COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 10.9.2009
SEC(2009) 937

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

Documento di accompagnamento del

REGOLAMENTO DEL CONSIGLIO

Proposta modificata di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce l'"EURODAC" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (CE) n. [.../...] [che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide]

(Rifusione)

e della

Proposta di

DECISIONE DEL CONSIGLIO

sulle richieste di confronto con i dati EURODAC presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto

SINTESI DELLA VALUTAZIONE D'IMPATTO

{COM(2009) 342 definitivo}
{COM(2009) 344 definitivo}
{SEC(2009) 936}

1. DEFINIZIONE DEL PROBLEMA

Secondo il comitato misto del Consiglio GAI del 12-13 giugno 2007, per conseguire pienamente l'obiettivo di migliorare la sicurezza e per intensificare la lotta al terrorismo, occorre permettere ai servizi di polizia e di contrasto degli Stati membri e all'Europol di avere accesso a determinate condizioni all'EURODAC a fini di consultazione nel quadro dell'esercizio delle loro competenze nel settore della prevenzione, dell'individuazione e dell'investigazione di reati terroristici e di altri reati gravi. La Commissione è stata pertanto invitata a presentare, quanto prima, le proposte necessarie al conseguimento di tale obiettivo.

A segnalare come lacuna tale impossibilità per le autorità di contrasto di accedere all'EURODAC per lottare contro il terrorismo e altre forme gravi di criminalità è anche la comunicazione della Commissione al Consiglio e al Parlamento europeo concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra le banche dati europee nel settore della giustizia e degli affari interni del 24 novembre 2005[1].

L'EURODAC è un sistema su scala comunitaria per il confronto delle impronte digitali dei richiedenti asilo. È stato istituito dal regolamento EURODAC, entrato in vigore il 15 dicembre 2000, che si applica in tutti gli Stati che attuano l'*acquis* di Dublino. Lo scopo dell'EURODAC è facilitare l'applicazione del regolamento Dublino[2] che è inteso a istituire un meccanismo chiaro ed efficace per determinare lo Stato competente per l'esame delle domande di asilo, a impedire il cosiddetto "asylum shopping" e a garantire un accesso efficace alle procedure pertinenti. Tale obiettivo è raggiunto attraverso un sistema di identificazione delle impronte digitali dei cittadini di paesi terzi cui si applica il regolamento, disciplinato da regole rigorosamente definite e armonizzate sulla conservazione, sul confronto e sulla cancellazione delle impronte digitali.

La banca dati contiene soltanto le seguenti informazioni: impronte digitali, Stato membro di origine, luogo e data della domanda di asilo, sesso, numero di riferimento attribuito dallo Stato membro di origine, data di rilevamento delle impronte digitali e data di trasmissione all'unità centrale.

Nell'ambito delle attività di contrasto, mentre gli Stati membri possono accedere senza difficoltà alle impronte digitali dei richiedenti asilo a livello nazionale, la consultazione delle stesse banche dati di altri Stati membri risulta più problematica.

Sebbene esistano attualmente alcuni strumenti UE che permettono ad uno Stato membro di consultare le impronte digitali e altri dati utili a fini di contrasto in possesso di un altro Stato membro, è stata riscontrata una *carenza strutturale in termini di informazione e verifica* per quanto riguarda lo scambio transfrontaliero dei dati dei richiedenti asilo, che rende *molto lunghe e molto onerose le procedure* di cooperazione.

Tale carenza strutturale è riconducibile al fatto che non esiste attualmente un sistema unico accessibile alle autorità di contrasto che consenta loro di determinare quale Stato membro sia in possesso di informazioni su un richiedente asilo. Se interrogando un sistema nazionale automatizzato d'identificazione dattiloscopica (AFIS), ai sensi della decisione 2008/615/GAI del Consiglio sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al

---

1 COM(2005) 597, pag. 6.

2 GU L 50 del 25.2.2003, pag. 1.

terrorismo e alla criminalità transfrontaliera (decisione Prüm) non si ottiene una "risposta pertinente", ciò non significa che non esistano informazioni in un altro Stato membro. Di conseguenza, le autorità di contrasto non sapranno né se esistono informazioni ed eventualmente in quale Stato membro, né addirittura in molti casi se l'informazione si riferisce alla stessa persona, ma saranno informate dell'esistenza di informazioni nella banca dati di un altro Stato membro soltanto se le loro autorità giudiziarie faranno richiesta di assistenza giudiziaria chiedendo all'altro Stato membro di consultare le sue banche dati e di inviare le informazioni pertinenti ai sensi della Convenzione relativa all'assistenza giudiziaria in materia penale[3]. La decisione quadro 2006/960/GAI relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge può essere applicata soltanto quando è noto lo Stato membro in possesso dei dati.

