I sistemi di prescreening dei passeggeri e i rischi per le libertà civili

Tesina per il corso di Aspetti Etici e Sociali dell'Informatica
Proff. Diego Latella e Gian Piero Siroli, anno accademico 2005-2006.

Corso di Laurea in Informatica – Università di Pisa

a cura degli studenti:
Valerio Borsò
Davide Cacci
Marco Cornolti
Gabriele Cristaudo
Cristina Puccinelli

Pisa, 9 giugno 2006

Indice

1. Introduzione

1.1. Presentazione

In questa tesina verranno affrontati alcuni aspetti relativi ai sistemi informatizzati di sorveglianza e controllo dei passeggeri, ed in particolare i rischi che tali sistemi possono presentare per il rispetto della privacy.
Gli aspetti più approfonditi saranno quelli economici, etici e politici, ovvero quelli che determinano un maggiore impatto sociale, oltre a quelli tecnici e legali, che forniscono elementi necessari per studiare il problema in modo più approfondito.

1.2. Metodologia adottata

Il lavoro è cominciato con uno sguardo globale alle tematiche collegate al problema. In seguito a questa ricerca abbiamo individuato e definito i capitoli da sviluppare, che ci siamo suddivisi in base all'interesse personale.
La stesura dei capitoli è stata preceduta da una ricerca individuale sul tema specifico accompagnata da uno scambio di informazioni all'interno del gruppo tramite una mailing-list creata ad hoc.
Il capitolo iniziale, curato da Marco Cornolti, tratta dell'approccio degli USA all'utilizzo dei sistemi computerizzati di prescreening.
Nel capitolo successivo, curato da Gabriele Cristaudo, sono analizzati i rischi dal punto di vista etico presentati dalla creazione di un database contenente informazioni biometriche.
Il quarto capitolo, curato da Davide Cacci, integra il secondo capitolo analizzando dal punto di vista tecnico le misure di sicurezza adottate per la creazione del database biometrico.
Il quinto capitolo, curato da Valerio Borsò, tratta il rapporto tra privacy e sicurezza in base all'affidabilità di un sistema e i costi in termini di limitazione delle libertà personali, prendendo come esempio il sistema CAPPS II.
Nell'ultimo capitolo, curato da Cristina Puccinelli, vengono presentati l'approccio dell'Unione Europea al problema.
Nel presentare le argomentazioni si è cercato di fornire una visione oggettiva dando risalto sia alle posizioni ufficiali sia a quelle delle organizzazioni e i movimenti non governativi che si sono occupati dell'argomento.
Tutte le informazioni servite per la stesura dei capitoli sono state reperite via Internet, vista la scarsità di materiale pubblicato su carta stampata.

2. I sistemi di prescreening dei passeggeri negli Stati Uniti

a cura di Marco Cornolti

2.1. Introduzione

Gli Stati Uniti rappresentano dal 1990 la nazione più avanzata per quanto riguarda i sistemi di prescreening e di sorveglianza dei passeggeri, dimostrandosi il paese pioniere in questo campo. La spinta verso la sicurezza è l'altra faccia della medaglia rispetto alla politica internazionale adottata dagli USA negli ultimi decenni, forse la più interventista a livello mondiale, che ha innalzato il rischio di attacchi terroristici sul suolo americano.
Al momento gli USA sono il paese occidentale col più alto numero di attacchi terroristici subiti con 7 attentati di grandi proporzioni dal 1985[1].
Per dare un'idea della spesa dedicata dal governo alla difesa bastano pochi dati: gli USA spendono per la difesa il 2.94% del PIL, collocandosi al primo posto tra i paesi occidentali (la media dei paesi UE è 1.85%) e di gran lunga al primo posto nel mondo per spesa netta in armamenti, con ben 291.2 miliardi di dollari contro i 10.45 della media UE[2].
D'altra parte la popolazione degli Stati Uniti è da sempre molto attenta alla salvaguardia dei propri diritti, e questo ha fatto esplodere la contraddizione tra sicurezza pubblica e libertà civili. Se infatti dopo gli attacchi dell'11 settembre il Congresso ha approvato compatto il Patriot Act, la legge speciale che tra gli altri provvedimenti dà poteri straordinari alla NSA permettendo le intercettazioni telefoniche dei cittadini anche senza il mandato di un magistrato, non è stato semplice per il governo farne approvare il rinnovo. Infatti al momento in cui sono scaduti i termini della legge, nel dicembre 2005, l'estensione del Patriot Act è stata respinta dal Senato e poi approvata solo nel marzo 2006 in seguito ad alcune modifiche.
A questo hanno contribuito le pressioni tanto delle organizzazioni in difesa dei diritti umani quali la ACLU[3] (American Civil Liberties Union) e Privacy International[4], quanto dell'opposizione del Partito Democratico all'interno del Parlamento, che anche dopo la modifiche ha opposto contro il rinnovo 131 voti ai 280 della maggioranza.
Qualcosa si è mosso anche nell'opinione pubblica, infatti alla domanda se il governo si fosse spinto troppo oltre nel restringere le libertà civili dei cittadini per favorire la lotta al terrorismo, nel 2002 solo l'11% ha risposto in maniera nettamente affermativa, mentre nel 2006 la percentuale è salita al 41%[5].

2.2. La cronologia dell'evoluzione dei sistemi di prescreening

Il sistema di prescreening per i passeggeri dei voli ha avuto uno sviluppo controverso, soprattutto per la mancanza di finanziamenti e per i problemi relativi alla privacy sollevati dai critici del sistema.
A seguire sono riportati i principali passaggi evolutivi.

CAPPS I

Nel 1996, in seguito alla bomba esplosa al Centennial Olympic Park e all'esplosione del volo TWA 800, venne creato il primo sistema anti-terrorismo di sorveglianza dei passeggeri dei voli in partenza ed in arrivo negli Stati Uniti. Il sistema si chiamava CAPPS (Computer Assisted Passenger

1 Fonte: http://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_the_U._S.
2 Dati 2002. Fonte: "The Military Balance" - The International Institute for Strategic Studies, 2001-2002 (London: Oxford University Press for the IISS, 2001
3 Sito ACLU: http://www.aclu.org
4 Sito di Privacy International: http://www.privacyinternational.org
5 Fonte: USA Today/Gallup Poll. – 12-13 maggio 2006. http://www.pollingreport.com/terror.htm

Prescreening System) ed era basato unicamente su delle liste di persone stilate dall'FBI e dalla FAA (Federal Aviation Administration). Nelle liste erano presenti nomi di persone che avrebbero potuto minacciare la sicurezza dei trasporti aerei e dei passeggeri. Nel novembre 2001 il controllo del sistema è passato dalle agenzie di volo alla governativa TSA (Transport Security Administration), creata in seguito agli attentati contro le torri gemelle.

