generale del SIS II»), il SIS II è istituito «affinché le autorità competenti degli Stati membri possano cooperare fra loro scambiandosi informazioni per il controllo di persone e oggetti» e «contribuisce a mantenere un elevato livello di sicurezza in uno spazio senza controlli alle frontiere interne degli Stati membri».

La finalità del SIS II è formulata in termini piuttosto ampi; le disposizioni citate qui sopra non costituiscono di per sé una precisa indicazione di ciò che l'obiettivo ricopre (significa).

L'obiettivo del SIS II sembra molto più ampio di quello dell'attuale SIS quale enunciato all'articolo 92 della convenzione Schengen che si riferisce in modo specifico a «(...) segnalazioni di persone e di oggetti, in occasione di controlli alle frontiere, di verifiche e di altri controlli di polizia e doganali (...) nonché (per la sola categoria di segnalazioni di cui all'articolo 96) ai fini della procedura di rilascio di visti, del rilascio dei documenti di soggiorno e dell'amministrazione degli stranieri (...)».

Questa finalità più ampia risulta altresì dall'aggiunta al SIS II di nuove funzionalità e accessi che non corrispondono all'obiettivo originale dei controlli di persone e oggetti, ma piuttosto a uno strumento di indagine. In particolare l'accesso è previsto per autorità che ricorreranno ai dati del SIS II per le loro proprie finalità e non per realizzare le finalità del SIS II (cfr. infra); l'interconnessione delle segnalazioni sarà generalizzata sebbene ciò sia un tipico aspetto dello strumento d'indagine di polizia.

Ci sono anche quesiti circa il motore di ricerca biometrico che dovrà essere elaborato nei prossimi anni, consentendo ricerche nel sistema che vanno oltre le esigenze di un sistema di controllo.

In conclusione, le proposte hanno una portata molto più ampia dell'attuale quadro. Ciò richiede garanzie supplementari. Al riguardo, il GEPD incentrerà l'analisi non tanto sull'ampia definizione che figura all'articolo 1, quanto piuttosto sulle funzionalità e gli altri elementi costitutivi del SIS II.

4. **MODIFICHE SIGNIFICATIVE DEL SIS II**

Il presente capitolo riguarda in primo luogo i nuovi elementi introdotti dal SIS II, ossia l'inserimento della biometria, la nuova concezione di accesso, con speciale attenzione all'accesso da parte di Europol, di Eurojust e delle autorità incaricate del rilascio delle carte di circolazione, l'interconnessione delle segnalazioni e l'accesso da parte delle varie autorità ai dati riguardanti l'immigrazione.

4.1. **Biometria**

Le proposte relative al SIS II introducono la possibilità di trattare una nuova categoria di dati che meritano una speciale attenzione: i dati biometrici. Come già sottolineato dal GEPD nel parere concernente il sistema d'informazione visti [1], il carattere inerentemente sensibile dei dati biometrici necessita di specifiche garanzie che non sono state introdotte nelle proposte relative al SIS II.

In generale la tendenza a ricorrere a dati biometrici nei sistemi d'informazione dell'ambito UE (VIS, EURODAC, EUCARIS, ecc.) aumenta costantemente, senza essere accompagnata da un attento esame dei rischi connessi e delle garanzie necessarie.

La necessità di approfondire la riflessione al riguardo è stata anche illustrata nella recente risoluzione sulla biometria pubblicata dalla Conferenza internazionale delle autorità di protezione dei dati svoltasi a Montreux [2]. Finora si era posto l'accento soltanto sul valore aggiunto della messa a punto di norme volte ad aumentare l'interoperabilità tra i sistemi e non a migliorare la qualità dei procedimenti biometrici.

---

[1] Parere del GEPD 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, 23 marzo 2005, punto 3.4.2.

[2] 27ª Conferenza internazionale delle autorità di protezione dei dati e della privacy, Montreux, 16 settembre 2005. Risoluzione sull'utilizzo della biometria in passaporti, carte di identità e titoli di viaggio.

Sarebbe utile stabilire una serie di obblighi ed esigenze comuni connessi con la specificità di tali dati, nonché una metodologia comune per l'attuazione. Tali esigenze comuni potrebbero comportare in particolare gli elementi indicati in appresso (la necessità dei quali è stata messa in rilievo nelle proposte relative del SIS II).

— **Analisi d'impatto mirata:** si deve sottolineare che le proposte non hanno costituito oggetto di un'analisi d'impatto per quanto riguarda il ricorso alla biometria ([1]).

— **Importanza del processo di registrazione:** l'origine dei dati biometrici e la maniera in cui saranno raccolti non sono descritte in modo dettagliato. La registrazione è una tappa essenziale nell'insieme della procedura di identificazione biometrica e non ci si può limitare a una definizione negli allegati o attraverso ulteriori discussioni in sede di sottogruppo, poiché essa condiziona direttamente i risultati finali della procedura, ossia il livello del tasso di respingimento ingiustificato o di accettazione ingiustificata.

— **Accento posto sul livello di precisione:** il ricorso alla biometria a fini di identificazione (confronto tra un elemento e molti altri), che è presentato nella proposta come futura attuazione di un motore di ricerca biometrico, è un aspetto più delicato poiché i risultati di tale processo sono meno accurati che nel caso del ricorso alla stessa a fini di autenticazione o controllo (confronto tra due elementi). L'identificazione biometrica non dovrebbe dunque costituire l'unico mezzo di identificazione o l'unica chiave di accesso a ulteriori informazioni.

— **Procedura di ripiego:** procedure di ripiego facilmente accessibili sono attuate per rispettare la dignità delle persone che potrebbero essere state identificate per errore ed evitare di trasferire su di loro l'onere delle imperfezioni del sistema.

Il ricorso a dati biometrici senza una corretta valutazione preliminare rivela altresì una sopravvalutazione dell'affidabilità della biometria. I dati biometrici sono «dati in tempo reale» che evolvono col tempo; i campioni che sono inseriti nella banca dati costituiscono soltanto un'istantanea di un elemento dinamico, la cui permanenza non è assoluta e deve essere controllata. La precisione della biometria deve sempre essere messa in prospettiva con altri elementi, poiché non sarà mai assoluta.

([1]) L'analisi potrebbe basarsi sui cosiddetti sette pilastri della saggezza biometrica in «Biometrica alle frontiere: valutare l'impatto sulla società» IPTS, DG-JRC, EUR 21585 EN, punto 1.2, pagina 32.

L'eventuale utilizzazione dei dati del SIS II a fini di indagine presenta gravi rischi per le persone interessate se si aumenta e sopravvaluta il ruolo delle prove biometriche, come è stato dimostrato in precedenti casi ([2]).

Le proposte dovrebbero pertanto tener conto delle reali capacità della biometria a fini di identificazione e richiamare l'attenzione su queste.

4.2. **Accesso ai dati del SIS II**

4.2.1. *Una nuova concezione dell'accesso*

Le autorità che hanno accesso ai dati del SIS sono definite per ciascuna segnalazione. In linea di principio si applica una duplice condizione per concedere l'accesso ai dati SIS: l'accesso deve essere accordato alle autorità nel rispetto integrale dell'obiettivo generale del SIS e dell'obiettivo specifico di ciascuna segnalazione.

Ciò risulta dalla definizione di segnalazione figurante nella proposta di regolamento e nella proposta di decisione (l'articolo 3, paragrafo 1, lettera a) di ciascuno dei due strumenti stabilisce che si *intende per «segnalazione» un insieme di dati inseriti nel SIS II che permetta alle autorità competenti di identificare un individuo o un oggetto in vista di una linea di condotta specifica*) L'articolo 39, paragrafo 2 della proposta di decisione conferma tale definizione: «*i dati di cui al paragrafo 1 sono utilizzati soltanto per identificare un individuo in vista della linea di condotta specifica da seguire in conformità della presente decisione*». Al riguardo il SIS II conserva le caratteristiche di un sistema «hit-no hit», nel quale ciascuna segnalazione è inserita in vista di un particolare obiettivo (procedura di consegna, non ammissione ...).