La cooperazione è ostacolata anche dal fatto che gli strumenti attuali non permettono di scambiarsi queste informazioni in modo rapido e agevole. Se non ottiene una risposta pertinente con una ricerca Prüm, lo Stato membro non ha altra scelta che rivolgere una richiesta di assistenza giudiziaria a tutti gli altri Stati membri. Senza un modo efficace per stabilire se un altro Stato membro disponga o meno di informazioni, l'azione delle autorità pubbliche è destinata ad avere costi proibitivi e tempi lunghissimi, compromettendo così seriamente l'applicazione della legge. Disporre delle informazioni in tempi brevi è particolarmente importante per evitare danni a beni o persone, o per proteggere le infrastrutture critiche. L'accesso rapido alle informazioni è necessario anche per impedire la distruzione delle prove di un reato grave o di un tentativo di reato.

2. ANALISI DELLA SUSSIDIARIETÀ

Il diritto dell'UE di intervenire in questo settore discende dal titolo VI del trattato sull'Unione europea relativo alla cooperazione giudiziaria e di polizia in materia penale. Gli attuali strumenti dell'UE per la cooperazione di polizia non sono sufficienti ad agevolare la cooperazione tra gli Stati membri in materia di consultazione e scambio delle impronte digitali dei richiedenti asilo. Senza misure opportune a livello europeo, le autorità di contrasto non saranno in grado di colmare la lacuna strutturale esistente in termini di informazione e verifica.

Europol sostiene che la criminalità transfrontaliera è in espansione e rappresenta uno dei pericoli più gravi per la nostra società. Se non potranno contare su un'efficace ed adeguata collaborazione reciproca, comprendente l'accesso alle informazioni pertinenti in possesso di altri Stati membri, sarà molto difficile, se non impossibile, per le autorità di contrasto degli Stati membri lottare contro tale criminalità. Data la natura stessa di questi reati, occorrono strumenti a livello dell'UE per porre le basi di una cooperazione tra Stati membri.

Inoltre, un'azione a livello europeo contribuirà a garantire l'applicazione di norme armonizzate sulla protezione dei dati; un livello armonizzato di protezione sarebbe difficilmente ottenibile se gli Stati membri dovessero legiferare da soli.

---

[3] Atto del Consiglio, del 29 maggio 2000, che stabilisce, conformemente all'articolo 34 del trattato sull'Unione europea, la convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (GU C 197 del 12.7.2000, pag. 1).

Anche se il numero potenziale di richiedenti asilo suscettibili di essere coinvolti in reati di terrorismo transfrontalieri o in altri reati gravi potrebbe rivelarsi piuttosto esiguo, la gravità di tali reati e il loro impatto sulla società e sulla vita di tutti i giorni dovrebbero bastare da soli a giustificare un'azione a livello europeo.

3. OBIETTIVI DELL'INIZIATIVA

Obiettivi generali:

- prevenzione, individuazione e investigazione di reati di terrorismo e altri reati gravi;
- protezione delle vittime del terrorismo e di altri reati gravi.

Obiettivi specifici:

- rafforzare la sicurezza dell'UE facilitando la verifica dell'identità di alcune categorie di cittadini di paesi terzi, colmando l'attuale carenza strutturale in termini di informazione e rendendo più rapide e meno onerose le procedure di verifica dell'identità di tali persone;
- facilitare l'identificazione delle vittime usando gli stessi mezzi.

Questi obiettivi strategici andrebbero realizzati sempre nel rispetto dei diritti fondamentali, specialmente il diritto di asilo e il diritto alla protezione dei dati personali, imponendo condizioni per l'accesso e adeguate salvaguardie.

4. OPZIONI STRATEGICHE

4.1. Rinuncia ad affrontare il problema a livello UE – Mantenimento dello statu quo (opzione strategica A)

Secondo questa opzione l'UE non dovrebbe prendere iniziative. Le procedure di identificazione e verifica resterebbero lunghe ed estremamente onerose e il risultato incerto.