CAPPS II

Nel 2003 la TSA, tramite il proprio ufficio ONRA, ha espresso una richiesta ufficiale perché il sistema venisse potenziato. Oltre alla semplice lista di nomi, il nuovo sistema prevede, nel progetto iniziale, la richiesta di dati più specifici del passeggero quali l'indirizzo di residenza, la data di nascita, la destinazione e il luogo di partenza del viaggio e il numero di telefono di casa. Nel momento in cui il passeggero prenota il volo, tutti i suoi dati vengono registrati e inviati alla TSA che, incrociando le informazioni con quelle presenti in database di ditte private, verifica l'identità. La TSA, secondo algoritmi segreti, assegna al passeggero un punteggio di rischio (risk score) che indica la pericolosità del passeggero in una scala a tre gradi: verde, giallo, rosso. In base al punteggio, la persona è sottoposta a diversi trattamenti: dall'acquisizione delle impronte digitali e la perquisizione dei bagagli nei casi meno gravi, fino all'arresto nel caso che l'individuo risultasse ricercato.

Numerose organizzazioni si sono opposte a questo piano, dalle compagnie aeree che si vedevano appesantite nel loro lavoro e che vedevano nel nuovo sistema una cattiva pubblicità verso i passeggeri[6], alle organizzazioni per i diritti civili quali EPIC e ACLU.

Le critiche sulla lesione delle libertà civili riguardavano principalmente i parametri secondo i quali viene assegnato il grado di pericolosità, che sono segreti al comune cittadino. Uno dei rischi denunciati dalle organizzazioni è che nell'algoritmo influisse il colore della pelle del passeggero o la propria religione, parametri che avrebbero evidentemente portato ad una discriminazione verso minoranze culturali.

Un altro elemento di critica era la gestione dei dati da parte delle aziende private proprietarie dei database, dato che i loro interessi commerciali avrebbero potuto mettere in pericolo i dati stessi.

Inoltre ACLU individuava nella stessa organizzazione di un database centralizzato con informazioni così sensibili una minaccia per la sicurezza pubblica nel caso che il database venisse violato.

Il colpo di grazia provenne dal GAO (General Accounting Office), un ufficio indipendente al quale il Congresso diede mandato per una verifica sulla sicurezza del sistema, il quale rivelò in un rapporto[7] delle gravi lacune nella protezione dei dati, messa in pericolo dalla scarsità dei fondi economici dedicati, e concluse il rapporto spiegando che degli otto punti critici individuati dal Congresso, solo uno era stato rispettato nel progetto.

La TSA cancellò il programma nell'estate del 2004.

Secure Flight

Nell'agosto 2005 la TSA lanciò Secure Flight, pensato per essere la versione sicura di CAPPS II. Ma un nuovo rapporto del GAO riscontrò esattamente gli stessi problemi e bocciò per la seconda volta il programma, che quindi venne cancellato nel Febbraio 2006.

US-VISIT

Visti gli insuccessi delle altre agenzie, il programma di prescreening dei passeggeri è continuato parallelamente negli uffici del DHS (il Department of Homeland Security, un altro organismo creato nel 2002 per rispondere agli attacchi dell'11 settembre) sotto il nome di US-VISIT. L'obbiettivo,

6 "Corps. Putting CAPPS II Direction In Question" – BTNonline.com – 9 febbraio 2004 – link: http://www.btnmag.com/businesstravelnews/headlines/frontpage_display.jsp?vnu_content_id=2085918

7 "Computer-Assisted Passenger Prescreening System Faces Significant Implementation Changes" – febbraio 2004 – link: http://www.gao.gov/new.items/d04385.pdf)

oltre a realizzare qualcosa di concreto del programma studiato per anni, è stato di compiere un salto di qualità. La svolta è nella concezione: da una semplice lista di persone sospette, il progetto diviene uno strumento di archiviazione di massa per i dati biometrici di tutti i passeggeri non americani. Se le finalità dichiarate sono le stesse di CAPPS I, il nuovo sistema risulta ben più invasivo e pericoloso per quanto riguarda la privacy dei passeggeri.
Le informazioni raccolte e schedate nei database non riguardano più solo i dati anagrafici, né gli spostamenti delle persone, ma anche informazioni biometriche come la rilevazione delle impronte digitali e la fotografia.
Inoltre la copertura del sistema è divenuta totale, comprendendo non più solo gli aeroporti, ma anche tutti gli altri punti di ingresso negli Stati Uniti. La sua applicazione su larga scala è cominciata il 5 gennaio 2004, data in cui US-VISIT è divenuto operativo in 115 aeroporti e nei principali 15 porti navali. Il 29 dicembre 2004 è stato attivato nei 50 maggiori punti di immigrazione via terra, e nel dicembre 2005 è terminato il lavoro di distribuzione e attivazione presso tutti i punti di immigrazione negli U.S.A..
Nell'agosto 2005 il sistema, dall'archiviazione di sole due impronte digitali, è passato all'archiviazione delle impronte di tutte le dita.

