Nel febbraio 2003, il gruppo d'ispezione dell'ACC esaminò approfonditamente gli archivi di lavoro per fini di analisi e concluse che periodi di conservazione più lunghi erano indubbiamente necessari in alcuni casi, ma che, per stabilire se dei dati di natura personale dovessero essere conservati o meno, sarebbe stato più utile ricorrere ad una verifica della necessità dell'archivio, anziché ad un limite temporale fisso.

Convinta di ciò, l'ACC ha quindi proposto di emendare la convenzione Europol in modo che il periodo di conservazione fosse collegato all'archivio anziché ai dati di natura personale in esso contenuti. L'Europol dovrebbe cancellare gli archivi di lavoro dopo un periodo di tre anni, salvo nel caso in cui, alla scadenza di tale periodo, l'Europol non ritenga assolutamente necessaria la prosecuzione di un particolare archivio. In tal caso, l'archivio potrebbe restare aperto per altri tre anni.

Sebbene in tal caso l'Europol avrebbe la possibilità di verificare la necessità dell'archivio alla fine di ogni triennio, una volta presa la decisione di tenere attivo un archivio, l'Europol dovrebbe ripetere la procedura per la costituzione di un archivio di lavoro per fini di analisi di cui all'articolo 10 della convenzione Europol. In tal modo, l'ACC e il consiglio di amministrazione dell'Europol avrebbero la possibilità di esaminare le ragioni per mantenere attivo un determinato archivio e il processo sarebbe tenuto sotto controllo, eliminando l'eventualità che un archivio resti aperto illimitatamente.

Per impedire che i dati personali siano conservati anche quando non è più necessario, è stato proposto che la convenzione continui a prevedere l'obbligo per l'Europol di valutare annualmente la necessità di conservare dati personali presenti negli archivi di lavoro. Inoltre, l'ACC potrà chiedere specificatamente al gruppo d'ispezione di esaminare qualsiasi archivio ancora attivo, nel corso di un'ispezione.

L'emendamento proposto dall'ACC è stato approvato e incluso nella versione finale del protocollo per la modificare la convenzione Europol[1].

Collaborare per promuovere la protezione dei dati

Attualmente le iniziative dell'UE che comportano la raccolta, la conservazione o lo scambio di dati personali ai fini dell'applicazione della legge, sono numerose; tra gli esempi più significativi vi sono misure per consentire lo scambio di dati sui passeggeri di voli aerei nonché proposte per richiedere la conservazione dei dati delle comunicazioni. Questi ed altri sviluppi, quali il suggerimento di trasformare un giorno l'Europol in un'agenzia investigativa, potrebbero avere rilevanti implicazioni per i diritti degli individui. Pertanto, l'ACC ha ricercato la collaborazione di altre autorità che si occupano della protezione dei dati per garantire che i responsabili delle decisioni politiche tengano conto dei problemi legati a questo aspetto.

Per un certo periodo di tempo l'ACC è stata schierata con istituzioni omologhe quali l'autorità di controllo comune di Schengen e l'autorità di controllo comune delle dogane, che hanno il compito di vigilare rispettivamente sul sistema d'informazione di Schengen e sul sistema d'informazione doganale. Tutte e tre le autorità di vigilanza si avvalgono dello stesso segretariato con sede a Bruxelles e, tra le iniziative volte a coordinare le loro attività, è rientrata la creazione di un gruppo di lavoro composto da esperti tecnici delle istituzioni nazionali incaricate della protezione dei dati. Questo gruppo, che è stato istituito per fornire sostegno tecnico alle autorità di controllo comune, sta attualmente sviluppando uno strumento standard per l'ispezione dei sistemi d'informazione del terzo pilastro.

Inoltre, in vista di un invito a presentare resoconto dinanzi a un comitato ristretto della "Camera dei Lord" (House of Lords), le tre autorità di controllo comune hanno di recente tenuto una riunione congiunta insieme ai rappresentanti dell'autorità di controllo comune di Eurjoust, da cui è scaturito un parere comune sulla protezione dei dati nell'ambito del terzo pilastro. Sono previsti ulteriori incontri di questo tipo, per consentire alle autorità di controllo comune di esaminare le questioni di mutuo interesse.

È chiaro, tuttavia, che molte delle nuove iniziative dell'Unione europea che riguardano dati personali non fanno parte di mandati specifici delle autorità di controllo comune e,

(1) Atto del Consiglio del 27 novembre 2003 che stabilisce un protocollo recante modifica alla convenzione Europol.

sicuramente, non tutte rientrano in modo netto in uno dei tradizionali pilastri dell'UE.

Per questo motivo, in occasione della conferenza delle autorità incaricate della protezione dei dati svoltasi a Rotterdam nel 2004, è stato deciso che i rappresentanti di quelle autorità che operano a livello comunitario, si riuniscano per coordinare la loro attività. Alla prima riunione di questo gruppo "di pianificazione", che ha avuto luogo nel giugno 2004, hanno partecipato il garante europeo della protezione dei dati, i presidenti delle autorità di controllo comune, la presidenza del gruppo di lavoro dell'articolo 29, che ha il compito di fornire consulenza alla Commissione su questioni inerenti alla protezione dei dati nell'ambito del primo pilastro.

La situazione si è ulteriormente evoluta nel settembre 2004 in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati a Wroclaw, quando una sessione a porte chiuse delle autorità europee ha approvato una risoluzione in cui si chiede che le istituzioni dell'UE promuovano un forum in cui le autorità europee incaricate della protezione dei dati possano discutere le implicazioni a livello di protezione dei dati degli sviluppi del terzo pilastro. Fino alla creazione di tale forum, le iniziative del terzo pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune, saranno esaminate da un gruppo di lavoro delle autorità europee incaricate della protezione dei dati.

CAPITOLO II
PARTE A - ATTIVITÀ DI VIGILANZA

1. Ispezione dell'Europol

La conduzione d'ispezioni in loco delle attività dell'Europol è uno dei modi adottati dall'autorità di controllo comune per ottemperare al suo mandato generale.

Ispezione - Febbraio 2003

Nel dicembre 2003, l'ACC ha dato incarico al suo gruppo d'ispezione di esaminare gli archivi di lavoro per fini di analisi e i sistemi d'informazione dell'Europol, nonché il grado di conformità agli accordi ufficiali tra Europol e Stati terzi.

Nel febbraio 2003, detto gruppo ha condotto un'ispezione di tre giorni presso l'Europol. Nella relazione finale, approvata nel luglio 2003, si dichiarava che il livello di protezione dei dati all'Europol era migliorato dalla prima ispezione effettuata nel 2000, pur notando che l'Europol aveva incontrato problemi per quanto riguarda la salvaguardia della qualità dei dati. Questo era da imputarsi soprattutto al fatto che l'Europol deve affidarsi alla qualità dei dati ricevuti dagli Stati terzi. L'ACC, pertanto, ha proposto alle autorità nazionali incaricate della protezione dei dati di cercare di risolvere questo problema a livello nazionale.

Nel complesso, il gruppo di ispezione ha concluso che, sulla base dei controlli effettuati durante l'ispezione, il trattamento dei dati di natura personale da parte dell'Europol avveniva nel pieno rispetto delle relative disposizioni in materia, osservando che in alcuni campi particolari, quali la verifica e la registrazione dei dati, l'Europol aveva applicato sistemi conformi ad elevati standard di protezione dei dati.

Sono state quindi formulate delle raccomandazioni con l'intento di migliorare ulteriormente la conformità dell'Europol; un'ispezione di verifica ha avuto luogo nel novembre 2003.

Ispezioni - Obiettivi strategici

È chiaro che il ruolo dell'Europol si sta sviluppando rapidamente, con un numero sempre maggiore di dati trattati. Poiché è ferma convinzione dell'ACC che le ispezioni dell'Europol debbano tenere il passo con tali evoluzioni, nel 2003 l'autorità di controllo comune ha fissato una serie di obiettivi volti a guidare le ispezioni future. In sintesi, gli obiettivi sono i seguenti:

- le ispezioni dell'Europol devono avvenire con scadenza annuale;
- occorre ispezionare con particolare attenzione la qualità dei dati personali conservati da Europol;
- infine, il gruppo di ispezione deve godere di una maggior discrezionalità relativamente

alla portata dell'ispezione, disponendo della duttilità necessaria per esaminare particolari aree di interesse nel momento in cui queste si presentino.