Le autorità che hanno accesso ai dati del SIS sono di fatto limitate nell'utilizzazione di questi dati, poiché in linea di principio vi hanno accesso soltanto in vista di una linea di condotta specifica.

Tuttavia alcuni accessi previsti nelle nuove proposte non sono coerenti con questa logica in quanto sono volti a fornire informazioni alle autorità e non a permettere loro di identificare una persona e di attenersi alla linea di condotta prevista nella segnalazione.

([2]) Nel giugno 2004 un avvocato di Portland (USA) è stato imprigionato per due settimane poiché l'FBI aveva stabilito che le sue impronte digitali corrispondevano a impronte trovate nel contesto degli attentati di Madrid (su un sacco di plastica che aveva contenuto il detonatore). È stato infine stabilito che la tecnica di confronto era stata imprecisa e ne era risultato un errore di interpretazione.

Più in particolare ciò riguarda:

— l'accesso delle autorità competenti in materia d'asilo ai dati dell'immigrazione

— l'accesso delle autorità autorizzate a concedere lo status di rifugiato ai dati dell'immigrazione

— l'accesso di Europol, a fini di confisca, alle segnalazioni concernenti l'estradizione, la sorveglianza discreta e i documenti rubati

— l'accesso di Eurojust ai dati concernenti l'estradizione e la localizzazione.

Tutte queste autorità condividono le stesse caratteristiche per quanto riguarda i dati del SIS II:

esse non sono in grado di attenersi alla linea di condotta specifica di cui alla definizione di segnalazione. L'accesso è accordato loro perché possano ottenere informazioni per le proprie finalità.

Anche tra queste autorità occorre stabilire una distinzione tra quelle che hanno accesso per le proprie finalità, ma con un obiettivo particolare, e quelle (ossia Europol ed Eurojust) per le quali non esiste alcuna precisazione quanto all'obiettivo dell'accesso. Le autorità competenti in materia di asilo ad esempio hanno accesso in vista di uno scopo particolare, anche se non è quello menzionato nella segnalazione. Esse possono accedere ai dati sull'immigrazione «per determinare se un richiedente asilo abbia soggiornato illegalmente in un altro Stato membro». Europol ed Eurojust tuttavia accedono ai dati contenuti in talune categorie di segnalazioni «in quanto necessarie all'assolvimento dei loro compiti.»

Per sintetizzare, l'accesso ai dati del SIS II è accordato in tre casi:

— per dare seguito a una segnalazione,

— per una finalità che non rientra nel SIS II, ma è ben delimitata nelle proposte,

— per una finalità che non rientra nel SIS II, ma non è descritta precisamente.

Secondo il GEPD quanto più è generale la finalità dell'accesso tanto più è necessario che siano rigorose le garanzie applicate. Le garanzie generali sono esposte nei dettagli in appresso. Sarà poi affrontata la situazione specifica di Europol ed Eurojust.

4.2.2. *Condizioni per la concessione dell'accesso*

1. L'accesso può in ogni caso essere accordato soltanto se è compatibile con la finalità generale del SIS II e conforme alla sua base giuridica.

   Ciò significa in pratica che l'accesso ai dati sull'immigrazione ai sensi della proposta di regolamento deve sostenere l'attuazione di politiche collegate alla libera circolazione delle persone e facenti parte dell'acquis di Schengen.

   Analogamente, l'accesso alle segnalazioni previsto dalla decisione è volto a sostenere la cooperazione operativa in materia penale tra i servizi di polizia e le autorità giudiziarie.

   Al riguardo il GEPD richiama l'attenzione sul capitolo concernente l'accesso al SIS II da parte dei servizi incaricati del rilascio delle carte di circolazione (cfr. infra, punto 4.6).

2. Deve essere dimostrata la necessità di accedere al SIS II, nonché l'impossibilità o la grande difficoltà di ottenere i dati con altri mezzi, meno intrusivi. Ciò avrebbe dovuto essere affermato in una motivazione, di cui, come già detto, si deplora l'assenza.

3. L'utilizzazione che sarà fatta dei dati deve essere definita in modo esplicito e restrittivo.

   Ad esempio le autorità competenti in materia di asilo hanno accesso ai dati sull'immigrazione «per determinare se un richiedente asilo abbia soggiornato illegalmente in un altro Stato membro». Tuttavia Europol ed Eurojust hanno accesso ai dati contenuti in certe categorie di segnalazioni, in quanto necessari all'assolvimento dei loro compiti; ma ciò non è sufficientemente precisato (cfr. infra).

4. Le condizioni di accesso devono essere ben definite e delimitate. In particolare soltanto i servizi appartenenti alle organizzazioni incaricate di trattare i dati del SIS II dovrebbero avervi accesso. Tale obbligo previsto all'articolo 40 della proposta di decisione e all'articolo 21, paragrafo 2 della proposta di regolamento dovrebbe essere completato prevedendo per le autorità nazionali l'obbligo di tenere un elenco aggiornato delle persone autorizzate ad accedere al SIS II. La stessa norma dovrebbe applicarsi ad Europol e ad Eurojust.

5. Il fatto che a queste autorità sia stato concesso l'accesso ai dati del SIS II non può in nessun caso giustificare che esse introducano o conservino nel sistema dati che non siano utili per la specifica segnalazione di cui fanno parte. Non possono essere aggiunte nuove categorie di dati a causa di una utilità per altri sistemi di informazione. Ad esempio l'articolo 39 della proposta di decisione prevede l'inserimento nelle segnalazioni di dati concernenti l'autorità della segnalazione. Questi dati non sono necessari per attenersi a una linea di condotta specifica (arresto, sorveglianza ...) e l'unica ragione per cui potrebbero essere inseriti è probabilmente il fatto che sarebbero utili per Europol o Eurojust. Occorre fornire una chiara motivazione per il trattamento di questi dati.

6. La durata di conservazione dei dati non può essere prorogata qualora non sia necessario in vista delle finalità per le quali i dati sono stati inseriti. Ciò significa che anche se Europol o Eurojust hanno accesso a questi dati, ciò non è motivo sufficiente perché siano conservati nel sistema (ad esempio qualora una persona ricercata sia stata estradata, i dati dovrebbero essere soppressi, anche se potrebbero essere utili per Europol). Pure in questo caso sarà necessario garantire un attento controllo affinché la norma sia rispettata dalle autorità competenti.

4.2.3. *Accesso di Europol ed Eurojust*

a. *Motivi dell'accesso*

L'accesso di Europol e di Eurojust ad alcuni dati del SIS è stato già oggetto di discussioni prima che fosse previsto nella decisione del Consiglio del 24 febbraio 2005 ([1]). Fra tutte le autorità che hanno accesso per le proprie finalità, essi beneficiano di un accesso formulato nei termini più generali. Sebbene l'uso di questi dati sia definito nel capitolo XII della decisione, non sono tuttavia sufficientemente precisati i motivi che in primo luogo giustificano l'accesso. Ciò è tanto più vero se si considera che probabilmente i compiti di Europol e di Eurojust evolveranno nel tempo.

Il GEPD chiede alla Commissione di definire in modo restrittivo i compiti per la cui esecuzione sia giustificato l'accesso di Europol e di Eurojust.

b. *Limitazione per quanto riguarda i dati*

Per evitare domande non circostanziate da parte di Europol e di Eurojust e per far sì che essi abbiano accesso soltanto ai dati necessari per l'assolvimento dei loro compiti, l'ACC di Schengen ha suggerito nel suo parere del 27 settembre 2005 concernente le proposte relative al SIS II di limitare l'accesso di Europol e di Eurojust ai dati relativi a persone i cui nomi figurano già nei loro schedari. Si avrebbe così la garanzia che consultino soltanto le segnalazioni che li riguardano. Il GEPD appoggia questa raccomandazione.

c. *Aspetti relativi alla sicurezza*

Il GEPD saluta con favore l'obbligo di registrare tutte le transazioni effettuate da Europol e da Eurojust nel quadro delle connessioni nonché il divieto di copiare o scaricare parti del sistema.