2.3. Visione globale di US-VISIT

US-VISIT è acronimo di "United States Visitor and Immigrant Status Indicator Technology" (in italiano: "Tecnologia per un indicatore dello stato dell'immigrazione degli ospiti e degli immigranti negli Stati Uniti"). Il suo scopo ufficiale è espresso nella presentazione del progetto, sul sito del DHS[8]:

- *Migliorare la sicurezza dei nostri cittadini e degli ospiti;*
- *Facilitare i legittimi viaggi e il commercio*
- *Assicurare l'integrità del nostro sistema di immigrazione*
- *Proteggere la privacy dei nostri visitatori*

US-VISIT è un sistema creato dal DHS per raccogliere informazioni al fine di garantire la sicurezza nazionale, incluso il controllo dell'immigrazione. Lo scopo è di impedire l'accesso negli Stati Uniti a persone considerate pericolose o che comunque cercano di entrare nel territorio violando la legge. Il nucleo principale attorno a cui ruotano le motivazioni per la creazione di questo sistema è la prevenzione di attentati terroristici sul suolo USA impedendo l'ingresso ai terroristi.
Come si legge su un documento ufficiale del DHS[9], US-VISIT è un sistema di sistemi. Il progetto ha infatti l'obbiettivo di collegare tra loro vari impianti affinché lavorino in modo coordinato. Inoltre i dati raccolti sono condivisi con tutte le strutture governative degli USA, così da rinforzare l'apparato della sicurezza interna.
Per come appare ai passeggeri poco attenti, l'applicazione del sistema non rappresenta una grande novità: nel momento dell'arrivo in territorio americano, il personale dell'aeroporto chiede se gentilmente il passeggero può appoggiare la mano su un vetro e guardare in un obbiettivo. In pochi secondi lo scanner delle impronte digitali e la macchina fotografica inviano i dati raccolti insieme a quelli relativi all'identità del passeggero e danno via al procedimento di verifica. Ciò che il passeggero non sa è che questo trattamento è riservato solo ai cittadini non americani e che riguardo all'archiviazione dei dati biometrici, registrati per anni nei database del DHS, non può avere grandi garanzie. D'altra parte il passeggero che colto da diffidenza si rifiutasse di dare le proprie impronte verrebbe, secondo la procedura, espulso dagli Stati Uniti dopo non meglio precisati "accertamenti".

8 Sito del DHS (www.dhs.gov), paragrafo US-VISIT – link: http://www.dhs.gov/dhspublic/display?theme=91
9 Privacy Impact Assessment, July 1, 2005, pag. 9 – link: http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_pia_usvisitupd1.pdf

2.4. L'evoluzione di US-VISIT

Il sistema si è sviluppato secondo passi progressivi chiamati Increment 1A, 1B, 2A, 2B, 2C, 3, 4. Nella seguente tabella sono riportate le caratteristiche principali degli Increment.

Incr. no.	Data di attivazione	Applicazione delle procedure US-VISIT
1A	5/1/2004	Ai soli passeggeri in arrivo in alcuni porti di aria e mare
1B	3/8/2004	Negli stessi porti, ma anche ai passeggeri in uscita
2A	26/10/2004	Attivazione del confronto biometrico e dell'autenticazione dei passaporti elettronici
2B	29/12/2004	Estensione a 50 punti di immigrazione via terra
2C	31/7/2005	Test e implementazione dell'interfaccia con RFID
3	1/7/2005	Estensione del sistema a tutti i punti di immigrazione non ancora coperti
4	?	Possibili aggiornamenti al sistema

2.5. Come funziona US-VISIT nel dettaglio

La struttura consiste nell'integrazione e la modifica di tre sistemi già esistenti sviluppati dal DHS:

1. The Arrival and Departure Information System (ADIS), che archivia le informazioni su arrivo e partenza del passeggero.
2. The Passenger Processing Component del TECS, che processa le informazioni raccolte
3. The Automated Biometric Identification System (IDENT), che si occupa dei dati biometrici.

Inoltre nell'incremento 2C viene introdotto l'Automated Identification Management System (AIDMS), ovvero l'interfaccia con l'RFID[10] (Radio Frequency Identification), un sistema di identificazione pensato per velocizzare il processo di attraversamento delle frontiere che consiste in un chip che risponde a degli apparecchi emettitori di radio frequenze trasmettendo un numero identificativo unico, col quale si possono ricevere informazioni riguardo alla persona dal database del TECS. Il sistema generalmente è installato nei camion di trasporto merci, ma nel caso di US-VISIT, si pensa alla versione sottocutanea del chip per l'identificazione delle persone.

Foto di un chip RFID sottocutaneo subito dopo l'operazione di impianto – foto da: http://flickr.com/photos/28129213@N00/7267161/in/set-181299/ pubblicata sotto Creative Commons Attribution ShareAlike 2.0.

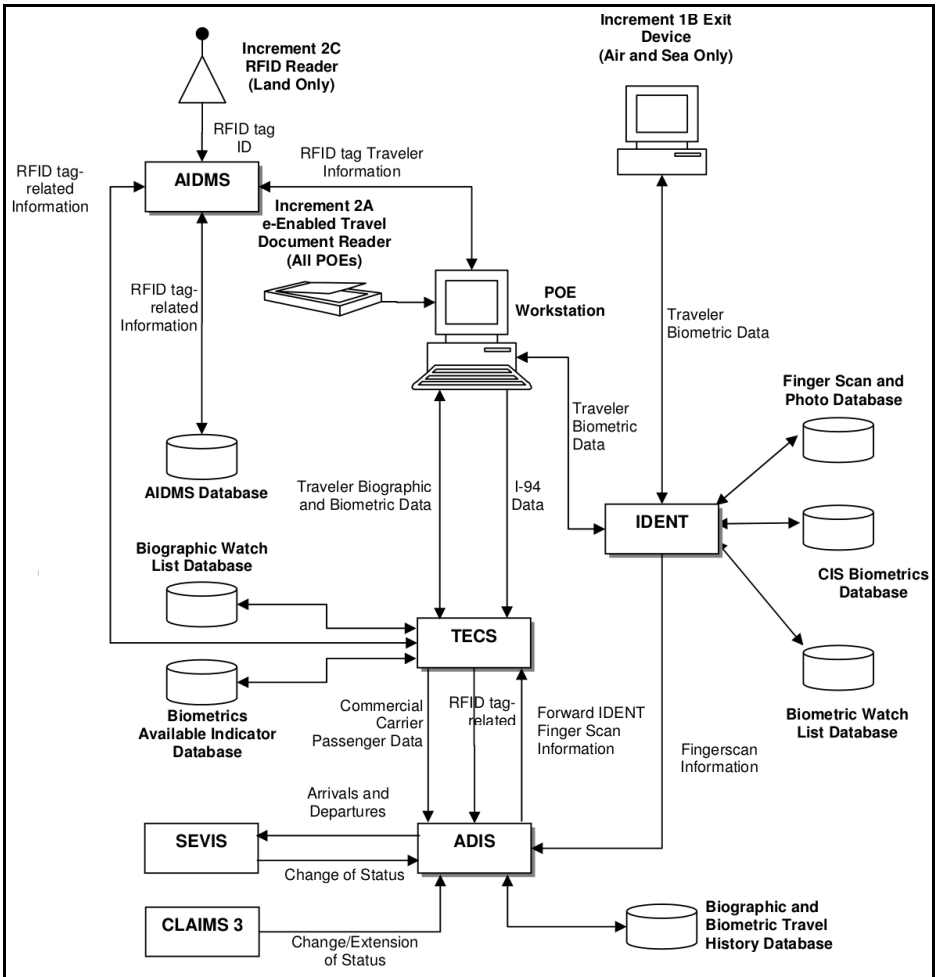
I terminali presenti negli aeroporti si collegano per lo scambio di informazioni con altri sistemi gestiti dal DHS ma non direttamente da US-VISIT, quali:

