PARLAMENTO EUROPEO

2004 *2009*

Commissione per le libertà civili, la giustizia e gli affari interni

30.9.2008

DOCUMENTO DI LAVORO N. 2

relativo alla comunicazione della Commissione "Preparare le prossime fasi della gestione delle frontiere nell'Unione europea" (COM(2008)0069)

Parte II: approccio comparativo e questioni ancora aperte

Commissione per le libertà civili, la giustizia e gli affari interni

Relatrice: Jeanine Hennis-Plasschaert

1. Programmi di paesi terzi: il modello statunitense

È impossibile negare le somiglianze evidenti che emergono tra le misure proposte nella comunicazione e il programma **US-VISIT (*United States Visitor and Immigrant Status Indicator Technology***). Il programma US-VISIT ha lo scopo di rafforzare la sicurezza dei cittadini statunitensi e di coloro che si recano negli USA, facilitare gli spostamenti legittimi e il commercio, garantire l'integrità del sistema di immigrazione statunitense e proteggere la privacy dei visitatori. Il programma US-VISIT intende raggiungere tali obiettivi attraverso le seguenti misure:

- raccolta, gestione e condivisione delle informazioni su taluni cittadini stranieri che entrano ed escono dagli Stati Uniti;
- identificazione di cittadini stranieri che 1) si siano trattenuti eccessivamente o abbiano violato i termini del loro soggiorno, 2) possano ricevere, prolungare o modificare il loro status di immigrazione oppure 3) debbano essere arrestati o detenuti da funzionari incaricati dell'applicazione della legge;
- individuazione di falsi documenti di viaggio, verifica dell'identità dei visitatori e determinazione dell'ammissibilità dei visitatori con l'ausilio della biometria (impronte digitali e fotografia digitale);
- agevolazione dello scambio e del coordinamento delle informazioni con i funzionari preposti alla gestione dell'immigrazione e delle frontiere.

In seguito ad alcune dichiarazioni formali rese dalle autorità degli Stati Uniti (come "altri paesi stanno adottando il modello US-VISIT per migliorare i sistemi di gestione delle frontiere [...]", "stiamo collaborando con questi paesi per condividere le buone prassi e proseguire verso un approccio unico che consenta spostamenti globali sicuri [...]" e "con l'evoluzione dei mezzi tecnologici di raccolta e utilizzo dei dati biometrici, è possibile rafforzare le capacità esistenti"), la relatrice desidera invitare la Commissione europea (CE) a fornire osservazioni dettagliate circa i colloqui in corso con le autorità statunitensi. La relatrice è ovviamente consapevole del fatto che società e mercati aperti dipendono fortemente da strutture sicure e affidabili e non sta quindi mettendo in dubbio la necessità di un dialogo crescente e ininterrotto con i paesi terzi, ma ritiene che tale dialogo debba essere sempre improntato alla trasparenza. A tale proposito, la relatrice desidera anche sottolineare la necessità di rafforzare il livello di dialogo politico tra i legislatori europei e statunitensi.

Ritiene infatti che sia importantissimo tenere conto degli insegnamenti appresi dagli Stati Uniti. Le relazioni pertinenti fornite dal GAO (*Government Accountability Office* - ufficio per la responsabilità governativa) sono, a tale proposito, particolarmente interessanti. Secondo una recente relazione del GAO "dopo un investimento di circa 1,3 miliardi di dollari nell'arco di 4 anni, il DHS (dipartimento per la sicurezza nazionale) ha attivato circa la metà del programma US-VISIT; ciò significa che in quasi 300 punti di ingresso (POE) aerei, marittimi e terrestri sono attive strutture di verifica dei dati biometrici all'ingresso, ma che non esistono strutture analoghe per l'uscita". Nel medesimo periodo "le strutture operative di ingresso hanno consentito di raggiungere alcuni risultati, in base a quanto riferito, tra cui oltre 1.500 persone sottoposte a misure quali il rifiuto dell'ingresso"[1]. Ciò suggerisce, come messo in

[1] GAO, testimonianza di fronte alla sottocommissione per il controterrorismo alle frontiere, marittimo e globale, commissione per la sicurezza nazionale, Camera dei rappresentanti, 28 giugno 2007, *"Prospects For Biometric US-VISIT*

evidenza dal garante europeo della protezione dei dati (GEPD) nelle sue osservazioni in merito alle misure presentate nella comunicazione, che "l'efficacia in termini di costi di tale sistema non è garantita e che anche gli aspetti economici trarrebbero beneficio da un'attenta valutazione delle esperienze all'estero"[2].