L'articolo 56 della proposta di decisione prevede da uno a due punti d'accesso per Europol ed Eurojust. Per quanto sia comprensibile che uno Stato membro necessiti di più di un punto d'accesso, per la posizione decentrata delle sue autorità competenti, lo status e le attività di Europol e di Eurojust non ne giustificano la richiesta. È altresì necessario sottolineare che dal punto di vista della sicurezza la moltiplicazione dei punti di accesso aumenta il rischio di abuso e dovrebbe quindi essere precisamente giustificato con elementi più consistenti. Pertanto, in mancanza di argomentazioni convincenti, il GEPD propone di concedere soltanto un punto d'accesso ad Europol e ad Eurojust.

4.3. **Interconnessione delle segnalazioni**

L'articolo 26 del regolamento e l'articolo 46 della decisione prevedono che gli Stati membri possano creare connessioni fra segnalazioni in conformità del proprio diritto interno, così da instaurare un nesso fra due o più segnalazioni.

Sebbene le connessioni fra segnalazioni possano essere utili per i controlli (ad esempio il mandato d'arresto nei confronti di un ladro di automobili può essere collegato al veicolo rubato), l'introduzione di connessioni fra segnalazioni è un aspetto assai tipico di uno strumento investigativo di polizia.

L'interconnessione di segnalazioni può avere un significativo impatto sui diritti degli interessati, in quanto essi non sono più «valutati» sulla base di dati riguardanti unicamente loro, ma sulla base della loro eventuale associazione con altri. Gli individui i cui dati sono collegati a quelli di criminali o di ricercati rischiano di essere trattati con maggior sospetto rispetto ad altri. L'interconnessione delle segnalazioni costituisce altresì un'estensione dei poteri investigativi del SIS, in quanto essa rende possibile la registrazione di presunte bande o reti (se ad esempio i dati relativi a immigrati clandestini vengono collegati ai dati relativi a trafficanti). Infine, poiché la definizione di connessioni rientra nelle legislazioni nazionali, si può verificare il caso in cui vengano stabilite in uno Stato membro connessioni illegali in un altro, alimentando così il sistema con dati «illegali».

([1]) Decisione del Consiglio 2005/211/GAI del 24 febbraio 2005 relativa all'introduzione di alcune nuove funzioni del sistema d'informazione Schengen, anche nel quadro della lotta contro il terrorismo (GU L 68/44 del 15.3.2005).

Le conclusioni del Consiglio del 14 giugno 2004 sui requisiti funzionali per il SIS II affermano che ogni connessione deve avere un chiaro requisito operativo, basarsi su una relazione chiaramente definita e rispettare il principio di proporzionalità. Essa potrebbe inoltre non avere incidenza sui diritti di accesso. Tuttavia, poiché l'interconnessione delle segnalazioni costituisce un'operazione di trattamento, essa deve soddisfare le disposizioni della legislazione nazionale che attua la direttiva 95/46/CE e/o la Convenzione 108.

Le proposte ribadiscono che l'esistenza di connessioni non può modificare i diritti di accesso (altrimenti essa permetterebbe l'accesso a dati il cui trattamento non sarebbe autorizzato nell'ambito della legislazione nazionale, in violazione dell'articolo 6 della direttiva).

Il GEPD sottolinea l'importanza di una rigorosa interpretazione dell'articolo 26 del regolamento e dell'articolo 46 della decisione proposti: questo può essere garantito chiarendo che le autorità non aventi diritto di accesso a determinate categorie di dati non solo non possono avere accesso a connessioni a queste categorie, ma non dovrebbero neppure essere a conoscenza della loro esistenza. La visualizzazione delle connessioni deve essere impossibile quando non vi è diritto di accesso ai dati connessi.

Il GEPD vorrebbe inoltre essere consultato sulle misure tecniche atte a garantire quanto.

4.4. **Segnalazioni ai fini della non ammissione**

4.4.1. *Motivazioni per l'inclusione*

Il ricorso alla «segnalazione di cittadini di paesi terzi ai fini della non ammissione» (articolo 15 del regolamento) ha un impatto significativo sulle libertà individuali: una persona segnalata in virtù di questa disposizione non ha più accesso allo spazio Schengen per diversi anni. A tuttoggi, questa è stata la segnalazione più utilizzata in termini di numero di persone segnalate. Considerando le conseguenze di queste segnalazioni, così come il numero di persone interessate, la loro concezione e attuazione devono richiedere la massima attenzione. Sebbene ciò valga anche per altre segnalazioni, il GEPD riserverà un capitolo specifico a queste segnalazioni, in quanto esse pongono problemi specifici per quanto riguarda le motivazioni per l'inclusione.

La nuova segnalazione ai fini della non ammissione presenta miglioramenti rispetto alla situazione attuale ma non è completamente soddisfacente in quanto si basa in gran parte su strumenti che non sono stati ancora adottati o neppure proposti.

I miglioramenti consistono in una descrizione più precisa dei motivi di inserimento dei dati. Il testo attuale della Convenzione Schengen ha portato ad una situazione che presenta differenze significative tra Stati membri per quanto riguarda il numero di persone segnalate ai sensi dell'articolo 96 della convenzione. L'autorità di controllo comune Schengen ha effettuato uno studio [1] approfondito sulla questione e ha raccomandato che i responsabili politici studino la possibilità di armonizzare i motivi di introduzione di una segnalazione nei vari Stati Schengen.

L'articolo 15 della proposta è più dettagliato nella sua formulazione e ciò è positivo.

L'articolo 15, paragrafo 2 stabilisce inoltre un elenco di casi in cui delle persone non possono essere segnalate perché risiedono legalmente nel territorio di uno Stato membro in applicazione di vari status. Benché questo meccanismo possa essere dedotto dall'attuale Convenzione Schengen, la pratica ha dimostrato che è applicato negli Stati membri in vari modi. Pertanto il chiarimento è utile.

Tuttavia questa disposizione è anche fortemente criticata in quanto basata in gran parte su un testo non ancora adottato, ossia la direttiva relativa al «rimpatrio».

Dopo l'adozione delle proposte relative al SIS II la Commissione ha proposto il 1º settembre 2005 una direttiva relativa alle norme e procedure comuni applicabili negli Stati membri al rimpatrio di cittadini di paesi terzi che risiedono illegalmente; tuttavia, fintanto che il testo non è definitivo non può essere considerato un valido motivo per inserire dati nel sistema. Ciò costituisce in particolare una violazione dell'articolo 8 della convenzione europea dei diritti dell'uomo in base a cui un'intrusione nella vita privata deve essere fondata, tra l'altro, su una norma legislativa chiara e accessibile;

Pertanto il GEPD invita la Commissione a ritirare questa disposizione o a riformularla in base alla legislazione esistente in modo che le persone possano sapere esattamente quali sono le misure che le autorità possono adottare nei loro confronti.

4.4.2 *Accesso alle segnalazioni effettuate a norma dell'articolo 15*

L'articolo 18 stabilisce quali autorità hanno accesso a tali segnalazioni e a quale fine. L'articolo 18, paragrafi 1 e 2 stabilisce quali autorità hanno accesso alle segnalazioni effettuate in base alla direttiva sul rimpatrio. Anche in questo caso valgono le osservazioni di cui sopra.

[1] Relazione dell'autorità di controllo comune Schengen su un'ispezione per quanto riguarda l'uso delle segnalazioni ai sensi dell'articolo 96 nel sistema di informazione Schengen, Bruxelles, 20 giugno 2005.

L'articolo 18, paragrafo 3 della proposta di regolamento accorda l'accesso alle autorità responsabili della concessione dello status di rifugiato in virtù di una direttiva che non è nemmeno stata proposta. In mancanza di un testo, il GEPD ribadisce le suddette osservazioni.

4.4.3 *Durata di conservazione delle segnalazioni ai sensi dell'articolo 15*

In base all'articolo 20 le segnalazioni non possono essere conservate oltre i termini del periodo di non ammissione stabiliti nella decisione (di espulsione o rimpatrio). Questa disposizione è coerente con le norme applicabili in materia di protezione dei dati. Inoltre le segnalazioni saranno cancellate automaticamente dopo cinque anni a meno che gli Stati membri che hanno inserito i dati nel SIS II decidano diversamente.