1. il SEVIS (Student and Exchange Visitor Information System), un database che contiene informazioni su studenti stranieri negli USA
2. il CLAIMS 3 (Computer Linked Application Information Management System), che contiene dati riguardo a cittadini stranieri speciali (es.: richiedenti asilo politico)
3. l'IBIS (Interagency Border Inspection System) che offre l'accesso ai database dell'FBI oltre che al NCIC dell'Interpol

10 Per maggiori informazioni: http://en.wikipedia.org/wiki/RFID)

Tra i sistemi non gestiti dal DHS con cui US-VISIT comunica, il principale è il CCD (Consular Affairs Consolidated Database) dal quale riceve informazioni biografiche e biometriche, inviando le impronte digitali. Nel CCD sono presenti dati sul soggiorno dei cittadini stranieri negli Stati Uniti.

Lo scambio di dati tra le varie strutture permette che gli stessi vengano confrontati, controllati e aggiornati.
Le postazioni da cui i dati vengono acquisiti e inviati si trovano in tutti i punti di immigrazione ("Ports Of Entry") presenti sul suolo americano, ovvero tutti i 115 aeroporti internazionali, i 14 porti navali internazionali, e 154 ports of entry situate sui confini raggiungibili via terra.
Uno schema esplicativo del funzionamento globale è fornito da un documento del DHS:



Schema: Il funzionamento di US-VISIT – US-VISIT PIA, versione del 1 luglio 2005 – link: http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_pia_usvisitupd1.pdf

Secondo la presentazione ufficiale del progetto tutte le informazioni, oltre ad essere utilizzate per decidere se concedere l'accesso negli USA, sono raccolte e archiviate per permettere una facile fruibilità ad altre strutture, in adempimento dei principi espressi dal PATRIOT Act. L'accesso alle informazioni raccolte è consentito agli impiegati del DHS, oltre che le forze dell'ordine americane a livello statale e federale, a quelle di altri paesi, a chiunque (comprese le agenzie private) investighi su atti criminali e infine ai servizi di intelligence.
Le agenzie esterne al DHS con cui vengono condivisi i dati devono accettare la clausola di garantire la segretezza dei dati in rispetto della privacy.

2.6. Problemi per la sicurezza della privacy

L'aspetto più controverso di US-VISIT è indubbiamente quello del rispetto della privacy delle persone. Creare un database con i dati sensibili, come i parametri biografici e biometrici degli individui, può essere un enorme rischio nel caso che lo stesso database venga violato.
La storia recente dell'informatica ha dimostrato a più riprese l'impossibilità pratica di rendere completamente sicuro un database. Nel sito del Web Application Security Consortium è stilato un elenco di attacchi informatici[11] avvenuti negli ultimi anni. Sono rappresentati unicamente i dati relativi ad attacchi via web a strutture di rilevanza globale, non si contano infatti i ben più numerosi attacchi a computer e siti internet minori o personali. Tra i bersagli degli attacchi riusciti compaiono motori di ricerca come Google, servizi di web hosting come Xoom e MySpace, interi sistemi web mail come Yahoo e Gmail, siti governativi come quello della NASA, aziende multinazionali come Microsoft e Novell.
Nell'aprile 2006 un baco nella sicurezza di una delle principali banche britanniche, la Clydesdale Bank, ha permesso a delle persone di acquisire migliaia di numeri di carte di credito MasterCard direttamente dal database centrale. Per evitare una cattiva pubblicità, il fatto è stato oscurato dalla banca, ed è diventato di dominio pubblico solo perché alcuni utenti hanno segnalato problemi con la carta di credito, causati dal tentativo da parte della banca di riparare al danno. Questo fa pensare che siano frequenti i casi in cui database ritenuti sicuri vengano violati senza che, per ragioni commerciali, l'attacco venga denunciato pubblicamente.

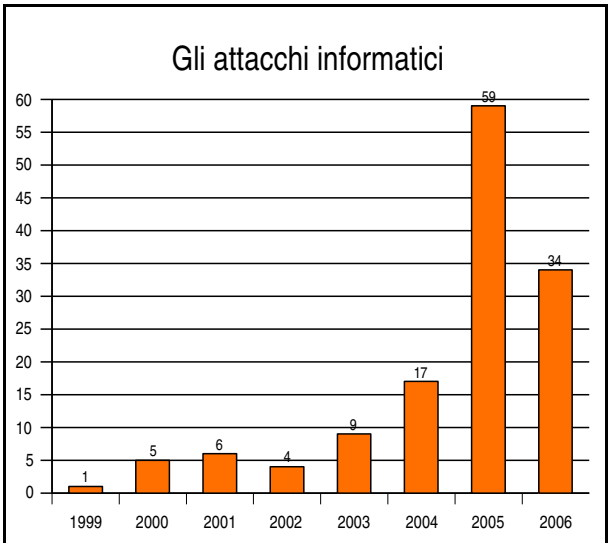


Grafico degli attacchi informatici riusciti contro obbiettivi di rilevanza globale. Dati aggiornati al maggio 2006.

Considerati questi dati, non occorre essere eccessivamente paranoici per rendersi conto di quanto sia concreta la possibilità che i dati raccolti da US-VISIT vengano rubati.