Ispezione - marzo 2004

Tenendo conto di questi obiettivi, l'ACC ha approvato una nuova ispezione dell'Europol, sottolineando che avrebbe dovuto incentrarsi sulla qualità dei dati trattati negli archivi per fini di analisi.

L'ispezione, durata tre giorni, è iniziata il 30 marzo 2004. Prima dell'ispezione, il gruppo aveva scelto un certo numero di archivi di lavoro da esaminare. Per ognuno di essi il gruppo valutava la conformità alla decisione costitutiva dell'archivio per stabilire se le categorie di dati personali conservati e gli Stati membri partecipanti all'attività dell'archivio corrispondessero a quelli elencati nella decisione. Da ogni archivio venivano poi estrapolati dei campioni di dati e la loro qualità era confrontata con quella del documento originale.

Nonostante siano state individuate alcune imprecisioni, nel complesso la qualità dei dati è stata ritenuta soddisfacente, almeno per quanto riguarda la rispondenza dei dati negli archivi con quelli forniti dagli Stati membri. Tuttavia, è stata riscontrata un'incapacità generale da parte degli Stati membri di valutare correttamente i dati (verificando la fonte, l'affidabilità e così via). Ancora una volta, l'ACC ha sottolineato che, per risolvere questo problema, occorre migliorare la cooperazione tra Stati Membri ed Europol.

Inoltre, il gruppo ha rilevato che, in alcuni casi, si presentava una palese divergenza tra quanto indicato nella decisione costitutiva di un particolare file e quanto avveniva in realtà. Per esempio, le decisioni costitutive non sempre comprendevano un elenco recente delle parti che contribuivano all'archivio e, in alcuni casi, soltanto alcune delle categorie di dati riportate nella decisione costitutiva venivano realmente trattate nell'archivio. Il gruppo, pertanto, ha raccomandato all'Europol di procedere ad un esame dell'archivio dopo un certo periodo di tempo dalla sua costituzione (per esempio un anno), per chiarire la natura dei contributi degli Stati partecipanti. La decisione costitutiva dovrebbe poi essere aggiornata per rispecchiare la reale portata della partecipazione.

Il sistema d'informazione dell'Europol

All'epoca dell'istituzione dell'Europol, una delle sue priorità era quella di sviluppare un sistema d'informazione a livello europeo, che avrebbe raccolto informazioni su persone sospettate di essere coinvolte in reati che rientrassero nell'area di competenza dell'Europol. Uno dei compiti principali dell'ACC è quello di controllare detto sistema (il sistema d'informazione dell'Europol) e verificare la sua ottemperanza alle disposizioni sulla protezione dei dati.

È opportuno fornire un breve resoconto dello sviluppo del sistema, che è stato irto di difficoltà.

Il processo di pianificazione e sviluppo del sistema ebbe inizio nel 1996. Questioni di carattere contrattuale emersero sin dall'inizio, aggravati da richieste di aggiunte al sistema (per esempio fu deciso di ampliare il sistema per includere funzionalità relative alla falsificazione dell'euro). Pertanto, ci sono state numerose versioni del sistema nel corso del suo sviluppo. Una versione limitata del sistema che consente all'Europol di scaricare la proprie responsabilità relativamente all'euro, è entrata in funzione nel 2001.

Nella relazione annuale 2003 dell'Europol sono stati illustrati i recenti problemi incontrati con la versione finale del sistema.

"Delivery of the Europol Information System (EIS) ... was planned for February 2003. However, it was not delivered due to the underestimation of the number of problems that would arise... The expected revised delivery date of June was met but when delivered, the product was not up to standard." [La consegna del sistema di informazione dell'Europol (Europol Information System - EIS)... era prevista per febbraio 2003. Tuttavia, la consegna non ha potuto aver luogo perché sono stati sottovalutati gli eventuali problemi... . La prevista data di consegna rivista di giugno è stata rispettata ma, il prodotto si è rivelato al di sotto dello standard richiesto.]

Quando la versione finale del sistema sarà operativa negli Stati membri (è stato anticipato che ciò potrebbe avvenire prima della fine del 2004), l'ACC ha intenzione di collaborare con le autorità nazionali incaricate della protezione dei dati per vigilare attentamente sul sistema, tenendo sotto costante sorveglianza il modo in cui viene utilizzato. Inoltre, una buona parte delle ispezioni future saranno dedicate a esaminare il sistema per garantire che ci si attenga alle disposizioni pertinenti sulla protezione dei dati.

2. Europol - Un ruolo di sostegno

Si continua a discutere in merito alla forma che con precisione deve assumere il sostegno in materia di analisi dell'Europol agli Stati membri. Il problema è sorto inizialmente alla luce di una scoperta fatta dal gruppo di ispezione dell'ACC.

Progetti operativi degli Stati membri con il supporto dell'Europol (MSOPES)

Nel corso della prima ispezione dell'Europol avvenuta nel novembre 2000 il gruppo di ispezione scoprì che l'Europol forniva sostegno in materia di analisi a indagini condotte dagli Stati membri. Questi progetti (noti come *Member States' Operational Projects with Europol Support – MSOPES*, ovvero Progetti operativi degli Stati membri con il supporto dell'Europol) prevedevano la creazione di archivi di lavoro per fini di analisi presso l'Europol, la cui responsabilità, tuttavia, era degli Stati membri anziché dell'Europol.

Nonostante l'Europol abbia il compito generico di contribuire alle indagini negli Stati membri, l'articolo 10 della convenzione Europol stabilisce una procedura da seguire quando si costituiscono archivi per fini di analisi all'Europol. Oltre a stabilire le categorie di dati di carattere personale che possono essere conservate in questi archivi, l'articolo prevede che il direttore dell'Europol dia all'ACC la possibilità di esprimersi sulla decisione costitutiva di un archivio. Gli archivi dei MSOPES, tuttavia, non erano costituiti conformemente a questa procedura. L'ACC puntualizzò che la creazione e l'uso di archivi per fini di analisi all'Europol, doveva essere limitato a quanto previsto dall'articolo 10 della convenzione Europol e che, pertanto, la costituzione degli archivi dei MSOPES era illegittima. In considerazione delle preoccupazioni dell'ACC, il Consiglio ha deciso di non creare un fondamento giuridico per i MSOPES, con la conseguente cessazione del funzionamento degli archivi associati.

Squadre investigative comuni

L'ACC sta attualmente valutando la portata del sostegno in materia di analisi fornito dall'Europol nell'ambito di un'altra struttura. Il Trattato di Amsterdam contemplava l'impegno a creare delle "squadre investigative comuni", con l'auspicio che questi gruppi contribuissero a indagini comuni condotte da due o più Stati.

Una decisione quadro del Consiglio[1] ha introdotto delle regole comuni per queste squadre e ha specificato che potevano includere "funzionari di organismi costituiti ai sensi del Trattato sull'Unione europea", una definizione che interessa anche il personale dell'Europol. I particolari specifici riguardanti la partecipazione di Europol a squadre investigative comuni sono quindi stati definiti in un Protocollo adottato dal Consiglio[2]. Anche se le disposizioni del protocollo stabilivano che il personale dell'Europol doveva partecipare con "funzioni di supporto", gli agenti dell'Europol che seguivano una squadra investigativa comune sarebbero stati inseriti nella catena di comando della squadra e le informazioni dell'Europol sarebbero state condivise direttamente attraverso il componenti della squadra dell'Europol; inoltre le informazioni raccolte dalla squadra sarebbero state inserite nelle banche dati dell'Europol.

L'ACC riconosce che dopo la ratifica da parte degli Stati membri del protocollo recante modifica della convenzione, l'Europol potrà partecipare a squadre investigative comuni e scambiare informazioni con gli altri componenti di una squadra in particolare. Ciò tuttavia non comporta un'aggiunta nell'elenco delle autorità con cui l'Europol è attualmente autorizzato a scambiare informazioni. Tuttavia, se la partecipazione ad una squadra investigativa comune dovesse comportare la creazione di archivi per fini di analisi presso l'Europol, si potrebbe stabilire un parallelo con la situazione verificatasi nel caso dei MSOPES, soprattutto dal momento che nel protocollo non si rinviene alcun fondamento giuridico per la costituzione di archivi per fini di analisi al di fuori di quanto previsto dall'articolo 10.