Un adeguato controllo a livello nazionale dovrebbe assicurare che non vi sia una proroga ingiustificata del periodo di conservazione e che gli Stati membri cancellino i dati prima della scadenza dei cinque anni se il periodo di non ammissione dovesse essere più breve.

4.5. **Periodi di conservazione**

Benché il principio della conservazione delle segnalazioni rimanga invariato (in generale una segnalazione dovrebbe essere cancellata dal SIS II non appena sia eseguita la linea di condotta richiesta con la segnalazione), le proposte comporteranno in generale un prolungamento del periodo di conservazione delle segnalazioni.

La Convenzione Schengen prevede che la necessità di conservare i dati deve esser riesaminata al più tardi tre anni dopo il loro inserimento (o un anno quando si tratta di dati inseriti a fini di sorveglianza discreta). Le nuove proposte prevedono la cancellazione automatica (dando allo Stato membro della segnalazione la possibilità di opporsi) dopo 5 anni per i dati relativi all'immigrazione, 10 anni per i dati relativi all'arresto, alle persone scomparse e alle persone ricercate nell'ambito di procedure giudiziarie, e 3 anni per le persone da sottoporre a sorveglianza discreta.

Benché in linea di massima gli Stati membri dovranno cancellare i dati quando lo scopo della segnalazione è stato raggiunto, si tratta di un aumento significativo del periodo massimo di conservazione (triplicato nella maggior parte dei casi), senza alcuna giustificazione da parte della Commissione. Nel caso dei dati relativi all'immigrazione si può supporre che il periodo di 5 anni sia collegato alla durata del divieto di ammissione proposto nel progetto di direttiva sul rimpatrio. In tutti gli altri casi il GEPD non è a conoscenza di una spiegazione logica.

Le eventuali ripercussioni di una segnalazione nel SIS sulla vita delle persone interessate possono essere considerevoli e ciò è particolarmente preoccupante nel caso di segnalazioni di persone a fini di sorveglianza discreta o di controlli specifici dato che tali segnalazioni possono essere fatte in base a sospetti.

Il GEPD vorrebbe una giustificazione valida per tale proroga dei periodi di conservazione dei dati. In mancanza di giustificazioni convincenti egli propone di ripristinare i periodi di conservazione attuali e insiste in particolare sul caso delle segnalazioni a fini di sorveglianza discreta o di controlli specifici.

4.6. **Accesso da parte delle autorità competenti per il rilascio della carta di circolazione degli autoveicoli**

Il problema principale è dovuto alla scelta di una base giuridica più che discutibile. La Commissione non riesce a motivare in modo convincente il ricorso ad una base giuridica «settore trasporti» del primo pilastro per una misura che consentirebbe l'accesso al SIS alle autorità amministrative per prevenire e combattere la criminalità (traffico di veicoli rubati). La necessità di una giustificazione credibile e di una base giuridica solida per concedere l'accesso al SIS II è stata illustrata dettagliatamente al punto 4.2.2 del presente parere.

Il GEPD rinvia alle osservazioni formulate al riguardo dall'Autorità di controllo comune di Schengen nel suo parere sulla base giuridica proposta per il SIS II. In particolare occorre dare seguito al suggerimento di quest'ultima di modificare la proposta di decisione per includervi tale accesso.

5. **RUOLO DELLA COMMISSIONE E DEGLI STATI MEMBRI**

Riguardo al SIS II è essenziale una chiara descrizione e attribuzione delle responsabilità, non solo per assicurare il corretto funzionamento del sistema ma anche ai fini del suo controllo. La ripartizione delle competenze di controllo deriverà dalla descrizione delle responsabilità; per questo è necessaria assoluta chiarezza.

5.1. **Ruolo della Commissione**

Il GEPD si compiace del capitolo III di entrambe le proposte, che descrive il ruolo e le responsabilità della Commissione nei confronti del SIS II (ruolo di «gestione operativa»). Questo chiarimento non figurava nella proposta sul sistema di informazione visti (VIS). Questo capitolo tuttavia non definisce in modo esauriente il ruolo della Commissione. Infatti, come menzionato al capitolo 9 del presente parere, la Commissione è coinvolta anche nell'attuazione e nella gestione del sistema tramite la comitatologia.

Per quanto riguarda la protezione dei dati, la Commissione svolge un ruolo già riconosciuto nei sistemi VIS e Eurodac, ossia quello di responsabile della gestione operativa. Se si aggiunge questo ruolo a quello molto importante svolto nello sviluppo e nel funzionamento del sistema, la Commissione potrebbe essere considerata un responsabile del trattamento «sui generis». Come già osservato nel parere del GEPD sul VIS si tratta di un ruolo che, da un lato, va molto al di là del trattamento dei dati ma che, dall'altro, è più limitato di quello di un normale responsabile del trattamento dato che la Commissione non ha accesso ai dati trattati nel SIS II.

Poiché il SIS II sarà fondato su sistemi assai complessi alcuni dei quali fanno ricorso a tecnologie emergenti, il GEPD insiste affinché alla Commissione venga attribuita maggiore responsabilità nell'aggiornamento dei sistemi tramite l'applicazione delle migliori tecnologie disponibili in materia di sicurezza e di protezione dei dati.

Occorre quindi aggiungere nell'articolo 12 delle proposte che la Commissione dovrebbe proporre periodicamente l'applicazione di nuove tecnologie più all'avanguardia in questo settore e che accrescono la protezione dei dati e i livelli di sicurezza e nel contempo agevolano i compiti delle autorità nazionali che hanno accesso a tali dati.

5.2. **Ruolo degli Stati membri**

La situazione degli Stati membri non è effettivamente chiara, poiché è piuttosto difficile sapere a quale (i) autorità spetti il controllo dei dati.

Nelle proposte viene descritto il ruolo dell'ufficio nazionale SIS II (incaricato di garantire l'accesso delle autorità competenti al SIS II) nonché quello delle autorità SIRENE (incaricate dello scambio di tutte le informazioni supplementari). Gli Stati membri devono inoltre garantire il funzionamento e la sicurezza dei rispettivi NS (sistemi nazionali). Non è chiaro se quest'ultima responsabilità spetti a una delle autorità summenzionate. È in ogni caso necessario chiarire tale aspetto.

Per quanto attiene alla protezione dei dati, si dovrebbe considerare che la Commissione e gli Stati membri esercitano il controllo congiuntamente, ciascuno con specifiche responsabilità. Il riconoscimento della complementarietà di tali compiti è la sola possibilità per far sì che nessun aspetto delle attività del SIS II sfugga al controllo.

6. **DIRITTI DELLE PERSONE INTERESSATE**

6.1. **Informazioni**

6.1.1. *Proposta di regolamento*

L'articolo 28 della proposta di regolamento prevede il diritto di informazione delle persone interessate, basandosi principalmente sull'articolo 10 della direttiva 95/46. Si tratta di una modifica salutare rispetto alla situazione attuale nella quale la convenzione non prevede in maniera esplicita alcun diritto di informazione. Si possono tuttavia introdurre ulteriori miglioramenti nei seguenti punti.

Occorrerebbe aggiungere alcune informazioni all'elenco, per contribuire a garantire un trattamento equo delle persone interessate [1]. Tali informazioni riguarderebbero il periodo di conservazione dei dati, l'esistenza del diritto di richiesta di revisione della decisione o di ricorso contro la decisione di effettuare una segnalazione (in taluni casi, si veda l'articolo 15, paragrafo 3, della proposta di regolamento), la possibilità di chiedere assistenza all'autorità incaricata della protezione dei dati, e l'esistenza di mezzi di ricorso.

Nella proposta di regolamento non si trova un'indicazione del momento in cui le informazioni debbano essere fornite. Ciò renderebbe impossibile esercitare i propri diritti alle persone interessate. Affinché tali diritti siano effettivi, il regolamento dovrebbe prevedere un momento preciso in cui le informazioni devono essere fornite, a seconda dell'autorità che ha effettuato la segnalazione.