In seguito all'approvazione dell'E-Government Act (2002) ogni sistema informatico che presenta rischi per la privacy deve stilare un documento chiamato Privacy Impact Assessment (PIA) che illustri tutte le minacce a cui il sistema è sottoposto e le contromisure di prevenzione adottate dal sistema. Il PIA è stilato dalla stessa agenzia che presenta il sistema, quindi nel caso di US-VISIT, dallo stesso DHS.
Il PIA[12], ripubblicato per US-VISIT in seguito ad ogni Increment, presenta nell'ultima parte una ricca e fantasiosa tabella dei possibili tipi di attacchi e delle soluzioni da adottare (si ipotizza addirittura un improbabile terrorista travestito da ufficiale del DHS che distribuisce hardware contraffatto, oltre a garantire la sorveglianza armata dei database centrali…). Nonostante lo sforzo di fantasia, è comunque improbabile che siano stati davvero pensati tutti i possibili metodi di introduzione nel sistema, visto che le tecniche di attacco sono in continua evoluzione.
Inoltre, se anche la tabella fosse completa e riuscisse a impedire gli attacchi dall'esterno, essa non tiene conto dei rischi legati all'accesso al database da parte degli operatori, quindi dei possibili attacchi provenienti dall'interno, sicuramente più facili da attuare e più difficili da individuare. Un

11 Link: http://www.webappsec.org/projects/whid/statistics.shtml
12 Documento PIA del DHS, versione del 1° luglio, 2005: http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_pia_usvisitupd1.pdf

database del genere ha un valore commerciale inestimabile e diverse realtà potrebbero essere interessate ad averne accesso, inclusi i terroristi contro i quali è stato costruito il sistema.
Ai rischi per le introduzioni illegali nel database, va affiancato il rischio provocato dall'enorme potere che comporta la gestione di simili database, che può essere utilizzato per fini poco etici.

Il GAO, nel suo rapporto del Febbraio 2006[13], critica la gestione del programma e denuncia l'eccessiva lentezza con cui avvengono i test di sicurezza che potrebbe compromettere il successo del programma.
Dal lancio del programma, il GAO ha espresso 18 consigli per migliorare US-VISIT. Il principale, formulato subito dopo la presentazione del programma, riguarda la necessità di un'attenzione maggiore verso i problemi di rispetto della privacy e richiede lo studio più accurato del PIA.
Nel rapporto del febbraio 2006, il GAO spiega che solamente due delle 18 richieste sono state seguite, per 11 l'attuazione è parziale, mentre per 5 è solo all'inizio.
Nel riassunto del rapporto, a pagina 2 del documento, si legge: *"Nonostante molto tempo sia passato da quando sono state formulate le raccomandazioni, non sono ancora state eseguite delle azioni chiave"* e: *"il DHS è lento nel garantire sicurezze sui rischi per la sicurezza e nella pianificazione del rapporto tra costi e benefici per eliminare i rischi, pesando il valore del progetto e i suoi costi e rischi."*. Inoltre: "*Quanto più ci metterà US-VISIT a implementare le raccomandazioni, tanto più è alto li rischio che il programma non raggiunga gli scopi dichiarati in tempo e rientrando nelle spese*".

2.7. Le risposte della società civile alla sorveglianza dei passeggeri

Sono diverse le associazioni per la difesa dei diritti civili che si sono opposte al piano del DHS denunciandone vari aspetti negativi.
Secondo EPIC (Electronic Privacy Information Center), US-VISIT non ha abbastanza a cuore la privacy delle persone e si è spinto ben oltre i propri scopi dichiarati. La diffusione di massa dei sistemi RFID presenta il rischio più grave[14], visto che i chip trasmettono il numero identificativo senza che la persona se ne accorga, e questo permette a chiunque abbia un apparecchio per leggere i chip RFID di tracciare gli spostamenti delle persone senza il loro consenso.
Nel commento generale su US-VISIT[15], EPIC spiega che il sistema non rispetta la Dichiarazione Internazionali dei Diritti dell'Uomo, secondo la quale ogni individuo, indipendentemente dalla propria nazionalità, ha il diritto al dominio delle proprie informazioni personali. EPIC ricorda che per queste motivazioni è già stato annullato CAPPS II, e si chiede per quale motivo US-VISIT dovrebbe essere più sicuro. Un'altra critica è indirizzata alla condivisione dei dati archiviati con altri sistemi delle forze dell'Ordine, infatti secondo EPIC il sistema dovrebbe limitarsi a garantire la prevenzione degli attacchi terroristici, senza adempiere ad altre funzioni di rinforzo della legge per le quali non è stato progettato.
Accanto a EPIC, a evidenziare i difetti del programma, si schiera la ACLU, che con le parole del portavoce Timothy Edgar esprime la propria preoccupazione per la possibilità che il sistema diventi discriminatorio per gli arabi e i musulmani, aumentando la confusione nel sistema di immigrazione e alimentando i pregiudizi verso determinate etnie e religioni.

13 HOMELAND SECURITY: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented – link: http://www.gao.gov/new.items/d06296.pdf
14 "Comments on US-VISIT's RFID Proposal" – 3 ottobre 2005 – link: http://www.epic.org/privacy/us-visit/100305_rfid.pdf
15 "Comments on US-VISIT" – 4 febbraio 2004 – link: http://www.epic.org/privacy/us-visit/us-visit_comments.pdf

2.8. Le reazioni internazionali ai sistemi di prescreening

Fuori dagli Stati Uniti, alcuni governi si sono opposti alla raccolta dei dati biometrici dei propri cittadini da parte degli USA, dichiarando ingiusto che i turisti venissero trattati alla frontiera come dei criminali.

Il governo del Giappone si è espresso contro l'applicazione delle nuove misure, dichiarando[16] di esigere maggiori sicurezze riguardo al modo in cui vengono protetti i dati personali. Il governo giapponese ricorda in una nota che gli USA sono gli unici ad adottare misure così rigide e chiede che le informazioni dei cittadini giapponesi vengano definitivamente cancellate dai database di US-VISIT nel momento in cui i turisti escono dal territorio USA[17].

Anche la Cina ha preso posizione ufficiale per chiedere che i cittadini cinesi non vengano schedati all'ingresso negli USA[18], minacciando di adottare simili misure se gli USA non fermeranno questo procedimento giudicato discriminatorio.