(1) Decisione quadro del Consiglio del 13 giugno 2002 relativa alle squadre investigative comuni.
(2) Atto del Consiglio del 28 novembre 2002 che stabilisce un protocollo recante modifica della convenzione.

L'ACC ha chiesto informazioni in merito all'esistenza di una eventuale politica formulata dall'Europol riguardante il tipo di sostegno che sarebbe offerto alle squadre investigative comuni. In particolare l'ACC si è informata sul modo in cui l'Europol intende utilizzare i suoi servizi di analisi.

Apparentemente il processo decisionale relativamente al tipo di sostegno da fornire alle squadre investigative comuni quando il protocollo sarà stato ratificato da tutti gli Stati membri, è attualmente in corso. Fino alla ratifica del protocollo, l'Europol potrà assistere le squadre investigative comuni conformemente a quanto previsto dalla convenzione Europol. L'Europol ha comunicato all'ACC che il sostegno fornito alle squadre investigative comuni nel frattempo si limiterà all'analisi di informazioni e di dati in linea con le disposizioni della convenzione, all'individuazione di divari nelle informazioni, alla divulgazione di relazioni analitiche che forniscono valutazioni di informazioni assemblate e all'identificazione di nuovi progetti in seguito all'analisi.

L'ACC ha intenzione di vigilare sulla situazione per assicurare il rispetto della convenzione Europol. Sarà particolarmente interessante vedere come l'Europol interpreterà il suo ruolo nelle squadre investigative comuni dopo la modifica della convenzione.

3. Decisione costitutiva di archivi per fini di analisi

Ogni qual volta l'Europol intenda costituire un nuovo archivio di lavoro per fini di analisi ai sensi dell'articolo 10 della convenzione Europol, è necessario adottare una decisione costitutiva. Tale decisione deve stabilire, tra i vari aspetti, le finalità dell'archivio e le categorie di dati di natura personale che possono essere conservati. Le decisioni devono essere approvate dal consiglio di amministrazione dell'Europol, che è obbligato a sottoporle al parere dell'autorità di controllo comune. È politica dell'ACC esprimere il proprio parere su ogni decisione costitutiva.

Nel periodo trattato dalla presente relazione, l'ACC ha formulato osservazioni relativamente a nove decisioni costitutive di archivi per fini di analisi. Nella maggior parte dei casi non ha espresso alcun commento, anche se in un'occasione l'ACC ha chiesto chiarimenti su un certo numero di punti e ha posto domande in merito all'inclusione di alcune categorie di dati nella decisione costitutiva. Europol ha risposto eliminando queste categorie di dati dalla decisione.

Al momento della stesura della presente relazione, Europol stava trattando dati personali in diciannove diversi archivi per fini di analisi.

4. Accordi con Stati/organismi terzi

Se l'Europol intende trasmettere dati personali al di fuori dell'UE, tale trasmissione deve essere preceduta dalla firma di un accordo ufficiale tra l'Europol e lo Stato in questione. Prima della stipulazione di un accordo di questo genere l'Europol deve ricevere il parere dell'ACC.

Negli ultimi due anni l'Europol ha siglato accordi con i seguenti Stati terzi: Repubblica slovacca, Cipro, Lettonia, Lituania e Malta (tutti questi paesi sono nel frattempo entrati a far parte dell'UE, cessando di essere Stati terzi) nonché Bulgaria e Romania. In tutte le occasioni, ha formulato numerose osservazioni a carattere generale, concludendo, tuttavia, che, sotto l'aspetto della protezione dei dati, non sussistevano impedimenti alla sottoscrizione dell'accordo da parte dell'Europol.

Eurojust

L'Europol ha altresì firmato un accordo ufficiale con Eurojust, l'autorità incaricata di migliorare la cooperazione giudiziaria nell'Unione europea. Nel suo primo parere formulato sull'accordo di massima tra Europol e Eurojust, l'ACC ha rilevato che la decisione del Consiglio che istituiva Eurojust prevedeva che il Consiglio consultasse l'autorità di controllo comune dell'Eurojust prima di approvare l'accordo stesso. Poiché in questo caso la procedura coinvolgeva due organismi di controllo comune, l'ACC dell'Europol ha chiarito che, prima di adottare la posizione definitiva, avrebbe voluto conoscere il parere dell'ACC dell'Eurojust. Visto che l'ACC dell'Eurojust non era ancora operativa all'epoca della formu-

lazione del primo parere dell'ACC dell'Europol (maggio 2003), tale primo parere doveva essere considerato un parere provvisorio sull'accordo di massima.

Nel suo parere provvisorio l'ACC sottolineava che, anche dopo la sottoscrizione dell'accordo, i membri nazionali del collegio di Eurojust avrebbero avuto diritto di ricevere dati personali dall'Europol soltanto nell'ambito dell'articolo 6 della decisione del Consiglio relativa alla costituzione di Eurojust e per nessun'altra finalità. Nel parere si suggeriva anche di modificare l'accordo in modo che Europol ed Eurojust fossero obbligati a rispettare eventuali condizioni relativamente all'uso dei dati trasmessi nell'ambito dell'accordo.

Una volta costituita l'ACC dell'Eurojust, il suo presidente e il sig. Kalk (all'epoca presidente dell'ACC dell'Europol) si sono incontrati per discutere l'accordo. Nel dicembre 2003, l'ACC dell'Europol ha espresso un secondo parere in cui si affermava che non sussistevano più impedimenti al perfezionamento dell'accordo, a condizione che lo scambio di dati iniziasse soltanto dopo l'applicazione da parte di Eurojust di misure supplementari per salvaguardare la sicurezza dei dati.

È possibile prendere visione dei pareri dell'ACC sui vari accordi nel sito web dell'ACC all'indirizzo: http://europoljsb.ue.eu.int.

5. Diritti

La convenzione Europol conferisce ai singoli individui numerosi diritti. Ai sensi dell'articolo 19 della convenzione, chiunque ha diritto di accesso a qualsiasi informazione detenuta da Europol che lo riguarda. Se l'informazione relativa al richiedente risulta errata, la persona interessata può domandare all'Europol di sopprimere o correggere l'informazione in questione.

Dai dati forniti dall'Europol emerge che sono state presentate dieci richieste di accesso nel 2002; nel 2003 sono state inoltrate soltanto sei domande e nel 2004 l'Europol ha fino ad ora ricevuto dieci richieste di accesso (a tutto settembre).

Gli interessati possono chiedere all'ACC di garantire la legittimità e la correttezza delle modalità di raccolta, memorizzazione, trattamento e impiego dei dati personali che li riguardano. Sinora, l'ACC ha ricevuto due richieste di questo tipo e, dopo aver effettuato le verifiche necessarie, è risultato che in entrambi i casi l'Europol aveva agito conformemente alla convenzione Europol.

PARTE B - GESTIONE DELL'AUTORITÀ DI CONTROLLO COMUNE

L'autorità di controllo comune si è riunita nove volte dal novembre 2002 all'ottobre 2004. L'ACC è costituita da rappresentanti delle autorità nazionali incaricate della protezione dei dati degli Stati membri. Un elenco dei membri è riportato nel sito web dell'ACC.

I preparativi all'allargamento hanno costituito una delle sfide che l'ACC ha dovuto affrontare; contestualmente, l'autorità di controllo comune ha riflettuto su come garantire maggiore trasparenza e accessibilità più agevole ai suoi utenti. Una breve sintesi di entrambi gli aspetti è illustrata qui di seguito.

1. Preparativi all'allargamento

In occasione della riunione del giugno 2003, l'ACC ha dato il benvenuto a colleghi degli Stati in fase di adesione. Anche se i dieci Paesi avrebbero aderito all'Unione soltanto nel 2004, i rappresentanti degli Stati in fase di adesione sono stati invitati a partecipare a questa riunione e a quelle future in qualità di osservatori, con la speranza che in tal modo acquisiscano familiarità con i lavori dell'ACC. Prima della riunione, è stato distribuito un questionario con l'intento di raccogliere informazioni sia sulla legislazione in materia di protezione dei dati di natura personale in detti Stati, sia sulla misura in cui tale legislazione si applica alle forze di polizia.