4.2. Disciplinare l'accesso all'EURODAC a fini di contrasto (opzione strategica B)

Questa opzione stabilisce le basi per l'accesso condizionato all'EURODAC delle autorità di contrasto degli Stati membri e di Europol modificando il regolamento EURODAC e disciplinando l'accesso effettivo ai dati personali contenuti nella banca dati e il loro uso in una proposta di decisione del Consiglio collegata. La risposta pertinente sarebbe accompagnata dall'indicazione del tipo di dati contenuti nell'EURODAC. Le richieste di informazioni supplementari a seguito di una risposta pertinente non sarebbero disciplinate nella proposta di decisione del Consiglio ma dagli strumenti vigenti, come la decisione quadro 2006/960 e l'assistenza giudiziaria reciproca.

Sono previste due possibili subopzioni: i) ricerca sulla base soltanto delle impronte digitali o ii) ricerca sulla base delle impronte digitali e di quelle latenti. Attualmente l'EURODAC non prevede la possibilità di ricerca sulla base di impronte latenti e questa funzione dovrebbe essere aggiunta al sistema. D'altronde, tale funzione è fondamentale nell'azione di contrasto in quanto sul luogo del reato si trovano di solito soltanto impronte latenti.

4.3. Disciplinare l'accesso all'EURODAC a fini di contrasto e lo scambio di informazioni supplementari sui richiedenti asilo (opzione strategica C)

Questa opzione stabilisce le basi per l'accesso condizionato all'EURODAC delle autorità di contrasto degli Stati membri e di Europol modificando il regolamento EURODAC e disciplinando l'accesso effettivo ai dati personali contenuti nella banca dati e il loro uso in una proposta di decisione del Consiglio collegata. La risposta pertinente sarebbe accompagnata dall'indicazione del tipo di dati contenuti in EURODAC. La proposta stabilirebbe inoltre una procedura specifica secondo la quale, a seguito di una risposta pertinente, lo Stato membro richiedente potrebbe chiedere allo Stato membro di origine informazioni supplementari sul richiedente asilo a cui appartiene l'impronta digitale, anziché presentare la sua richiesta ricorrendo agli strumenti vigenti, come nel caso dell'opzione strategica B.

Come per l'opzione strategica B esistono due sottoopzioni: i) ricerca sulla base soltanto delle impronte digitali o ii) ricerca sulla base delle impronte digitali e di quelle latenti.

4.4. Disciplinare l'accesso ai dati nazionali sui richiedenti asilo a fini di contrasto (opzione strategica D)

Questa opzione prevede l'istituzione di un meccanismo di rete decentrato che permetterebbe a ciascuno Stato membro di effettuare ricerche automatizzate nelle banche dati sui richiedenti asilo di tutti gli altri Stati membri. Questi ultimi dovrebbero costituire banche dati nazionali distinte da usare esclusivamente a fini di contrasto e un meccanismo separato per collegare tra loro le banche dati di tutti gli Stati membri. La nuova rete sarebbe creata sul modello dell'EURODAC per quanto riguarda i dati contenuti e le funzioni previste. Il sistema di ricerca sarebbe simile a quello "hit/no hit" istituito dalla decisione Prüm. L'accesso a informazioni supplementari sarebbe reso possibile da disposizioni speciali previste nella decisione EURODAC o dal ricorso agli strumenti vigenti.

I costi di questa opzione strategica sarebbero sproporzionati poiché una scelta in tal senso richiederebbe la creazione di speciali banche dati in ciascuno Stato membro e l'istituzione di un rete complessa per collegare tra loro le banche dati di tutti gli Stati membri. Sembra superfluo e inopportuno creare una struttura tecnica complessa del tutto nuova al solo scopo di permettere alle autorità di contrasto di cercare informazioni che figurano già in una banca dati esistente. Pertanto, questa opzione strategica non è considerata appropriata ed è esclusa.

5. VALUTAZIONE D'IMPATTO

L'impatto delle opzioni strategiche proposte è valutato in relazione ai seguenti criteri:

– rafforzare la sicurezza dell'UE facilitando la verifica dell'identità di alcune categorie di cittadini di paesi terzi e colmando la carenza strutturale in termini di informazione;

– rafforzare la sicurezza dell'UE e facilitare l'identificazione delle vittime assicurando procedure tempestive e meno onerose per la verifica dell'identità;

– impatto sui diritti fondamentali, sul diritto d'asilo e sulla protezione dei dati personali;

– costi di attuazione per le amministrazioni degli Stati membri;

– bilancio dell'UE.