La posizione più interessante è quella espressa dal Brasile del Presidente Lula che, preoccupato per la privacy dei propri cittadini, dopo aver fortemente richiesto e non ottenuto l'esenzione per i brasiliani da US-VISIT, ha risposto creando nei propri aeroporti un sistema analogo per l'acquisizione delle impronte digitali riservato esclusivamente ai cittadini statunitensi in ingresso in Brasile[19]. Tale decisione ha suscitato il malcontento dell'ambasciata statunitense[20] e il commento indignato del segretario di stato Colin Powell secondo cui il provvedimento è mosso da ideali anti-americani.

2.9. Aspetti economici legati all'implementazione dei sistemi di prescreening

La progettazione di un sistema così articolato e complesso e la sua diffusione su larga scala ha messo in moto dei meccanismi economici rilevanti.

Per calcolare il costo con cui US-VISIT è gravato finora sulla spesa pubblica americana, sono da tenere in considerazione anche i costi dei progetti genitori, ovvero CAPPS II e Secure Flight, per i quali sono stati spesi 45 milioni di dollari nel 2004 e 35 nel 2005[21].

Ancora più ingenti sono i fondi dedicati a US-VISIT: 330 milioni di dollari nel 2004, 340 nel 2005 e 340 nel 2006[22]. Per il 2007, il presidente Bush ha chiesto al Congresso di destinare per US-VISIT 399.5 milioni di dollari, 62.9 in più rispetto al 2006.

L'aumento della spesa è dovuto all'aggiornamento del sistema per permettere l'acquisizione di tutte e 10 le impronte digitali invece di 2 e per implementare la condivisione dei dati raccolti con tutte le strutture governative[23].

La spesa fino al 2006 per i programmi di prescreening supera dunque il miliardo di dollari.

Nel 2004, al DHS sono stati destinati quasi 5 miliardi di dollari, dei quali il 6,7% è stato destinato a US-VISIT.

Chi ha guadagnato sicuramente è Accenture, una compagnia che fornisce apparecchiature tecnologiche, che con altre ditte ha composto un cartello chiamato Accenture's Smart Border Alliance[24] e con la quale il DHS ha stipulato un contratto per la realizzazione di US-VISIT. Il

16 secondo un documento reperibile dal sito del ministero degli esteri giapponese al link: http://www.mofa.go.jp/region/n-america/us/visa0402.pdf

17 "Japan to Demand U.S. Erase Fingerprints, Photos After Visitors Leave Country" – Mainichi Daily News – 29 settembre 2004

18 "FM: US urged not to fingerprint Chinese" - China Daily – 24 marzo 2004 – link: http://www.chinadaily.com.cn/english/doc/2004-03/24/content_317687.htm

19 "Brazil to fingerprint US citizens" – BBC news – 31 dicembre 2003 –link: http://news.bbc.co.uk/1/hi/world/americas/3358627.stm

20 US 'regrets' Brazil's tit-for-tat move" – The Age – 7 gennaio 2004 – link: http://www.theage.com.au/articles/2004/01/06/1073268031785.html

21 Fonte: FY 2006 TSA Budget Request – pagina 5 – link: http://www.tsa.gov/interweb/assetlibrary/FY2006Budget_Brief.ppt

22 Fonte: DHS Press Room – 30 dicembre 2005 – link: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0710.xml

23 Fonte: "US-VISIT under the microscope" – FCW.com – 13 febbraio 2006 – link: http://www.fcw.com/article92294-02-13-06-Print

24 Le principali compagnie che fanno parte del cartello sono: Accenture, AT&T, Dell Inc., Titan Corp., Deloitte Consulting Global Technology Management Inc., Raytheon Inc., SRA International, Sprint Communications.

contratto ha un massimale di 10 miliardi di dollari in 10 anni, anche se difficilmente il congresso approverà una simile spesa[25].
Questa scelta da parte degli uffici del DHS non è stata preceduta da alcuna gara di appalto, ed ha provocato la meraviglia degli esperti di mercato e le proteste della Lockheed-Martin, la compagnia che maggiormente collabora col governo per i programmi di difesa, scavalcata da Accenture che è, a suo dire, priva di esperienza nel settore[26]. Va ricordato che le ditte raccolte sotto il cartello di Accenture hanno finanziato nel 2004 la campagna elettorale per un totale di 6 milioni di dollari, sbilanciati per il 66% verso il Partito Repubblicano[27].
Inoltre va considerato che in seguito alla scelta da parte del DHS di questa ditta per la realizzazione di US-VISIT, le sue azioni in borsa sono balzate, dal valore di 15$ dell'inizio 2003, ai 33$ dell'inizio 2006. Secondo la German Association for Information Technology, Telecommunications and New Media, il mercato dell'identificazione elettronica avrà un balzo in borsa dai 21 milioni di euro del 2005 a 377 milioni nel 2009[28], sarebbe quindi interessante studiare chi potrebbe aver guadagnato un profitto personale investendo in questi titoli di borsa prima del lancio di US-VISIT.

2.10. L'effettiva funzione di US-VISIT

Un aspetto controverso del sistema riguarda il rapporto tra costi e benefici. Secondo una nota del DHS[29], il sistema, *"dal gennaio 2004 ha processato più di 44 milioni di visitatori* […] *I dati biometrici hanno permesso a US-VISIT di intercettare, all'ingresso negli USA, più di 970 persone con un passato di criminalità o di problemi di immigrazione, tra cui fuggitivi da prigioni federali, rapitori condannati, trafficanti di droga, e molti che hanno violato le leggi sull'immigrazione"*.
Tra le righe si legge che probabilmente la grande maggioranza dei 970 fermati sono persone con problemi di permesso di soggiorno oltre a qualche criminale che sarebbe stato catturato anche senza US-VISIT, al semplice controllo del nome. Ma il dato più significativo è che non è stato catturato alcun terrorista o sospetto tale.
Secondo l'esperto di sicurezza informatica Bruce Schneier, il sistema ha avuto un costo sproporzionato rispetto a ciò per cui è servito. Considerando la spesa di 1 miliardo di dollari per il progetto e il numero di persone fermate, giudica il milione di dollari spesi per ogni persona fermata eccessivo per catturare un piccolo criminale o qualcuno che ha dimenticato di rinnovare il visto e alcuni utenti, tra i commenti sul suo sito, propongono, scherzando, di istituire una taglia di un milione di dollari per ogni criminale, creando così un sistema più efficiente e sicuramente meno intrusivo.
Schneier fa notare, in un articolo sul suo blog, che è piuttosto remota la possibilità che un terrorista già ricercato si presenti alle porte di imbarco per gli Stati Uniti sperando di non essere fermato. Piuttosto, nel caso volesse fare un attentato, sceglierebbe di entrare clandestinamente oltrepassando la frontiera colabrodo col Canada o col Messico. Inoltre Schneier fa notare[30] che i terroristi, prendendo ad esempio il caso dell'11 settembre, non sono mai ricercati prima che facciano gli attentati ma solo dopo, e che il sistema US-VISIT avrebbe fatto passare senza difficoltà i dirottatori degli aerei esplosi contro le torri gemelle.