Particolarmente incoraggiante è stato apprendere che le autorità incaricate della prote-

zione dei dati negli Stati in fase di adesione si sono impegnate a fondo per creare rapporti di lavoro con le autorità di polizia. Dai risultati del questionario è emerso che, tra le varie iniziative, le autorità incaricate della protezione dei dati hanno condotto ispezioni sulle procedure adottate dalla polizia, hanno svolto verifiche delle condizioni di sicurezza, hanno tenuto riunioni per discutere la politica da adottare e hanno tenuto formazioni per la polizia su questioni relative alla protezione dei dati personali.

L'ACC ha organizzato una visita dell'Europol per gli osservatori per dare loro un'idea di come l'Europol svolge i suoi vari compiti. Nell'ottobre 2003, le delegazioni di cinque Stati in fase di adesione hanno trascorso due giorni al quartiere generale dell'Europol a L'Aia. Erano presenti anche i rappresentanti delle autorità incaricate della protezione dei dati di Islanda e Norvegia, Stati terzi che beneficiano del diritto di partecipare allo scambio di dati personali.

Nonostante gli Stati in fase di adesione siano entrati a far parte dell'UE nel maggio 2004, le loro delegazioni sono diventate membri a pieno titolo dell'ACC soltanto dopo che i rispettivi Paesi hanno aderito alla convenzione Europol, soddisfacendo tutte le condizioni dell'articolo 46. Dal 1° ottobre 2004, le delegazioni che rappresentano le autorità incaricate della protezione dei dati di Cipro, Repubblica ceca, Ungheria, Lettonia, Lituania e Slovacchia sono diventate membri a tutti gli effetti.

In qualità di membri dell'ACC, questi nuovi colleghi ricopriranno un ruolo cruciale nella protezione dei diritti fondamentali in tutta l'Unione europea allargata.

2. Trasparenza

L'ACC svolge le sue funzioni per conto del pubblico e quindi è importante che l'Accstessa e i suoi processi decisionali siano trasparenti.

Il regolamento interno dell'ACC stabilisce che i documenti prodotti dall'autorità di controllo comune sono riservati, tranne nel caso in cui essa non decida altrimenti. È attualmente in corso una modifica del regolamento che prevede l'inversione di questo principio, per cui tutti i documenti saranno accessibili al pubblico a meno non si ritenga che esiste un interesse pubblico prevalente contro la pubblicazione, per esempio nel caso in cui rendere noto un particolare documento possa compromettere seriamente l'attività dell'Europol.

I documenti saranno messi a disposizione del pubblico o direttamente in forma elettronica (nel sito *web* dell'Acc), oppure in seguito ad una richiesta scritta. Ogni domanda di accesso ad un documento comporterà una valutazione dell'eventuale esistenza di motivi per cui il documento non possa essere messo a disposizione. Nei casi in cui soltanto una parte del documento sia esente dalla proibizione di pubblicazione, il documento sarà nuovamente redatto e sarà fornita la versione parziale.

L'ACC si propone di pubblicare tutti i nuovi pareri unitamente alle decisioni del comitato per i ricorsi nel suo sito web all'indirizzo: *http://europoljsb.ue.eu.int*

CAPITOLO III - IL COMITATO PER I RICORSI

Chiunque ha accesso alle informazioni che lo riguardano in possesso dell'Europol ed ha il diritto di richiedere che tali informazioni siano verificate, corrette o soppresse. Chiunque volesse esercitare uno di questi diritti e non fosse soddisfatto della risposta dell'Europol, può appellarsi al comitato per i ricorsi dell'ACC. Nonostante i suoi componenti facciano parte dell'ACC, il comitato per i ricorsi è un organismo autonomo ed imparziale, e non è condizionato da istruzioni dell'ACC. Le decisioni del comitato per i ricorsi sono definitive per tutte le parti interessate.

Sebbene il comitato per i ricorsi abbia deciso in merito a due casi soltanto nel corso degli ultimi due anni, il numero dei ricorsi è aumentato e attualmente vi sono parecchi casi su cui il comitato deve esprimersi. È ragionevole supporre che il numero di ricorsi continuerà ad aumentare a mano a mano che i cittadini impareranno a conoscere l'Europol e saranno mag-

giormente consapevoli dei propri diritti; il comitato per i ricorsi si è pertanto preoccupato di snellire le sue procedure per assicurare che i ricorsi futuri siano trattati celermente.

I due casi illustrati dettagliatamente qui di seguito hanno portato a decisioni relative a importanti questioni di principio.

Nel primo caso, il comitato per i ricorsi ha deciso che l'Europol deve considerare nel merito ogni richiesta di accesso, anziché applicare un approccio generale.

Nel secondo caso, il comitato per i ricorsi ha deciso che l'Europol deve rispondere ad una richiesta di accesso nella lingua in cui tale richiesta è stata formulata, purché essa sia una delle lingue ufficiali dell'Unione europea.

1. Sintesi del ricorso presentato dal signor Y

Il signor Y si è rivolto all'autorità olandese incaricata delle protezione dei dati per chiedere di accedere ad eventuali dati che lo riguardano in possesso dell'Europol. La richiesta è stata inoltrata all'Europol.

Nella sua risposta, l'Europol ha concluso affermando che:

"Ai sensi dell'articolo 19 della convenzione Europol e della legislazione dei Paesi Bassi, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della convenzione Europol".

In risposta a quest'argomentazione, il sig. Y ha presentato un ricorso al comitato per i ricorsi, lamentandosi del "velo di segretezza" che circondava la decisione dell'Europol.

Il diritto di accesso è sancito dall'articolo 19, paragrafo 1, della convenzione Europol e, nonostante l'estensione di tale diritto non sia specificatamente definita alla luce dell'articolo 14, paragrafo 1 delle convenzione Europol, deve essere considerata alla stregua del diritto definito dall'articolo 8 della convenzione d'Europa del 28 gennaio 1981. Tale diritto consente a chiunque di accertare se sono archiviati dati di carattere personale che lo riguardano e, in caso affermativo, gli conferisce il diritto di prenderne conoscenza. Il ricorso del sig. Y riguardava entrambi gli aspetti del diritto di accesso.

Ai sensi dell'articolo 19, paragrafo 3, il diritto di accesso deve essere esercitato conformemente alla legislazione dello Stato membro presso il quale la persona interessata l'ha fatto valere, in questo caso i Paesi Bassi. L'articolo 19, paragrafo 3, stabilisce altresì che, qualora la legislazione dello Stato membro interpellato preveda la "comunicazione relativa ai dati" (con cui si intende sia la comunicazione di un'eventuale trattamento dei dati, sia la comunicazione dei dati che sono trattati), quest'ultima è rifiutata dall'Europol se ciò è necessario per: il corretto svolgimento delle funzioni dell'Europol; per la protezione della sicurezza e dell'ordine pubblico; per la lotta contro i crimini; oppure per la protezione dei diritti di terzi.

Le eccezioni previste al diritto di accesso agli archivi di polizia ai sensi della legislazione olandese sono molto simili a quelli elencati nella convenzione Europol e il comitato per i ricorsi ha stabilito che le disposizioni sia della convenzione Europol, sia della legislazione olandese impongono che, per ogni richiesta di accesso, si proceda a una verifica della necessità di applicare un'eccezione al pieno esercizio del diritto di accesso. Le eccezioni sono ammesse soltanto se gli interessi della polizia o di terzi contano di più dell'interesse della persona interessata nell'esercizio del proprio diritto di accesso.

L'argomentazione dell'Europol per non confermare, né negare l'esistenza di informazioni in suo possesso riguardanti il sig. Y si basa sull'articolo 19, paragrafo 4 della convenzione Europol. In base a questo articolo, se uno Stato membro obietta alla comunicazione dei dati, l'Europol notifica al richiedente che le verifiche sono state effettuate *senza fornire informazioni che possano rivelargli se abbia o meno informazioni sul suo conto.* L'Europol sosteneva che, per poter adempiere a questo obbligo, non avrebbe mai potuto informare apertamente una persona interessata l'effettiva inesistenza presso l'Europol di dati sul suo conto, poiché, facendolo, si consentirebbe ad altri di dedurre che l'Europol detiene informazioni su di loro,

confrontando le varie risposte ricevute dall'Europol. Pertanto, dire al sig. Y che l'Europol non è in possesso di informazioni che lo riguardano, costituirebbe, stando all'argomentazione, un indiretto inadempimento dell'obbligo di cui all'articolo 19, paragrafo 4.