2. Protezione dei dati

I tre cosiddetti nuovi blocchi costitutivi comporterebbero indubbiamente "ampie operazioni di trattamento dei dati personali, con un'invasione significativa della privacy"[3] e potrebbero "portare ad [...] attribuire ai singoli un "punteggio" basato sulla valutazione preventiva del rischio o sulla definizione del profilo"[4]. È quindi alquanto sorprendente che la Commissione non abbia consultato il GEPD e il gruppo di lavoro Articolo 29 prima dell'adozione della comunicazione. Sarebbe opportuno chiedere alla Commissione di procedere a una consultazione prima di qualunque azione basata sulla predetta comunicazione. Lo stesso vale per qualunque proposta futura che preveda la raccolta e/o il trattamento di grandi quantità di dati e la possibile condivisione o messa in comune di tali dati. In questo contesto, occorre valutare, inoltre, quali sono le tecnologie meno invasive, in grado di ridurre al minimo il trattamento dei dati personali e di consentire maggiore sicurezza, conformemente all'approccio "*Privacy by design*" (privacy tutelata nella struttura stessa)[5].

3. Condivisione dei dati con paesi terzi

Se l'UE decidesse di condividere i dati con gli Stati Uniti, si renderebbe necessario concludere accordi specifici, che definiscano i dettagli (come il periodo di conservazione, le persone a cui è consentito accedere ai dati, le tutele speciali per i dati sensibili, i mezzi di ricorso) di ogni singolo strumento. Deve essere chiaro che i *principi* per la protezione dei dati, attualmente in fase di "negoziazione" nel quadro del gruppo di contatto di alto livello UE-USA (HLCG), non avranno alcuno status formale e saranno quindi privi di forza di legge. Come affermato dal commissario Barrot, infatti, i principi non saranno mai sufficientemente dettagliati da consentire di risolvere casi particolari, in un momento in cui ci si appresta a raccogliere informazioni per finalità politiche specifiche.

In questo momento, la relatrice nutre alcune preoccupazioni in merito al sistema US-ESTA. Benché le autorità statunitensi abbiano chiarito che i dati degli individui che vogliono entrare negli Stati Uniti, raccolti ai sensi della legge statunitense, non sono oggetto di negoziazione, la relatrice ritiene che l'UE dovrebbe applicare all'utilizzo dei dati da parte degli Stati Uniti, lo stesso livello di controllo applicato dall'Unione e dai suoi Stati membri (o meglio che essi dovrebbero applicare) all'interno dell'UE. Insiste pertanto sulla massima importanza di definire un approccio coerente e forte, parlando con un'unica voce a nome dell'Unione, invece di far sentire ventisette voci distinte.

In tale contesto, gli interrogativi in merito alla protezione dei dati personali nel quadro del

---

Exit Capability Remain Unclear", GAO-07-1044T.

[2] Osservazioni preliminari del GEPD in merito alla comunicazione COM(2008) 69 def., 3 marzo 2008, pag. 4.

[3] Ibid (n, 2), pag. 1.

[4] Osservazioni congiunte del gruppo di lavoro Articolo 29 e del gruppo di lavoro in materia di polizia e giustizia (*Working party on police and justice*) in merito alla comunicazione COM(2008) 69 def. adottate il 29 aprile 2008, WP 149, pag. 4.

[5] Ibid (n. 4), pag. 5.

sistema US-ESTA, sollevati dalla Commissione nella lettera del 4 agosto 2008 (all'attenzione del segretario statunitense alla sicurezza nazionale Chertoff), sono assolutamente legittimi. Tuttavia, dopo aver letto la risposta statunitense del 15 settembre 2008, la relatrice teme che non sarà possibile ottenere risposte soddisfacenti in tempo utile. La relatrice è altrettanto preoccupata del fatto che la Commissione non sia (a quanto sembra) in grado di fornire una risposta soddisfacente alle domande poste dalle autorità statunitensi (per esempio in che modo le forze di polizia europea utilizzano i dati raccolti attraverso le registrazioni presso gli alberghi per tenere traccia dei viaggiatori stranieri). Inoltre, la relatrice vorrebbe ottenere una risposta dettagliata e concreta circa la dichiarazione resa dal segretario Chertoff nella lettera del 15 settembre che "i sistemi europei operano senza la trasparenza del sistema degli avvisi di registrazione e delle valutazioni di impatto sulla privacy, un aspetto che limita la capacità delle autorità e dei cittadini statunitensi di conoscere i loro diritti e le modalità di trattamento dei loro dati in Europa".

4. Dati biometrici

L'organizzazione internazionale dell'aviazione civile (ICAO) utilizza tre tipi di identificatori biometrici: riconoscimento del volto, riconoscimento delle impronte digitali e riconoscimento dell'iride.