25 Vedi "House Approves $10B Accenture Deal" – Earth Web News – 18 giugno 2004 – link: http://news.earthweb.com/bus-news/article.php/3370781
26 Vedi "Accenture secures U.S. Visit" – Washington Technology – 6 luglio 2004 – link: http://www-wtonline.iproduction.com/news/19_5/homeland/23660-1.html
27 Fonte dei dati: Center for Responsive Politics – link: www.opensecrets.org
28 Fonte: "Gesicht im Chip" – Sueddeutsche.de – 5 ottobre 2005 – link: http://www.sueddeutsche.de/,polm1/deutschland/artikel/868/61807/
29 DHS Press Room – "DHS Completes Foundation of Biometric Entry System" – 30 dicembre 2005 – link: http://www.dhs.gov/dhspublic/display?content=5314
30 "The failure of US-VISIT" – Schneier on Security – 31 gennaio 2006 – link: http://www.schneier.com/blog/archives/2006/01/the_failure_of_1.html

3. Il Database Biometrico nel progetto US-VISIT

a cura di Gabriele Cristaudo

3.1. Passaporto e Database Biometrico

In questo capitolo verrà affrontato il tema della creazione di un database Biometrico e le varie considerazioni etiche o meno che ne conseguono.
Il sistema US-VISIT integra i normali controlli di identità degli stranieri in visita agli Stati Uniti con una raccolta di dati biometrici che vengono prelevati tramite appositi terminali presenti in porti e aeroporti e poi spediti in un database generale che accumula tutti questi dati e permette un successivo controllo incrociato.
Per integrare questo sistema di controllo, sempre gli Stati Uniti (e alcuni stati Europei quali Germania, Regno Unito, Norvegia e Svezia) dagli inizi del 2006 spingono verso la creazione e diffusione di un passaporto elettronico basato su un chip denominato RFID che può contenere vari dati biometrici quali impronte digitali scansioni facciali e della retina sotto forma di dati digitali e che essendo di dimensioni ridotte può essere inserito in una scheda di piccole dimensioni. Anche questi dati del chip verrebbero poi spediti al database centrale.
Questa politica di controllo adottata dal governo degli Stati Uniti ha fatto sorgere da più parti, in special modo tra le associazioni sulla difesa della privacy, parecchi interrogativi relativi alla sicurezza un simile sistema e ai rischi che la creazione di un database biometrico di grandi dimensioni possa portare con se.
I principali interrogativi emersi sono:

- Fin dove il governo si può spingere nel sacrificio della privacy in nome della lotta contro il terrorismo?
- Quali sono i limiti nell'utilizzo di dati contenenti informazioni private sui cittadini? Non vengono violati i diritti alla privacy?
- Cosa costituisce un dato autentico? C'è un rischio di alterazione di informazioni?
- Quanto dell'errore dovuto all'uso delle tecnologie è ritenuto accettabile? E quali sono le implicazioni dei falsi positivi e dei falsi negativi dovuti ad un errore di macchina?

3.2. Le posizioni e i punti di discussione

Il Department of Homeland Security (DHS, Reparto sicurezza del Paese in italiano) ovvero l'istituzione che ha progettato e creato il sistema US-VISIT, assicura che i dati raccolti nel Database siano al sicuro e non verranno usati se non per gli scopi prefissi nel progetto US-VISIT[31]:

- Tutti i dati raccolti saranno protetti in modo constante e sempre nel rispetto delle leggi e regole applicabili sulla segretezza.
- Tutte le informazioni personali raccolte non verranno rivelate ad altri all'infuori del progetto US-VISIT.
- Misure di sicurezza attente, compresi i controlli di sicurezza, assicurano che i dati non possano essere rubati o subire attacchi esterni.

Tutti coloro che fanno parte del progetto US-VISIT aderiscono inoltre ad un contratto che detta i principi per ottenere il massimo rispetto della privacy[32].
Sulla carta questi principi dovrebbero quindi assicurare la sicurezza del paese e nello stesso tempo garantire la privacy di tutti coloro che vengono coinvolti nel sistema. Come fanno notare però molte associazioni, i rischi spesso sono più grandi dei vantaggi che un tale sistema di pre-screening può portare. Un database biometrico di tale entità, basandosi su tecnologie che ovviamente non possono

31 Pagina ufficiale del DHS su US-VISIT – link: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0678.xml
32 Il documento e' reperibile al link: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0681.xml