Il comitato per i ricorsi ha rilevato che anche se l'articolo 19, paragrafo 4, impone all'Europol di tenere conto dei desideri delle parti interessate nel trattamento dei dati di natura personale in questione, le disposizioni non stabiliscono la procedura nei casi in cui non sono conservati dati. Il comitato per i ricorsi ha pertanto decretato che la procedura di cui all'articolo 19, paragrafo 4, non doveva essere considerata come un obbligo per l'Europol alla stessa stregua dell'articolo 19, paragrafo 3. Una richiesta di accesso, quando non ci sono dati trattati, deve sempre essere valutata caso per caso e l'Europol non è libero di decidere in merito alla richiesta basandosi soltanto su di un obbligo che esiste in situazioni in cui è in possesso dati personali trattati.

Dopo aver considerato la risposta dell'Europol alla richiesta di accesso del sig. Y, il comitato per i ricorsi ha concluso che la decisione dell'Europol non si basava su di una valutazione del singolo caso e pertanto non era conforme all'articolo 19, paragrafo 3 della convenzione Europol. L'Europol avrebbe almeno dovuto verificare se le eccezioni menzionate nell'articolo 19, paragrafo 3 della convenzione Europol erano applicabili a questo caso in particolare. In assenza di tale evidenza, o anche di elementi che la suggeriscano, l'Europol non avrebbe dovuto rifiutare una comunicazione.

La decisione dell'Europol è stata ritenuta contravvenire alla legislazione olandese applicabile e all'articolo 19, paragrafo 3, della convenzione Europol. Dopo un'attenta valutazione delle informazioni disponibili, il comitato per i ricorsi ha concluso che in questo caso l'articolo 19, paragrafo 3 della convenzione Europol non poteva giustificare un'eccezione al diritto di accesso e ai sensi dell'articolo 19, paragrafo 7 di tale convenzione e ha decretato che l'Europol avrebbe dovuto chiarire al sig. Y che nessun dato che lo riguardava era stato trattato.

2. Sintesi del ricorso presentato dal sig. Z

Dopo aver inoltrato una richiesta di accesso (attraverso l'autorità incaricata della protezione dei dati), il sig. Z ha ricevuto una risposta dall'Europol, in cui si dichiarava quanto segue:

"In conformità con la procedura stabilita dalla convenzione Europol e della legislazione del Belgio, desidero comunicarLe che, facendo seguito alla sua richiesta sono state compiute le verifiche negli archivi dell'Europol. Ai sensi dell'articolo 19 della convenzione Europol e della legislazione del Belgio, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della convenzione Europol".

Il sig. Z ha presentato ricorso al comitato per i ricorsi, comunicandogli successivamente che poiché aveva "scelto l'olandese come lingua ufficiale" voleva una traduzione della decisione dell'Europol, che era stata fornita soltanto in inglese. Il ricorso del sig. Z è stato riconosciuto ammissibile per quanto attiene al suo reclamo di non aver ricevuto una risposta nella propria lingua.

Il comitato per i ricorsi ha chiesto all'Europol perché avesse risposto in inglese, dato che tutta la corrispondenza con il sig. Z era stata in olandese.

L'Europol, a sua volta, ha informato il comitato che rispondere alle domande relative all'articolo 19 in inglese costituiva la procedura standard, tranne nel caso in cui il richiedente chiedesse esplicitamente di volere ricevere una risposta nella propria lingua, nel qual caso l'Europol cercava di soddisfare la richiesta purché ciò non richiedesse eccessivo sforzo. L'Europol non era stato informato, se non dal comitato per i ricorsi, del desiderio del sig. Z di ricevere la traduzione in olandese della risposta alla sua domanda di accesso.

La convenzione Europol non prevede un regime linguistico specifico per l'Europol. Tuttavia, ai sensi dell'articolo 14 della convenzione, il diritto di accesso alle informazioni in possesso dell'Europol deve essere considerato alla stessa stregua di quello contemplato dall'articolo 8 della convenzione del 1981 del Consiglio d'Europa relativo alla protezione dei

dati. L'articolo 8 della convenzione del Consiglio d'Europa dispone che ogni persona deve ottenere la conferma dell'esistenza o meno nel casellario automatizzato dei dati di carattere personale a essa relativi, come pure la trasmissione di tali dati "in forma intelleggibile". Il comitato per i ricorsi ha ritenuto che la lingua in cui le informazioni sono state fornite era rilevante per stabilire se una risposta poteva essere considerata intelleggibile.

Considerando l'Europol un organismo dell'Unione europea che prevede l'attiva partecipazione delle autorità incaricate del rispetto della legge nei singoli Stati membri, il comitato per i ricorsi ha suggerito che, nei casi di domande di accesso ai sensi dell'articolo 19 della convenzione Europol, esso applichi un regola simile a quella contemplata dall'articolo 21 del Trattato che istituisce la Comunità europea, il quale prevede che chiunque scriva a uno qualsiasi degli organismi dell'UE in una lingua ufficiale dell'Unione, riceva una risposta in quella stessa lingua.

Il comitato per i ricorsi ha pertanto deciso che l'Europol non aveva ottemperato ai principi dell'articolo 8 della convenzione del 1981 del Consiglio d'Europa nel rispondere alla richiesta di accesso del sig. Z: l'Europol avrebbe dovuto comunicare la sua decisione nella lingua impiegata dal sig. Z, anche se egli non l'aveva richiesto esplicitamente. Poiché il diritto di accesso ha lo scopo di consentire alle persone interessate di accertarsi che le informazioni che le riguardano siano archiviate conformemente alla legge, l'Europol deve rispondere ai richiedenti nella loro lingua, se questa è una lingua ufficiale dell'UE.

In conclusione il comitato ha osservato che, poiché l'Europol aveva poi fornito al sig. Z una traduzione in olandese della decisione originale, il caso era chiuso. Il comitato per i ricorsi ritiene che l'Europol da allora abbia aggiornato le sue procedure e che adesso risponda alle richieste di accesso nella lingua utilizzata dal richiedente.

È possibile prendere visione di tutte le decisioni del comitato per i ricorsi, unitamente ad altre informazioni sui diritti sanciti dalla convenzione Europol, nel sito web dell'ACC all'indirizzo: http://europoljsb.ue.eu.int

CAPITOLO IV - GLI ULTIMI DUE ANNI

Il primo capitolo della presente relazione fornisce un resoconto del modo in cui l'ACC ha affrontato due situazioni diverse che si sono verificate proprio nel momento in cui l'UE è stata costretta a riflettere sulla sua sicurezza.

Nel trattare questi due casi, l'ACC ha adottato un approccio pragmatico. Il parere dell'ACC sull'accordo dell'Europol con gli Stati Uniti, con il suo riconoscimento della necessità di migliorare la cooperazione, è stato oggetto di critiche da parte di certi ambienti. Ciononostante, l'ACC continua a tener fede al suo impegno di vigilare sull'attuazione dell'accordo per assicurare che questa sia conforme con le disposizioni dell'accordo stesso.

L'ACC ha adottato un atteggiamento proattivo nel proporre la modifica della convenzione Europol e la proposta in sé rispecchia la convinzione dell'ACC che le disposizioni relative alla protezione dei dati contenute nella convenzione Europol non vogliono essere un ostacolo al lavoro dell'Europol, bensì esistono per garantire il rispetto dei diritti dei singoli da parte dell'Europol nello svolgimento dei suoi compiti legittimi.

Anche se l'aggiunta di nuovi colleghi provenienti da dieci nuovi Stati membri ha ovviamente fatto una notevole differenza per l'ACC come organismo, l'allargamento è risultato un fatto positivo e l'ACC sta oggi beneficiando del patrimonio di esperienze dei suoi nuovi membri.