Una soluzione pratica consisterebbe nell'aggiungere informazioni riguardanti la segnalazione nella decisione che costituisce il motivo della segnalazione in primo luogo: o una decisione giudiziaria o amministrativa motivata da una minaccia per l'ordine pubblico e la sicurezza pubblica (…) o una decisione di rimpatrio o un ordine di allontanamento accompagnato da un divieto di reingresso. Ciò dovrebbe essere aggiunto nell'articolo 28 del regolamento.

6.1.2. *Proposta di decisione*

L'articolo 50 della decisione stabilisce che le informazioni sono fornite su richiesta dell'interessato ed espone gli eventuali motivi di rifiuto di comunicare tali informazioni. Le limitazioni di questo diritto sono naturalmente comprensibili, se si considera la natura dei dati e il contesto in cui sono trattati.

Tuttavia, il diritto di informazione non dovrebbe essere subordinato a una richiesta da parte della persona interessata (che in realtà sarebbe anzi la definizione di una domanda di accesso). Si può supporre che la necessità di «richiedere» le informazioni trovi una giustificazione nei casi in cui la persona interessata non possa essere informata perché non è stata rintracciata.

La questione sarebbe meglio trattata inserendo un'eccezione al diritto di informazione per i casi in cui la comunicazione delle informazioni si riveli impossibile o implichi sforzi sproporzionati. L'articolo 50 dovrebbe essere quindi modificato in tal senso.

---

[1] Si veda per analogia il parere del garante europeo della protezione dei dati concernente l'istituzione del sistema di informazione visti (VIS), punto 3.10.1.

Tale soluzione sarebbe inoltre coerente con l'applicazione del progetto di decisione quadro sulla protezione dei dati nell'ambito del terzo pilastro.

6.2. **Accesso**

Il regolamento e la decisione proposti fissano entrambi termini per la risposta alle domande di accesso, il che rappresenta un'evoluzione positiva. Nondimeno, poiché la procedura per esercitare tale diritto di accesso è definita a livello nazionale, si dà adito alla questione su come i termini previsti nelle proposte possano interagire con le procedure esistenti, specialmente se gli Stati membri fissano termini più brevi per la risposta a una richiesta di accesso. Sarebbe necessario chiarire che debbono essere applicati i termini più favorevoli alle persone interessate.

6.2.1. *Proposta di regolamento*

Vale la pena di notare che le restrizioni al diritto di accesso («La comunicazione dell'informazione alla persona interessata è rifiutata se essa può nuocere all'esecuzione di un compito legale indicato nella segnalazione o ai fini della tutela dei diritti e delle libertà altrui») che figurano attualmente nella convenzione Schengen non compaiono nella proposta di regolamento.

Questo tuttavia è dovuto probabilmente all'applicabilità della direttiva 95/46/CE che prevede (all'articolo 13) la possibilità di applicare deroghe nelle legislazioni nazionali. Occorre far presente che in ogni caso il ricorso all'articolo 13 nella legislazione nazionale per limitare il diritto di accesso deve essere sempre conforme all'articolo 8 della CEDU, e soltanto in casi limitati.

6.2.2. *Proposta di decisione*

La proposta di decisione fa propria la limitazione del diritto di accesso prevista nella convenzione Schengen. Poiché la proposta di decisione quadro contiene essenzialmente le stesse limitazioni del diritto di accesso, l'adozione di tale strumento non comporterebbe una differenza significativa quanto al suddetto aspetto.

Dato che in vari Stati membri l'accesso ai dati raccolti ai fini dell'applicazione della legge è «indiretto» (il che significa che avviene tramite l'autorità nazionale garante della protezione dei dati), sarebbe opportuno prevedere l'obbligo nei confronti delle autorità garanti della protezione dei dati di cooperare attivamente nell'esercizio del diritto di accesso.

6.3. **Diritto di revisione o ricorso contro la decisione di effettuare una segnalazione**

L'articolo 15, paragrafo 3 del regolamento, prevede il diritto di presentare una domanda di revisione della decisione ovvero di proporre ricorso dinanzi un'autorità giudiziaria quando a decidere la segnalazione è un'autorità amministrativa. Si tratta di una positiva integrazione rispetto alla convenzione Schengen attuale.

Questo evidenzia la necessità di disporre di informazioni complete e tempestive sulle persone interessate come si è detto al precedente punto 6.1: in mancanza di tali informazioni questo nuovo diritto resterebbe teorico.

6.4. **Mezzi di ricorso**

L'articolo 30 della proposta di regolamento e l'articolo 52 della proposta di decisione prevedono il diritto di promuovere un'azione ovvero presentare denuncia dinanzi gli organi giurisdizionali di uno Stato membro, se la persona interessata si è vista negare il diritto di accesso, rettifica o cancellazione di dati che la riguardano o il diritto di informazione o di indennizzo.

La formulazione («chiunque nel territorio di qualunque Stato membro») fa ritenere che il ricorrente debba essere fisicamente presente sul territorio per poter promuovere un'azione dinanzi un organo giurisdizionale. Questa restrizione territoriale non trova giustificazione ed è suscettibile di rendere inefficace il diritto ai mezzi di ricorso, considerato che, molto spesso, il ricorrente può promuovere un'azione proprio perché gli viene negato l'accesso alla zona Schengen. Inoltre, per quanto attiene alla proposta di regolamento, dato che la direttiva 95/46/CE è la *lex generalis*, occorre tener conto del relativo articolo 22, il quale stabilisce che «chiunque» ha diritto a un ricorso giurisdizionale, a prescindere dal luogo di residenza. Neanche la proposta di decisione quadro contiene a sua volta una restrizione territoriale. Il GEPD propone di eliminare la restrizione territoriale che figura rispettivamente negli articoli 30 e 52.

7. **CONTROLLO**

7.1. **Osservazione introduttiva: ripartizione delle competenze**

Le proposte ripartiscono i compiti di controllo tra le autorità nazionali di controllo ([1]), da un lato, e il GEPD, dall'altro, ciascuno nel proprio ambito di competenza. Questa impostazione è coerente con l'approccio che le proposte hanno per quanto riguarda la legge applicabile e le competenze per l'esercizio e l'uso del SIS II e risponde alla necessità di un efficace controllo.

Il GEPD accoglie pertanto con favore questo approccio figurante rispettivamente nell'articolo 31 della proposta di regolamento e nell'articolo 53 della proposta di decisione. Tuttavia, ai fini di una migliore comprensione e in un'ottica di chiarificazione dei rispettivi compiti, il GEPD propone che ciascuno dei due articoli sia suddiviso in varie disposizioni, ognuna delle quali sarà dedicata ad un livello di controllo, come si era già opportunamente fatto nella proposta VIS.

([1]) Sono interessate, ma in misura minore, anche le autorità di controllo per l'Europol e l'Eurojust.

7.2. **Controllo da parte delle autorità nazionali garanti della protezione dei dati**

A norma rispettivamente dell'articolo 31 del regolamento e dell'articolo 53 della decisione proposti, ogni Stato membro deve provvedere affinché un'autorità indipendente controlli la liceità del trattamento dei dati personali SIS II.

L'articolo 53 della proposta di decisione aggiunge, per chiunque, il diritto di chiedere all'autorità di controllo di verificare la liceità del trattamento di dati che lo riguardino. Nella proposta di regolamento non è stata introdotta una disposizione analoga in quanto si applica la direttiva come *lex generalis*. Pertanto, si deve considerare che le autorità nazionali garanti della protezione dei dati possano esercitare, per quanto riguarda il SIS II, tutti i poteri loro conferiti dall'articolo 28 della direttiva 95/46/CE, compresa la verifica della liceità di un trattamento di dati. L'articolo 31, paragrafo 1 del regolamento costituisce un chiarimento sui loro compiti ma non può rappresentare una limitazione di tali poteri. Nel testo della proposta di regolamento dovrebbe essere precisato chiaramente che sono loro riconosciuti tali poteri.