Le opzioni B e C avrebbero un impatto equivalente molto positivo sul rafforzamento della sicurezza dell'UE e lo stesso impatto sui diritti fondamentali. Differiscono però per quanto riguarda i costi di attuazione per le amministrazioni degli Stati membri poiché l'opzione C risulta molto più costosa. L'opzione C comporterebbe costi aggiuntivi per la creazione di una nuova architettura tecnica e amministrativa per lo scambio delle informazioni supplementari. Questi costi potrebbero risultare considerevoli dal momento che gli Stati membri dovrebbero fare in modo che le informazioni supplementari siano fornite entro un certo lasso di tempo e assicurare che siano messe a disposizione rapidamente nei casi d'urgenza.

6. CONFRONTO DELLE OPZIONI

L'opzione del non intervento non serve a migliorare la sicurezza dell'UE. Lo status quo implica che le autorità di contrasto continueranno a non sapere se esistono informazioni su una data impronta digitale, quale Stato membro ne sia in possesso e se le eventuali informazioni si riferiscono alla stessa persona, e a non essere in grado di ottenere tali dati. L'alternativa consistente nel chiedere un'ipotetica assistenza giudiziaria a tutti gli Stati membri è troppo lenta e onerosa per costituire un'opzione realistica.

Le opzioni B e C, che prevedono le proposte necessarie per permettere ai servizi di contrasto di accedere all'EURODAC, presentano il chiaro vantaggio di contribuire a rafforzare la sicurezza dell'Unione facilitando la verifica dell'identità di alcune categorie di cittadini di paesi terzi e colmando la carenza strutturale in termini di informazione, rendendo meno onerose le procedure di verifica dell'identità delle persone in questione e garantendo la possibilità di interrogare la banca dati sulla base di impronte latenti.

Anche se questi obiettivi possono essere raggiunti più efficacemente con l'opzione C rispetto alla B, i costi di attuazione dell'opzione C sono considerati più elevati. Inoltre, allo stato attuale delle cose non c'è motivo di pensare che la decisione quadro 2006/960 non sia uno strumento sufficiente per lo scambio di informazioni supplementari.

L'opzione B permetterebbe comunque di scambiare agevolmente le informazioni, rispettando al tempo stesso le eccezioni e le condizioni che disciplinano lo scambio generale di informazioni a fini di contrasto. Non sembrano sussistere motivi validi per introdurre regole speciali sullo scambio di informazioni relative ai richiedenti asilo, né tantomeno per creare una nuova architettura tecnica e organizzativa (più costosa) per lo scambio di informazioni supplementari, quando i sistemi attuali sono adeguati e adattati a tale scopo. L'opzione B è quindi l'opzione privilegiata.

Questa opzione strategica potrebbe presentare diverse subopzioni. La scelta non è effettuata nella presente valutazione d'impatto ma è lasciata ai responsabili politici.

Una delle subopzioni riguarda il campo di applicazione dello strumento, che sarebbe limitato alla prevenzione, all'individuazione e all'investigazione di reati di terrorismo e altri reati gravi. L'espressione "reati gravi" potrebbe riferirsi: i) all'elenco dei reati gravi di cui alla decisione quadro sul mandato di arresto europeo, secondo quanto auspicato dagli Stati membri, ii) a un elenco ridotto adottato specificamente per questo strumento da cui sarebbero esclusi i reati che potrebbero riguardare in particolare i richiedenti asilo, come l'ingresso illegale, secondo quanto auspicato dai difensori delle libertà civili, o iii) all'elenco previsto nel mandato d'arresto europeo ma con l'introduzione di speciali salvaguardie per i reati riguardanti specificamente i richiedenti asilo.

Un’altra subopzione riguarda le autorità pubbliche a cui consentire l’accesso ai dati EURODAC. Dovrebbe trattarsi delle autorità responsabili della prevenzione, dell’individuazione e dell’investigazione di reati di terrorismo e altri reati gravi. La loro designazione potrebbe essere i) affidata completamente agli Stati membri o ii) soggetta all’approvazione della Commissione. In quest’ultimo caso gli Stati membri dovrebbero informare la Commissione.

Una terza serie di subopzioni riguarda la durata dello strumento. La differenza principale tra le tre subopzioni consiste nel valutare se prevedono o meno una clausola di caducità (sunset clause) ed eventualmente la sua durata.

7. CONTROLLO E VALUTAZIONE

Ciascuno Stato membro effettuerà valutazioni annuali dell’efficacia delle consultazioni EURODAC e, dopo cinque anni dall’entrata in vigore, la Commissione esaminerà il funzionamento della banca dati e presenterà una relazione al Consiglio.