L'ACC ha continuato a svolgere la sua funzione di vigilanza, esaminando tutti gli accordi che l'Europol ha formulato con Stati ed organismi terzi e verificando le decisioni di costituzione di archivi. L'ACC attribuisce una notevole importanza alle ispezioni dell'Europol, in quanto forniscono ai gruppi d'ispezione un'esperienza diretta del lavoro dell'Europol e danno un'idea di come le procedure scritte volte alla salvaguandia dei diritti funzionano realmente nella pratica. L'ACC ha riscontrato che durante queste ispezioni il personale

dell'Europol è estremamente collaborativo e dalle ispezioni di controllo è emerso che l'Europol considera prioritaria l'attuazione delle raccomandazioni dell'ACC.

Nel corso degli ultimi due anni, l'ACC ha cercato di adottare un approccio costruttivo, garantendo nel contempo l'adozione di misure di tutela per salvaguardare i diritti fondamentali.

Il futuro

Ci sono stati molti sviluppi che hanno coinvolto l'Europol negli ultimi due anni e ci sono indicazioni che il ruolo dell'Europol continuerà ad evolversi. La creazione di squadre investigative comuni, per esempio, lascia supporre che le attività dell'Europol siano destinate a diventare di natura sempre più operativa.

Contemporaneamente, degli sviluppi altrove (in particolare i progetti di un sistema d'informazione di Schengen di seconda generazione) hanno suggerito l'idea di rendere interoperativi i sistemi d'informazione dell'Unione con finalità collegate. Tutti questi cambiamenti devono essere affrontati con cautela, specialmente in considerazione dei problemi che sono stati incontrati nello sviluppare il sistema d'informazione dell'Europol. Inoltre qualsiasi intervento in questa direzione dovrebbe essere preceduto da una valutazione del suo impatto sulla privacy, per stabilire le potenziali implicazioni per i diritti delle persone.

Le misure per salvaguardare la protezione dei dati devono andare di pari passo con gli sviluppi, e sarà particolarmente importante assicurare una reale vigilanza dell'Europol, oltreché degli altri sistemi d'informazione a livello europeo. Da parte sua l'ACC ha intrapreso azioni per migliorare la cooperazione con altre autorità incaricate della protezione dei dati nel tentativo di superare le intese alquanto rigide per vigilare sulla protezione dei dati a livello UE. L'ACC si aspetta di contribuire a qualsiasi dibattito relativo a modi per migliorare queste soluzioni.

C'è anche la questione di più vasta portata del controllo parlamentare dell'Europol. Nel 2002 la Commissione ha concluso che le misure di controllo esistenti, adottate per vigilare sull'operato dell'Europol (esercitate dai parlamenti nazionali, dal Parlamento europeo, dalle autorità incaricate della protezione dei dati, dall'ACC e dal consiglio di amministrazione dell'Europol), non erano da considerarsi "giuridicamente insufficienti". Si osservava, tuttavia, che "era necessario qualcosa di più chiaro e trasparente".(1)

Questioni di questo genere non rientrano nell'ambito di responsabilità dell'ACC, ma è chiaro che nel momento in cui i compiti dell'Europol diventeranno sempre più operativi, l'attività di controllo e vigilanza dell'operato dell'Europol dovrà adeguarsi per tenere conto di questo cambiamento.

Obiettivi per i prossimi due anni

Nei prossimi due anni l'ACC si adopererà per:

- svolgere le ispezioni annuali dell'Europol, riservando una particolare attenzione all'attuazione del sistema d'informazione dell'Europol;
- elevare il suo profilo all'interno delle istituzioni dell'UE per assicurare che i problemi relativi alla protezione dei dati siano presi in considerazione al momento della formulazione di nuove iniziative che coinvolgono l'Europol. In particolare, l'ACC ha intenzione di proporre l'instaurazione di regolari contatti con il comitato del Parlamento europeo sulle libertà civili, giustizia e affari interni;
- collaborare con i colleghi dei nuovi Stati membri, aiutandoli a fornire informazioni alle autorità di polizia sulle disposizioni in materia di protezione dei dati della convenzione Europol;
- collaborare con le autorità omologhe e la più vasta comunità che si occupa della protezione dei dati per formulare una risposta coerente e costruttiva alle nuove iniziative che coinvolgono l'impiego di dati personali per finalità legate all'applicazione della legge;
- accrescere la consapevolezza dei diritti conferiti alle persone dalla convenzione Europol;
- continuare a esaminare le decisioni costitutive di archivi e gli accordi per lo scambio di dati di carattere personale con Stati e organismi terzi.

(1) Comunicazione della Commissione al Parlamento europeo e al Consiglio - Controllo democratico dell'Europol 26 febbraio 2002 COM (2002) 95 finale.

Autorità di controllo comune Schengen

55 Il parere 2004 SIS II

1. Introduzione

Nell'intento di garantire che il sistema informativo Schengen di seconda generazione – SIS II – rispettasse gli standard più elevati di protezione dei dati, l'Autorità Comune di Controllo (ACC) si è adoperata per incidere sullo sviluppo del sistema fin dall'inizio.

Nonostante che il Consiglio, nelle conclusioni raggiunte in data 5 e 6 giugno 2003, avesse previsto alcuni requisiti generali per il nuovo sistema, non si è pervenuti ad una decisione definitiva rispetto agli specifici contenuti ed alle funzionalità da includere nel sistema stesso né, elemento questo di essenziale importanza, in merito alle specifiche finalità di questo sistema di seconda generazione[1].

Il presente parere prende in esame l'evoluzione subita dalle finalità per le quali il SIS è stato inizialmente costituito, e passa in rassegna le varie proposte concernenti il SIS II analizzando quali possibili modifiche esse comportino rispetto alla natura del sistema. Infine, sono esposte le motivazioni per le quali l'ACC ritiene che sia necessario giungere quanto prima ad una decisione sui compiti che si intende attribuire al nuovo sistema.

L'ACC continuerà a seguire gli sviluppi del SIS II e fornirà indicazioni più puntuali non appena siano confermate proposte specifiche in merito al sistema.

2. Il Sistema Informativo Schengen

2.1. Il contesto di riferimento

Il SIS è stato costituito inizialmente quale una delle misure compensative previste al fine di consentire la libera circolazione delle persone. Il sistema in quanto tale offriva lo strumento per effettuare controlli alle frontiere ed altri controlli di polizia e doganali.

Poiché le competenti autorità dovevano avere la possibilità di effettuare rapidamente tali controlli, il sistema fu sviluppato secondo una configurazione hit/no-hit. In pratica, ciò significava che la ricerca effettuata nel SIS rispetto ad una determinata persona avrebbe indicato se tale persona era oggetto di una segnalazione e, in caso affermativo, le misure da adottare immediatamente. Si prevedeva che il SIS avrebbe trattato esclusivamente i dati necessari a tal fine, e che ogni ulteriore informazione dovesse essere ottenuta attraverso gli uffici SIRENE.

La Convenzione Schengen ha stabilito chi fosse responsabile del trattamento dei dati contenuti nel SIS, ed ha previsto una serie di garanzie per i diritti degli interessati. Secondo i dati più recenti, nel SIS sono contenute attualmente informazioni relative a circa un milione di individui.

2.2. Il contesto si modifica

Nel 2003, si leggeva quanto segue nelle conclusioni del Consiglio:

"Il SIS è un sistema a configurazione hit/no-hit che consente lo scambio di informazioni

(1) Nel presente documento ogni riferimento alle conclusioni del Consiglio deve intendersi come relativo alle conclusioni dell'incontro del Consiglio europeo nel settore giustizia ed affari interni tenutosi a Lussemburgo il 5 e 6 giugno 2003.

al fine di regolamentare la libera circolazione delle persone e mantenere la pubblica sicurezza, ed in particolare assistere autorità nazionali nella lotta contro la criminalità transnazionale, nel quadro dell'obiettivo fissato dall'UE di mantenere e sviluppare l'Unione come un'area di libertà, sicurezza e giustizia".

Si tratta di una definizione più ampia di quella prevista dall'Articolo 93 della Convenzione di Schengen, e ben segnala il contesto in cui il SIS è venuto a collocarsi dopo l'incorporazione dell'acquis di Schengen nella struttura giuridica e istituzionale dell'Unione europea.

Il potenziamento della cooperazione fra le autorità di polizia nazionali e la creazione di nuovi organismi, come Europol, hanno dato luogo ad una situazione in cui le informazioni detenute nel SIS sono considerate una preziosa risorsa nella lotta alla criminalità ed al terrorismo.