Quanto alla proposta di decisione, essa conferisce funzioni più ampie alle autorità nazionali di controllo in quanto la sua *lex generalis* è differente. Tuttavia, una fattispecie in cui le autorità di controllo avessero mansioni e competenze diverse in funzione della categoria di dati oggetto di trattamento non avrebbe senso e, nella pratica, sarebbe molto difficile da gestire. Andrebbe pertanto evitata, sia conferendo a dette autorità poteri identici nel testo stesso della proposta di decisione, sia rinviando ad un'altra *lex generalis* (segnatamente, la decisione quadro sulla protezione dei dati nell'ambito del terzo pilastro) che conferisca competenze più ampie alle autorità garanti della protezione dei dati.

7.3. **Controllo da parte del GEPD**

Il GEPD verifica che le attività di trattamento dei dati siano svolte dalla Commissione in conformità delle proposte. Analogamente, il GEPD dovrebbe poter esercitare tutte le competenze conferitegli nell'ambito del regolamento 45/2001, tenendo peraltro conto dei poteri limitati di cui gode la Commissione in relazione ai dati stessi.

È utile aggiungere che, in conformità dell'articolo 46, lettera f) del regolamento 45/2001, il GEPD «collabora con le autorità nazionali di controllo … se ed in quanto ciò risulti necessario per l'adempimento dei rispettivi obblighi». Tale collaborazione con gli Stati membri in materia di controllo del SIS II scaturisce non soltanto dalle proposte ma anche dal regolamento 45/2001.

7.4. **Controllo congiunto**

Nelle proposte si riconosce parimenti la necessità di coordinare le attività di controllo delle varie autorità interessate. L'articolo 31 della proposta di regolamento e l'articolo 53 della proposta di decisione dispongono che le autorità nazionali di controllo e il garante europeo della protezione dei dati cooperino attivamente tra loro e che il garante europeo della protezione dei dati convochi una riunione a tal fine almeno una volta l'anno.

Il GEPD accoglie con favore questa proposta, che contiene in sostanza gli elementi necessari per instaurare la cooperazione — che è in effetti cruciale — tra le autorità preposte al controllo a livello nazionale e quelle responsabili a livello europeo. Si rilevi che le proposte prevedono una riunione almeno una volta all'anno, ma che questa periodicità va considerata come minima.

Queste disposizioni (agli articoli 31 e 53, rispettivamente della proposta di regolamento e della proposta di decisione) potrebbero tuttavia essere migliorate con qualche precisazione circa il contenuto di un siffatto coordinamento. L'attuale autorità comune di controllo (ACC) è competente ad esaminare i problemi di interpretazione o applicazione della convenzione, a studiare i problemi che potrebbero insorgere allorché vengono esercitati un controllo indipendente o i diritti di accesso e a formulare proposte armonizzate per trovare soluzioni comuni per i problemi esistenti.

Le nuove proposte non possono attenuare l'attuale portata del controllo congiunto. Se è chiaro che le autorità garanti della protezione dei dati possono esercitare, in relazione al SIS II, tutti i poteri di controllo loro conferiti in virtù della direttiva, la cooperazione di dette autorità può riguardare ampi aspetti del controllo del SIS II, comprese le funzioni dell'attuale ACC, conformemente all'articolo 115 della convenzione Schengen.

Tuttavia, affinché ciò sia assolutamente chiaro, sarebbe utile ribadirlo esplicitamente nelle proposte.

8. **SICUREZZA**

La gestione ed il mantenimento di un livello ottimale di sicurezza per il SIS II rappresentano un presupposto essenziale per assicurare un'adeguata protezione dei dati personali conservati nella base di dati. Per ottenere questo livello soddisfacente di protezione, vanno implementate opportune garanzie per gestire i rischi potenziali connessi con l'infrastruttura del sistema e con le persone interessate. La questione è attualmente discussa in vari punti della proposta e mette conto apportare qualche miglioria.

Gli articoli 10 e 13 della proposta contengono varie misure finalizzate a garantire la sicurezza dei dati e specificano i tipi di abuso da evitare. Il GEPD si rallegra che siano state inserite in questi articoli disposizioni riguardanti il controllo (interno) sistematico delle misure di sicurezza.

Tuttavia, l'articolo 59 della proposta di decisione e l'articolo 34 della proposta di regolamento, che dispongono il monitoraggio e la valutazione, dovrebbero riguardare non soltanto gli aspetti dei risultati, del rapporto costi/efficacia e della qualità dei servizi, ma anche l'ottemperanza ai requisiti di legge, specialmente nel settore della protezione dei dati. Il GEPD raccomanda pertanto che il campo di applicazione di questi articoli sia esteso al monitoraggio e all'elaborazione di rapporti sulla liceità del trattamento.

Inoltre, a complemento dell'articolo 10, paragrafo 1, lettera f) o dell'articolo 18 della proposta di decisione e dell'articolo 17 della proposta di regolamento riguardanti le persone autorizzate che hanno accesso ai dati, si dovrebbe aggiungere che gli Stati membri (nonché Europol ed Eurojust) dovrebbero provvedere affinché siano disponibili precisi profili di utente (che, a fini di controllo, dovrebbero essere tenuti a disposizione delle competenti autorità nazionali). Oltre a tali profili, deve essere stilato e tenuto costantemente aggiornato dagli Stati membri un elenco completo di identità degli utenti. Ciò vale, mutatis mutandis, anche per la Commissione.

Queste misure di sicurezza sono integrate da misure di salvaguardia in materia di monitoraggio e organizzazione. L'articolo 14 di entrambe le proposte definisce le finalità della tenuta di registri di tutte le operazioni di trattamento di dati effettuate e le relative condizioni. Questi registri serviranno non soltanto a monitorare la protezione dei dati e assicurare la sicurezza dei medesimi ma anche a consolidare il regolare controllo interno del SIS II disposto dall'articolo 10. I rapporti sul controllo interno contribuiranno a far sì che le autorità di controllo possano espletare efficacemente le loro mansioni, poiché saranno in grado di individuare i punti deboli su cui concentrare la loro attenzione nel quadro della procedura di controllo interno.

Come già precisato in precedenza nel presente parere, il moltiplicarsi dei punti d'accesso al sistema deve essere rigorosamente giustificato, in quanto aumenta automaticamente i rischi di abusi. All'articolo 4, paragrafo 1, lettera b) di entrambe le proposte dovrebbe pertanto essere previsto l'obbligo di comprovare concretamente la necessità di un secondo punto di accesso.

Le proposte non esplicitano chiaramente perché siano necessarie copie nazionali del sistema centrale e suscitano una profonda inquietudine quanto al livello generale di rischio e di sicurezza del sistema:

— il proliferare delle copie aumenta il rischio di abusi (tenuto conto, segnatamente, della presenza di nuovi dati, quali quelli biometrici),

— non si definisce con precisione quale tipo di dati possano essere interessati da queste copie,

— i requisiti di esattezza, qualità e accessibilità di cui all'articolo 9 rappresentano una considerevole sfida tecnica e comportano dunque un aumento dei costi connesso allo stato dell'arte della tecnologia disponibile,

— il controllo di tali copie da parte delle autorità nazionali necessiterà di risorse umane e finanziarie supplementari, che potrebbero non essere sempre disponibili.

Considerati i rischi in causa, il GEPD non è convinto né della necessità di realizzare copie nazionali (tenuto conto delle tecnologie disponibili) né del loro valore aggiunto. Egli raccomanda di eliminare la possibilità, per gli Stati membri, di utilizzare copie nazionali.

Tuttavia, nell'eventualità che si debbano elaborare copie nazionali, il GEPD rammenta che al loro uso a livello nazionale va applicato un principio di rigorosa limitazione delle finalità. Analogamente, la copia nazionale non deve mai poter essere chiesta secondo modalità diverse da quelle stabilite dalla banca dati centrale.

La liceità dell'operazione di trattamento dei dati personali poggia sul rigoroso rispetto della sicurezza e dell'integrità dei dati. Il GEPD controllerà con efficacia tali processi soltanto se attraverso l'analisi delle registrazioni disponibili gli sarà possibile controllare, oltre alla sicurezza dei dati, anche la loro integrità. È pertanto necessario aggiungere all'articolo 14, paragrafo 6, l'«integrità dei dati».