La relatrice è consapevole del fatto che i dati biometrici costituiscono, in teoria, identificatori personali efficaci, poiché le caratteristiche misurate sono considerate tratti distintivi di ogni persona; pertanto, a differenza dell'identificazione convenzionale, i dati biometrici sono ritenuti più affidabili, in quanto impossibili da dimenticare e più difficili da perdere, rubare o indovinare. Nel contempo, la relatrice desidera sottolineare che i dati biometrici non sono mai assoluti né sempre accurati e che tutti i tipi di identificatori biometrici presentano vantaggi e svantaggi. A titolo di esempio, menziona uno studio condotto nel 2005 dal Centro comune di ricerca della Commissione dal titolo "*Biometrics at the Frontiers: Assessing the Impact on Society*" (i dati biometrici alle frontiere: valutazione dell'impatto sulla società) che cerca di fornire un quadro chiaro dei diversi tipi di identificatori biometrici e di analizzare i problemi legati alla diffusione su vasta scala della biometria[6].

La relatrice desidera inoltre rammentare (come già messo in luce dal GEPD) che una serie di persone non sarà in grado di registrarsi, in ragione di impronte digitali illeggibili o dell'assenza di impronte[7]. Ritiene pertanto che sia sempre necessario predisporre soluzioni di ripiego, giacché esse costituiscono una tutela essenziale per l'introduzione della biometria, in quanto i dati biometrici non possono essere forniti da tutti, né sono del tutto accurati[8].

La relatrice vorrebbe sapere, inoltre, se la Commissione intende prendere in considerazione altre tecnologie biometriche come opzioni future (iride) e lavorare pertanto a dati biometrici multimodali, al fine di incrementare l'accuratezza e l'efficienza dei rilevamenti. Desidera anche sapere se è disponibile (oppure se è in fase di elaborazione) un protocollo standard per l'utilizzo e lo scambio di informazioni biometriche, oltre ad accordi in merito al controllo

[6] ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf.
[7] A tale proposito è opportuno osservare che il programma US-VISIT ha previsto due eccezioni alla raccolta di dati biometrici: per i minori di quattordici anni e per le persone con più di 79 anni.
[8] Ibid (n. 2), pag. 5.

delle interfacce che descrivano come verrà utilizzato il protocollo.

5. Conclusioni

L'obiettivo di una gestione realmente integrata delle frontiere è legittimo. È importante continuare a sviluppare e rafforzare la politica comune dell'UE in materia di gestione delle frontiere. È tuttavia impossibile negare che nel quadro della gestione delle frontiere, proposte di ampia portata si stiano accumulando a un ritmo impressionante. L'assenza di un piano generale esaustivo, che definisca l'architettura globale della strategia dell'UE in materia di frontiere, nonché i dettagli di come tutti i programmi e i meccanismi correlati (già attivi, in fase di preparazione oppure in fase di definizione) debbano funzionare collettivamente e le modalità con cui il rapporto tra programmi correlati possa essere ottimizzato, rendono molto difficoltoso disporre di un quadro generale chiaro.

La relatrice sottolinea la necessità di operare, in via prioritaria, una valutazione dei sistemi esistenti e di quelli in fase di preparazione. Sottolinea inoltre che la capacità dell'UE di conseguire i suoi obiettivi strategici dipende in gran parte del suo successo nel gestire le interdipendenze tra programmi correlati. È quindi essenziale definire, gestire e coordinare i programmi dell'UE in materia di frontiere, controlli e immigrazione, affinché tengano conto delle prassi di collaborazione e massimizzino in modo efficace le prestazioni organizzative, oltre a raggiungere obiettivi e risultati organizzativi. In assenza di tale collaborazione, esiste un rischio elevato di sovrapposizioni. Le duplicazioni e le incongruenze nei programmi avranno un effetto negativo sulle prestazioni organizzative e, di conseguenza, sui risultati.

Prima di investire, è fondamentale definire con chiarezza il contesto operativo, per allineare tutte le misure e le iniziative che stanno emergendo. Dovrebbe inoltre essere assolutamente chiaro quali siano le strutture, o le modifiche alle strutture, necessarie per assicurare che la tecnologia e i processi funzionino in modo armonico. Tutti gli investimenti dovrebbero essere giustificati, da un punto di vista economico, in base ai vantaggi conseguiti e dovrebbero produrre valore aggiunto. Per il momento, pare che l'UE continui a non avere una strategia chiara e perfettamente definita e non sappia, di conseguenza, come ottenere risultati efficienti in termini di costi e a prezzi accessibili.

La relatrice riconosce che è arduo trovare il giusto equilibrio tra garantire la libera circolazione di un numero sempre più elevato di persone alle frontiere e assicurare ai cittadini europei maggiore sicurezza e non nega che l'utilizzo dei dati offre vantaggi evidenti. Nel contempo, però, sottolinea che la fiducia dell'opinione pubblica nelle azioni del governo può essere preservata soltanto se vi saranno tutele dei dati e mezzi di ricorso sufficienti; insiste pertanto sulla stretta collaborazione con le autorità per la protezione dei dati a livello europeo e nazionale. È necessario poter sempre disporre di meccanismi adeguati di vigilanza sulla protezione dei dati.