È stato proposto un nuovo Sistema informativo Schengen per fare fronte all'allargamento dell'UE, nella convinzione che tale nuovo sistema avrebbe potuto beneficiare delle nuove tecnologie tenendo conto, al contempo, di altri sviluppi nel settore della giustizia e degli affari interni. È in questo contesto, ed alla luce di questi obiettivi generali, che sono state messe a punto le proposte concernenti il SIS II.

3. SIS II

3.1. Lo sviluppo di un nuovo sistema

Si potrebbe affermare che lo sviluppo di un nuovo sistema del tipo descritto si svolge su tre fronti: il processo decisionale di natura politica, che dovrebbe definire quali siano le finalità previste per il sistema e le relative modalità di funzionamento; il quadro giuridico, che dovrebbe fornire la base giuridica specificando le finalità del sistema e stabilendo le norme relative all'accesso e ad altri elementi; lo sviluppo tecnico del sistema in quanto tale.

La previsione iniziale era che dal Consiglio del giugno 2003 sarebbero dovute emergere proposte ben definite sulle finalità e le funzionalità del SIS II; tuttavia, come sottolineato dal Parlamento europeo nella raccomandazione adottata sul punto, "il Consiglio non ha ancora adottato decisioni in merito a questioni concrete come le nuove categorie di oggetti o persone da inserire".(1)

Questa mancanza di indicazioni univoche ha generato una situazione tale da obbligare la Commissione a formulare una proposta in cui si chiede di garantire la massima flessibilità possibile al nuovo sistema. Pertanto, la messa a punto del sistema avviene sotto l'impulso delle mutevoli istanze provenienti dal settore giustizia e affari interni dell'UE, anziché sulla base di obiettivi espressi e definiti all'interno di un quadro giuridico preciso. Se questo stato di cose dovesse permanere, la natura del sistema potrebbe modificarsi in misura radicale trasformando il SIS II in uno strumento investigativo ed amministrativo multiscopo. Sarebbe un fatto preoccupante che lo sviluppo del SIS II proseguisse in questo modo frammentario, poiché la mancanza di trasparenza connaturata a tale approccio complica la valutazione delle modifiche che tutto ciò comporta rispetto alla natura del sistema stesso.

3.2. SIS II – Uno strumento flessibile

"Fin dalle prime riflessioni sul SIS II è stato chiaro che il sistema dovrebbe essere uno strumento flessibile, ... in grado di adattarsi al mutare delle circostanze e di rispondere, in tempi ragionevoli e senza eccessivi costi e sforzi aggiuntivi, alle richieste formulate dagli utenti durante il suo periodo di operatività".

Il brano sopra riportato è tratto dalle conclusioni del Consiglio del giugno 2003 ed evidenzia un elemento basilare nello sviluppo del SIS II. In effetti, nella sua più recente Comunicazione in merito, la Commissione ha indicato la "flessibilità" fra i requisiti essenziali del nuovo sistema, affermando che "Il SIS II dovrebbe avere le potenzialità per trattare un numero di dati molto più grande e per essere inoltre in grado, una volta che il sistema sarà operativo, di gestire nuovi tipi di informazioni, nuovi oggetti e nuove funzioni, di cui si sta discutendo all'interno del Consiglio".(2)

(1) Raccomandazione del Parlamento europeo al Consiglio sul Sistema informativo Schengen di seconda generazione (SIS II), del 20 novembre 2003.

(2) Comunicazione della Commissione al Consiglio ed al Parlamento europeo: Sviluppo del Sistema di informazione Schengen II e possibili sinergie con un futuro Sistema di informazione visti, dell'11 dicembre 2003.

Il requisito di configurare un sistema flessibile di natura indefinita comporta vari problemi.

In primo luogo, esiste la preoccupazione che un sistema flessibile si presti più facilmente ad una "deriva funzionale", nel senso che le richieste provenienti da un'ampia gamma di organismi ed enti potrebbero dare luogo ad una situazione per cui le informazioni detenute nel sistema verrebbero utilizzate per scopi diversi da quelli inizialmente previsti.

In secondo luogo, è difficile comprendere come sia possibile valutare adeguatamente le implicazioni potenziali del SIS II se il suo sviluppo deve essere flessibile al punto da non fare luce sulla configurazione finale del sistema. La creazione di un sistema caratterizzato da un tale margine di flessibilità in assenza di limitazioni di alcun genere non può che rendere più difficile per chi sta lavorando alla sua messa a punto tenere conto del principio di proporzionalità, che dovrebbe essere uno dei cardini nella definizione di qualsiasi progetto di tale natura.

Man mano che procede lo sviluppo del sistema, ed aumentano gli utenti e le categorie di dati, anche la cornice giuridica dovrà subire un'evoluzione conseguente – non da ultimo perché le garanzie attualmente in vigore per tutelare i diritti degli interessati sono state progettate soltanto in rapporto al SIS nella sua configurazione originale. A parere dell'ACC, il primo passo da compiere al riguardo dovrebbe consistere in una valutazione dell'impatto-privacy per stabilire in quali termini il SIS II e le sue nuove e molteplici funzionalità potrebbero incidere sui diritti degli interessati. Le risultanze di tale valutazione potrebbero successivamente fungere da base per la definizione di una nuova cornice giuridica.

4. SIS II – Le proposte di modifica del sistema

4.1. Accesso al sistema

Le istanze avanzate nei confronti del SIS durante gli ultimi anni riflettono gli sviluppi intervenuti nell'UE per quanto riguarda la lotta alla criminalità ed al terrorismo. Vi è stata, ad esempio, un'iniziativa del Regno di Spagna finalizzata a consentire ad Europol ed Eurojust di accedere al SIS.[1] Permettere a tali soggetti di accedere al sistema comporterà alcune conseguenze sulla natura del SIS II, essendo maggiormente probabile che i dati ricavati dal sistema siano utilizzati operativamente dai due soggetti in questione, ad esempio per quanto riguarda le Squadre Investigative Comuni in ambito Europol. L'ACC resta dell'opinione che le attività in rapporto alle quali si consente l'accesso debbano essere conformi agli articoli della Convenzione Schengen che regolamentano l'accesso a e l'utilizzazione delle informazioni contenute nel sistema.

Consentire che soggetti esterni accedano al SIS può persino modificare radicalmente le finalità per le quali si utilizzano le informazioni presenti nel sistema. In un recente parere su una proposta della Commissione che mirava a concedere l'accesso al SIS alle autorità responsabili dell'immatricolazione dei veicoli, l'ACC ha rilevato che una scelta del genere avrebbe costituito una deviazione rispetto alle finalità originali del sistema in quanto, dando corso alla proposta, il SIS sarebbe stato utilizzato a sostegno della politica comune dell'UE in materia di trasporti.

Ciononostante, la tendenza a consentire ad un numero crescente di soggetti di accedere al SIS sembra destinata a continuare. Il Consiglio ha concluso che altre autorità devono avere la possibilità di accedere al SIS, anche se ciò dovesse comportare la possibilità di "un accesso parziale o per scopi diversi da quelli inizialmente previsti dalla segnalazione".

L'ACC è consapevole dell'essenzialità di un potenziamento della cooperazione fra autorità giudiziarie e di polizia per migliorare la sicurezza in Europa e, in tal senso, potrebbe risultare opportuno consentire ad altri soggetti, in determinati casi, di accedere ai dati presenti nel SIS. Tuttavia, si dovrebbe permettere l'accesso al sistema soltanto se ciò risulti necessario e proporzionato, e non semplicemente perché ne è data la possibilità. È per tale motivo che l'ACC ritiene necessario che si chiariscano le specifiche finalità per le quali Europol ed Eurojust – e qualsiasi altro ente – chiedono di accedere al SIS II. L'adeguamento normativo che dovrebbe accompagnare la messa a punto del nuovo sistema sembra offrire

(1) L'iniziativa è culminata, da ultimo, nell'adozione del Regolamento del Consiglio (CE) n. 871/2004 del 29 aprile 2004.

l'occasione ideale per garantire che le finalità ed i rapporti in questione siano fissati nell'ambito di una chiara cornice giuridica.