9. **COMITATOLOGIA**

Le proposte prevedono il ricorso a procedure di comitatologia in vari casi in cui per l'attuazione o la gestione del SIS II sono necessarie scelte tecnologiche. Come enunciato nel parere relativo al VIS, per motivi analoghi, queste scelte avranno un impatto determinante sulla corretta attuazione del principio della finalità e della proporzionalità.

Il GEPD suggerisce che le decisioni che hanno un impatto significativo sulla protezione dei dati, quali ad esempio quelle riguardanti l'accesso ai dati e l'inserimento di dati, lo scambio di informazioni supplementari, la qualità dei dati e la compatibilità tra le segnalazioni, l'ottemperanza ai requisiti tecnici delle copie nazionali, ecc., siano assunte tramite un regolamento o una decisione, preferibilmente nel quadro di una procedura di codecisione [1].

[1] Si vedano, in tal senso, il parere del GEPD sul sistema di informazione visti, punto 3.12, e il parere del GEPD sulla proposta di direttiva riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica, del 26 settembre 2005, punto 60.

Per tutti gli altri casi che hanno ripercussioni sulla protezione dei dati, il GEPD dovrebbe avere la possibilità di formulare un parere sulle scelte operate da tali comitati.

Agli articoli 60 e 61 della decisione e all'articolo 35 del regolamento proposti andrebbe inserito il ruolo consultivo del GEPD.

Nel caso più specifico delle norme tecniche per le connessioni tra le segnalazioni (articolo 26 del regolamento e articolo 46 della decisione), va spiegato perché siano necessarie modalità diverse in termini di comitatologia (ruolo consultivo per la decisione e ruolo regolamentare per il regolamento).

10. **INTEROPERABILITÀ**

Poiché non è ancora disponibile la comunicazione della Commissione sull'interoperabilità dei sistemi UE emergenti, è difficile valutare correttamente il valore aggiunto delle sinergie previste ma non ancora definite.

Al riguardo, il GEPD rinvia parimenti alla dichiarazione del Consiglio sulla lotta al terrorismo, del 25 marzo 2004, in cui si invita la Commissione a presentare proposte intese a migliorare l'interoperabilità e potenziare le sinergie tra i sistemi di informazione (SIS, VIS e Eurodac). Rimanda inoltre alle discussioni in corso sull'organismo cui potrebbe essere affidata in futuro la gestione dei vari sistemi su vasta scala (si veda anche il punto 3.8 del presente parere).

Il GEPD ha già dichiarato nel suo parere sul Sistema di informazione visti che l'interoperabilità è un presupposto fondamentale e vitale per l'efficienza dei sistemi informatici su vasta scala, quali il SIS II. Essa offre la possibilità di ridurre i costi globali in maniera consistente e di evitare ridondanze naturali di elementi eterogenei.

— L'interoperabilità può inoltre contribuire all'obiettivo rappresentato dal mantenimento di un elevato livello di sicurezza in uno spazio senza controlli alle frontiere interne tra gli Stati membri, 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 Stati membri dell'UE è fortemente auspicabile; in effetti le segnalazioni inviate dalle autorità di uno Stato membro devono essere interoperabili con quelle inviate dalle autorità di qualsiasi altro Stato membro,

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

Tra le misure di salvaguardia disponibili che possono contribuire a limitare la finalità del sistema ed impedire lo «slittamento di funzione», figura l'utilizzo di norme tecnologiche differenti. Inoltre, qualsiasi forma di interazione tra due sistemi diversi dovrebbe essere documentata in modo esauriente. L'interoperabilità non dovrebbe mai condurre ad una situazione in cui un'autorità, non autorizzata ad accedere a taluni dati o ad utilizzarli, può ottenere tale accesso tramite un altro sistema di informazione. Da quanto si può evincere dalla lettura delle proposte, sembra, ad esempio, che nei primi anni del SIS II non sarà disponibile un sistema di identificazione automatizzato delle impronte digitali (AFIS); si fa soltanto riferimento ad un futuro motore di ricerca sulla base di parametri biometrici. Se si prevede uno scenario in cui saranno utilizzati AFIS provenienti da altri sistemi UE, esso dovrebbe essere chiaramente documentato ed essere corredato delle indispensabili misure di salvaguardia che siffatte sinergie richiedono.

Il GEPD desidera sottolineare ancora una volta che l'interoperabilità dei sistemi non può essere attuata in violazione del principio di limitazione delle finalità e che qualsiasi proposta in materia dovrebbe essergli sottoposta.

11. **SINTESI DELLE CONCLUSIONI**

11.1. **Osservazioni di ordine generale**

1. Il GEPD accoglie con soddisfazione vari aspetti positivi di queste proposte, che su alcuni punti rappresentano un miglioramento rispetto alla situazione attuale. Riconosce che le disposizioni sulla protezione dei dati, in generale, sono state redatte con grande cura.

2. Il GEPD sottolinea che il nuovo regime giuridico, per quanto complesso, dovrebbe

   — assicurare un elevato livello di protezione dei dati,

   — essere affidabile sia per i cittadini che per le autorità che si comunicano i dati,

   — essere coerente nella sua applicazione ai vari contesti (primo o terzo pilastro).

3. Inoltre, l'aggiunta di nuovi elementi nel SIS II, che ne accrescono il possibile impatto sulla vita delle persone, dovrebbe essere corredata di misure di salvaguardia più rigorose, descritte nel parere. In particolare,

   — non può essere concesso l'accesso ai dati del SIS II a nuove autorità, senza che ciò sia rigorosamente motivato. Tale accesso dovrebbe inoltre essere quanto più possibile limitato, sia in termini di dati accessibili che di persone autorizzate ad accedervi,

   — l'interconnessione delle segnalazioni non deve mai condurre, nemmeno indirettamente, ad una modifica dei diritti di accesso,

   — un atto legislativo non adottato non può essere considerato un valido motivo per inserire dati nel SIS II (segnalazioni ai fini della non ammissione),

   — occorre riesaminare la scelta della base giuridica su cui fondare l'accesso da parte delle autorità competenti per il rilascio delle carte di circolazione dei veicoli, in quanto detto accesso è destinato principalmente a lottare contro la criminalità,

   — il GEPD riconosce che l'uso di dati biometrici può migliorare le prestazioni del sistema ed aiutare le vittime di furti di identità. L'impatto dell'inserimento di tali dati nel sistema non sembra essere stato analizzato sufficientemente in profondità e l'affidabilità di tali dati sembra tuttavia essere stata sopravvalutata.

11.2. **Osservazioni specifiche**

1. Il GEPD si compiace che la Commissione abbia riconosciuto che il regolamento 45/2001 si applica a tutte le attività di trattamento dei dati nel SIS II svolte dalla Commissione, in quanto ciò contribuirà ad assicurare un'applicazione coerente ed omogenea delle norme riguardanti la tutela dei diritti e delle libertà fondamentali delle persone in relazione al trattamento dei dati personali.

2. Per assicurare una rigorosa limitazione della finalità a livello nazionale, il GEPD raccomanda di introdurre nelle proposte riguardanti il SIS II (segnatamente all'articolo 21 della proposta di regolamento e all'articolo 40 della proposta di decisione) una disposizione avente un effetto identico a quello dell'attuale articolo 102, paragrafo 4 della convenzione Schengen che limita, per gli Stati membri, la possibilità di prevedere un utilizzo dei dati non previsto nei testi riguardanti il SIS II.

3. Nell'accordare ad un'autorità l'accesso ai dati del SIS II andrebbero applicate condizioni rigorose:

   — l'accesso deve essere compatibile con la finalità generale del SIS II e coerente con la sua base giuridica,

   — va comprovato che è necessario accedere ai dati del SIS II,

   — l'uso che si farà dei dati deve essere precisato esplicitamente ed in modo restrittivo,

   — le condizioni dell'accesso devono essere ben definite e limitate. In particolare, dovrebbe esistere un elenco aggiornato di persone autorizzate ad accedere al SIS II anche per Europol ed Eurojust,

   — il fatto che a tali autorità sia accordato l'accesso ai dati del SIS II non può in alcun caso costituire un motivo per inserire o conservare dati nel sistema se essi non sono utili per la segnalazione specifica di cui fanno parte,

   — il periodo di conservazione dei dati non può essere esteso se la proroga non è necessaria per lo scopo per il quale sono stati inseriti i dati.

4. Nel caso specifico di Europol e di Eurojust, il GEPD esorta la Commissione a definire in modo restrittivo i compiti per il cui espletamento l'accesso sarebbe giustificato. L'accesso da parte di Europol e di Eurojust, inoltre, dovrebbe essere limitato ai dati relativi a persone il cui nome già figura nei loro schedari. Si suggerisce parimenti, per Europol ed Eurojust, di accordare un unico punto d'accesso.

5. Per quanto riguarda le segnalazioni ai fini della non ammissione, le disposizioni che si basano su atti normativi non ancora adottati dovrebbero essere rimosse o riformulate in modo da permettere alle persone, in base alla legislazione vigente, di sapere esattamente quali misure le autorità possano adottare nei loro confronti.

6. I periodi di conservazione dei dati sono stati estesi senza fornire una valida motivazione. In assenza di una giustificazione convincente, dovrebbero essere riportati alla loro attuale durata, in particolare nel caso delle segnalazioni ai fini della sorveglianza discreta o dei controlli specifici.

7. La funzione della Commissione è descritta come funzione di responsabile della gestione operativa. A fianco del significativo ruolo che le compete in materia di sviluppo e manutenzione del sistema, il suo ruolo andrebbe visto come ruolo di responsabile del trattamento sui *generis*. Si tratta di una funzione che trascende di gran lunga quella del semplice trattamento, pur essendo più limitata di quella di un responsabile del trattamento ordinario, dal momento che la Commissione non ha alcun accesso ai dati trattati nel SIS II.

   Nel quadro di tale ruolo, si dovrebbe aggiungere all'articolo 12 di entrambe le proposte che la Commissione dovrebbe regolarmente proporre l'attuazione di nuove tecnologie rappresentanti lo stato dell'arte in questo settore, che rafforzeranno i livelli di protezione e di sicurezza dei dati.

8. Quanto al ruolo degli Stati membri, occorre chiarire quali autorità svolgano la funzione di responsabile del trattamento.

9. Per quanto riguarda l'informazione della persona interessata:

   — nella proposta di regolamento, si dovrebbero aggiungere all'elenco attuale alcuni elementi informativi: il periodo di conservazione dei dati, l'esistenza del diritto di presentare domanda di revisione della decisione di effettuare una segnalazione o di proporre ricorso, la possibilità di ottenere assistenza dall'autorità garante della protezione dei dati, nonché l'esistenza di mezzi di ricorso.

     Inoltre, per quanto riguarda il momento in cui comunicare queste informazioni, si dovrebbe aggiungere l'obbligo di comunicare le informazioni riguardanti la segnalazione nella decisione su cui in origine si basa la segnalazione stessa:

   — nella proposta di decisione, occorre modificare l'articolo 50 in modo da non subordinare il diritto di informazione ad una richiesta della persona interessata.

10. Per quanto riguarda i termini di risposta ad una richiesta di accesso, il fatto che nelle proposte siano stabiliti dei termini è positivo. Qualora anche le legislazioni nazionali prevedano dei termini, occorre precisare chiaramente che vanno applicati quelli più favorevoli alla persona interessata.

    Inoltre, sarebbe utile prevedere, per le autorità garanti della protezione dei dati, l'obbligo di collaborare attivamente all'esercizio del diritto di accesso.

11. Quanto al diritto di proporre ricorso, il GEPD suggerisce di stralciare dall'articolo 30 e dall'articolo 52 la limitazione territoriale.

12. In relazione alle competenze delle autorità nazionali garanti della protezione dei dati:

   — nel regolamento: occorre prevedere che esse possano esercitare, in relazione al SIS II, tutte le competenze conferite loro dall'articolo 28 della direttiva 95/46/CE; ciò dovrebbe essere precisato nel testo della proposta di regolamento,

   — quanto alla proposta di decisione: alle autorità di controllo dovrebbero essere attribuiti poteri identici nel regolamento e nella direttiva.

13. Per quanto riguarda le competenze del GEPD: il GEPD dovrebbe poter esercitare tutte le competenze conferitegli a norma del regolamento 45/2001, tenendo conto, tuttavia, dei limitati poteri della Commissione per quanto riguarda i dati stessi.

14. Quanto al controllo coordinato: nelle proposte si riconosce altresì la necessità di coordinare le attività di controllo delle varie autorità interessate. Il GEPD considera positivo il fatto che esse contengano in sostanza gli elementi necessari per instaurare la cooperazione tra le autorità preposte al controllo a livello nazionale e quelle responsabili a livello europeo. Queste disposizioni (l'articolo 31 della proposta di regolamento e l'articolo 53 della proposta di decisione) potrebbero tuttavia essere migliorate con qualche precisazione circa il contenuto di un siffatto coordinamento.

15. Gli articoli 10 e 13 della proposta contengono varie misure relative alla sicurezza dei dati; l'inserimento di disposizioni relative ad un controllo interno sistematico delle misure di sicurezza è positivo.

   — Tuttavia l'articolo 59 della proposta di decisione e l'articolo 34 della proposta di regolamento, che dispongono il monitoraggio e la valutazione, dovrebbero riguardare non soltanto gli aspetti dei risultati, del rapporto costi/efficacia e della qualità dei servizi, ma anche l'ottemperanza ai requisiti di legge, specialmente nel settore della protezione dei dati. Queste disposizioni dovrebbero essere modificate di conseguenza.

   — Inoltre, a complemento dell'articolo 10, paragrafo 1, lettera f) o dell'articolo 18 della proposta di decisione e dell'articolo 17 della proposta di regolamento, si dovrebbe aggiungere che gli Stati membri, Europol ed Eurojust dovrebbero provvedere affinché siano disponibili precisi profili di utenti (che, a fini di controllo, dovrebbero essere tenuti a disposizione delle competenti autorità nazionali). Oltre a tali profili, gli Stati membri devono stilare e tenere costantemente aggiornato un elenco completo di identità degli utenti. Ciò vale anche per la Commissione.

   — La liceità dell'operazione di trattamento dei dati personali poggia sul rigoroso rispetto della sicurezza e dell'integrità dei dati. Il GEPD dovrebbe avere la possibilità di verificare non soltanto la sicurezza dei dati ma anche la loro integrità attraverso l'analisi delle registrazioni disponibili. È pertanto necessario aggiungere all'articolo 14, paragrafo 6, l'«integrità dei dati».

16. L'utilizzo di copie nazionali può comportare molti rischi supplementari. Il GEPD non è convinto né della necessità (in considerazione delle tecnologie disponibili) né del valore aggiunto dell'uso di copie nazionali. Raccomanda di evitare o quantomeno limitare notevolmente la possibilità, per gli Stati membri, di utilizzare copie nazionali. Tuttavia, nell'eventualità che si debbano elaborare copie nazionali, va applicato all'uso che si fa delle medesime a livello nazionale un principio di rigorosa limitazione delle finalità. Analogamente, la copia nazionale non deve in alcun caso poter essere chiesta secondo modalità diverse da quelle stabilite dalla banca dati centrale.

17. In merito alla comitatologia: le decisioni che hanno un impatto significativo sulla protezione dei dati dovrebbero essere assunte tramite un regolamento o una decisione, che prevedano preferibilmente una procedura di codecisione. Allorché si ricorre effettivamente alla comitatologia, agli articoli 60 e 61 della decisione e all'articolo 35 del regolamento si dovrebbe inserire il ruolo consultivo del GEPD.

18. L'interoperabilità dei sistemi non può essere attuata in violazione del principio di limitazione della finalità ed eventuali proposte in materia dovrebbero essere sottoposte al GEPD.

Bruxelles, addì 19 ottobre 2005

Peter HUSTINX

Garante europeo della protezione dei dati