Tale cornice giuridica dovrebbe prevedere una serie di limiti all'utilizzabilità dei dati ricavati dal sistema, ed è importante garantire che i soggetti abilitati ad accedere al SIS siano tenuti a rispettare gli stessi standard di protezione dei dati previsti nella Convenzione Schengen ed in altri atti normativi pertinenti, come la Convenzione del Consiglio d'Europa del 1981 sulla protezione dei dati.

L'approccio frammentario seguito nello stabilire quali autorità debbano accedere al SIS continua ad essere fonte di preoccupazione per l'ACC. Nonostante le conclusioni del Consiglio del giugno 2003, e l'intenzione manifestata dalla Commissione di configurare il nuovo sistema con la massima flessibilità possibile, l'ACC ritiene di fare propria la raccomandazione formulata dal Parlamento europeo secondo cui "l'uso dei dati [deve avvenire] per motivi espressamente dichiarati in anticipo". Nella raccomandazione, il Parlamento si opponeva a qualsiasi deroga rispetto a tale principio, "come quella di cui alle conclusioni del Consiglio del 5 e 6 giugno 2003 che chiede lo studio ulteriore della "possibilità per talune autorità di utilizzare i dati SIS a scopi diversi da quelli per i quali essi sono stati inizialmente inseriti nel SIS".

Se si vuole assicurare la possibilità che altri soggetti siano abilitati ad accedere al SIS II una volta che quest'ultimo sia operativo, devono essere stabiliti chiaramente i parametri sui quali basare ogni decisione in materia. Tali parametri dovrebbero essere fissati attraverso norme di rango legislativo che prendano in considerazione, ad esempio, la possibilità di consentire l'accesso sia ai soggetti privati sia a quelli pubblici.

4.2. Le informazioni presenti nel sistema

4.2.1. Ulteriori categorie di dati

Appare verisimile un aumento delle pressioni finalizzate all'ampliamento delle categorie di dati presenti nel sistema, soprattutto perché la proposta di configurare il SIS II come sistema flessibile faciliterà l'aggiunta in futuro di nuove categorie. Vi sono già stati alcuni sviluppi in questo campo. La decisione-quadro del Consiglio che stabilisce un mandato di arresto europeo prevede che le informazioni contenute nel nuovo mandato di arresto siano trattate in ambito SIS. L'aggiunta di nuove categorie di dati potrebbe trasformare il SIS II in un doppione di altri sistemi informativi UE quali il sistema di informazione Europol o il sistema informativo doganale, ed uno sviluppo del genere potrebbe avere riflessi sul livello di protezione dei dati.

L'ACC ritiene che siano necessari parametri univoci onde stabilire quali informazioni possano essere contenute nel SIS II e, ancora una volta, il punto di partenza per giungere ad una decisione in materia non può che essere la valutazione delle finalità del sistema.

4.2.2. Nuove tipologie di dati: identificatori biometrici

Vi sono progetti che prevedono l'introduzione di nuove tipologie di dati, e particolare interesse hanno suscitato i dati biometrici.

Si afferma che è necessario che il SIS II contenga identificatori univoci allo scopo di consentire alle competenti autorità nazionali di risolvere eventuali problemi legati all'identità di singoli individui, e nelle conclusioni del Consiglio si legge che il SIS II dovrebbe permettere "la conservazione, il trasferimento e l'eventuale ricerca di dati biometrici, in particolare fotografie ed impronte digitali".

La Comunicazione della Commissione (dicembre 2003) fornisce alcuni esempi di situazioni nelle quali sarebbe utile disporre di identificatori biometrici. Una di esse riguarda il caso in cui le autorità arrestino una persona in possesso di documenti falsi. Attualmente non sarebbe possibile stabilire, sulla base delle informazioni presenti nel SIS, se sia stata inserita una segnalazione concernente la stessa persona ma sotto altro nome. Tuttavia, se nel sistema fossero conservati anche identificatori biometrici, come le impronte digitali, si potrebbe riuscire a confrontare i rilievi dattiloscopici della persona in oggetto con tutti quelli conservati

nel sistema. In tal modo gli utenti potrebbero stabilire se sia stata inserita o no una segnalazione concernente la stessa persona sotto un altro nome.

In un altro esempio citato per dimostrare l'utilità di accedere a identificatori biometrici, la Commissione menzionava il caso in cui il sistema rilevi uno hit ma la persona in oggetto affermi che la segnalazione riguarda un'altra persona (risulta che i "falsi positivi" siano molto frequenti quando si ha a che fare con nomi di larga diffusione). Si affermava che casi del genere troverebbero rapida soluzione se le autorità potessero confrontare l'identificatore biometrico della persona in oggetto con quello conservato unitamente alla segnalazione presente nel sistema. In tal modo, le autorità sarebbero in grado di stabilire se la persona in oggetto sia realmente quella nei cui confronti era stata inserita una precedente segnalazione.

Questi esempi illustrano i due possibili campi di applicazione delle tecnologie biometriche incorporate in un sistema di informazione. La prima opzione, in cui l'utente effettua una ricerca su tutti gli identificatori biometrici nel sistema fino a trovare una corrispondenza (one-to-many), è nota come sistema di "identificazione"; la seconda opzione, in cui l'identificatore biometrico di uno specifico individuo viene confrontato con una specifica segnalazione presente nel sistema per stabilire se si tratti della stessa persona (one-to-one), è nota come sistema di "verifica".

L'affidabilità dei due sistemi è diversa, come diversi sono gli scopi per i quali i due sistemi possono essere utilizzati; tuttavia, quale che sia il sistema prescelto, siamo di fronte ad un altro esempio di decisione da assumere partendo dalla valutazione delle finalità del sistema ed applicando un test di proporzionalità.

4.2.3. Nuove tipologie di dati: alcune garanzie fondamentali

L'inserimento di dati biometrici comporta tutta una serie di problemi di natura pratica che attendono ancora soluzione (ad esempio, le modalità di raccolta degli identificatori biometrici), e fin quando non saranno disponibili progetti più dettagliati sarà difficile individuare le garanzie ulteriori da prevedere; tuttavia, l'inserimento di dati biometrici richiederebbe quantomeno la definizione di un chiaro quadro giuridico, in cui si stabilisca con precisione in quali circostanze e per quali scopi sia consentito effettuare interrogazioni su dati biometrici. Si tratta di un elemento di particolare importanza, poiché l'inserimento di dati biometrici aumenta la probabilità di una deriva funzionale: vari soggetti, ed in particolare le autorità giudiziarie e di polizia, potrebbero sfruttare la prevista flessibilità del SIS II per chiedere l'accesso a dati biometrici in rapporto ad una molteplicità di scopi.

I rischi sarebbero ancora più consistenti se i dati biometrici fossero conservati nelle sezioni nazionali oltre che nella sezione centrale del SIS II, in quanto le autorità giudiziarie e di polizia dei singoli Stati avrebbero maggiori occasioni di utilizzare tali dati per finalità che esulano da quelle previste nella Convenzione di Schengen.

Per garantirsi contro una simile eventualità, si dovrebbe prevedere la registrazione degli accessi a queste nuove categorie di dati e l'effettuazione di verifiche periodiche del sistema onde assicurare che ai dati si acceda soltanto per scopi legittimi e da parte di soggetti autorizzati. Inoltre, nelle norme concernenti la conservazione di nuove tipologie di dati deve essere specificato con chiarezza che tali dati possono essere conservati esclusivamente per il periodo necessario a raggiungere uno scopo determinato.

4.3. Nuove funzionalità tecniche

Uno dei motivi alla base dello sviluppo del SIS II era la volontà di beneficiare delle nuove tecnologie introducendo nuove funzionalità. Si propone che il SIS II consenta la "interconnessione" delle segnalazioni presenti nel sistema al fine di migliorarne l'efficienza. L'ACC ha indicato che, prima di procedere in tal senso, è necessario prevedere il quadro giuridico di riferimento e, in un precedente parere, ha segnalato che l'interconnessione delle segnalazioni potrebbe permettere agli utenti di accedere ad informazioni per le quali non sono abilitati. Pertanto, l'ACC accoglie con favore l'affermazione contenuta nelle conclusioni del Consiglio, secondo cui è necessario prevedere garanzie atte ad assicurare che l'interconnessione di segnalazioni "non modifichi i diritti di accesso in essere rispetto alle singole categorie di segnalazioni".