essere perfette, porta inevitabilmente dei rischi con se che non possono essere né ignorati né eliminati definitivamente.
In un rapporto[33] precedentemente citato di Privacy International (PI), oltre che ad essere esposti alcuni interrogavi riguardo i pericoli di un potenziale sistema di controllo di massa, vengono fatte delle considerazioni etiche e morali. Anzitutto si discute sul chi e sul quanto si possano consultare le informazioni raccolte nel database: secondo quando riportato dal DHS le informazioni saranno condivise con "*other law enforcement agencies at the federal, state, local, foreign, or tribal level"*che *"need access to the information in order to carry out their law enforcement duties*"[34] Le informazioni personali raccolte saranno poi immagazzinate per un periodo che va dai 75 ai 100 anni a seconda dell'individuo interessato e del "rischio" che gli viene associato. Un periodo così prolungato unito ad una quantità di dati così grande non può fare altro che mettere in pericolo in modo ancora più grave la privacy e la sicurezza di tutti colori che vengono coinvolti nel sistema.
Sempre dal documento di Privacy International si può leggere della reazione del Brasile che ha deciso di applicare lo stesso procedimento di raccolta di impronte digitali nei confronti degli Americani in visita nel Brasile[35]. Reazione che si presenta come una sfida a cui però il DHS ha risposto dichiarando: "*We welcome other countries moving to this kind of system. We fully expect that other countries will adopt similar procedures*"[36]. Gli Stati Uniti sono quindi favorevoli alla diffusione di tale sistema e si augurano che questo metodo venga utilizzato da molti stati, come arma per combattere terrorismo, criminalità e immigrazione clandestina.
Nel documento di PI ci si chiede poi se la raccolta delle informazioni usata per combattere il terrorismo, ovvero se la "causa" per cui è nato e per cui viene giustificata la raccolta di dati privati, sia un obiettivo prioritario del sistema US-VISIT. Dalle dichiarazioni ufficiali si capisce che gli scopi sono quelli di garantire la sicurezza nazionale, controllare l'immigrazione e altri obiettivi secondari: "*identifying, investigating, apprehendind and/or removing aliens unlawfully entering or present in the U.S.; preventing the entry of inadmissible aliens into U.S.; facilitating the legal entry of individuals into the U.S.; recording the departure of individuals leaving the U.S.; maintaining immigration control; preventing aliens from obtaining benefit to which they are not entitled;(…)*"[37].
Non vi sono dunque riferimenti diretti al terrorismo, ma si presenta più che altro come un sistema di controllo per l'immigrazione, rischiando a tutti gli effetti di divenire un sistema di sorveglianza di massa per la ricerca di pochi reali colpevoli.
Nel sistema US-VISIT si parte infatti da un'altra considerazione: tutti coloro che vengono coinvolti sono considerati a priori colpevoli. Essere considerati colpevoli, anche sapendo di non aver nulla da nascondere, unitamente a un possibile errore che si può verificare, espone tutti a un rischio di accusa ingiusta.
Un sistema di tale grandezza, basato su raccolta di dati biometrici, è infatti soggetto inevitabilmente ad un errore. Le tecnologie biometriche non sono mai state applicate ad un sistema di tale portata e inevitabilmente i controlli incrociati tra dati del database e dei passaporti portano all'identificazione di falsi positivi e falsi negativi. Ogni persona è inoltre inevitabilmente soggetto a cambiamenti fisici che non possono essere aggiornati se non con ulteriori controlli. Secondo un report del GAO, con la raccolta di impronte digitali si è soggetti ad un 36% di errore di cadere in FNMR (*"False Non-Match Rate"*) ovvero in controlli incrociati non corrisposti. Il 2% delle persone nel mondo non può essere soggetto a raccolta di impronte digitali soprattutto in quanto lavoratori manuali. Anche la scansione facciale presenta un margine di errore non indifferente che arriva al 15% in base all'età del soggetto interessato. Considerando infine il fatto che tra 50 anni il Database potrebbe

33 Report di PI sui rischi di US-VISIT – link: http://www.privacyinternational.org/issues/terrorism/rpt/dangers_of_visit.pdf
34 U.S. Departement of Homeland Security.2003.US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary, December 18
35 Khalip, Andrei, 2004. "Samba Beat Keeps U.S. Tourists Coming to Brazil". Reuters, January 16
36 Swarns, Rachel L. 2004. Millions More Travelers to U.S. to Face Fingerprints and Photos. The New York Times, April 3
37 Federal Register, 2003. Department of Homeland security[DHS] Privacy Act of 1974; System of Records, Federal Register, Volume 68 Number 239, December 12

raggiungere il miliardo di identità raccolte, l'errore determinatosi potrebbe raggiungere dimensioni drammatiche[38].

3.3. Possibili scenari

L'uso che si può fare di un Database contenente una tale quantità di dati personali può essere di molti tipi. Se veramente usato contro possibili terroristi potrebbe essere un'efficace arma di prevenzione; purtroppo però nella pratica è alquanto difficile poter individuare questo tipo di criminali che molto probabilmente non avrebbero precedenti penali. Schedare milioni di persone per individuare pochi colpevoli pare infatti non essere molto efficace in termini pratici né sempre accettabile dal lato morale. Il sistema si connota più come un sistema di sorveglianza di massa: Immaginiamo se un governante decidesse di usare in modo improprio questi dati. Egli potrebbe attuare un vero e proprio sistema di sorveglianza diretta sui cittadini rendendo chiunque, colpevole o meno, esposto ad accuse più o meno giustificate e minando la sicurezza e la libertà di tutti.
Se i sistemi di controllo basati sui chip RFID si diffondessero si potrebbe poi avere un controllo diretto sul singolo individuo e ogni spostamento potrebbe essere registrato facendo venir meno i diritti di una persona. Il passaporto biometrico passerebbe dall'essere un documento di identità fino a diventare un vero e proprio dispositivo di controllo della persona.
Un uso scorretto potrebbe anche venire da qualche compagnia commerciale, che avendo accesso ad una mole di dati come questa potrebbe trovare qualche modo per arricchirsi. Si potrebbe pensare ad esempio ad una compagnia aerea che avendo accesso in modo più o meno diretto a questi dati, potrebbe registrare gli spostamenti di coloro che viaggiano e capirne gli interessi così da sfruttarli per fini commerciali.
Se un malintenzionato con la giusta conoscenza informatica riuscisse poi a superare i sistemi di difesa del database, potrebbe raccogliere i dati informatici e diffonderli rendendo di fatto vulnerabile la sicurezza di tutti. Se fossero addirittura dei terroristi ad avere accesso a questi dati, il sistema potrebbe essere usato contro lo stesso paese che lo adotta rendendo del tutto inutile quanto fatto per la sicurezza.

38 Report di PI sui rischi di US-VISIT – pagina 8 – link: http://www.privacyinternational.org/issues/terrorism/rpt/dangers_of_visit.pdf

4. Il sistema US-VISIT e la sicurezza: sinonimi o no?

a cura di Davide Cacci

4.1. Introduzione

Il sistema US-VISIT si applica durante l'ingresso e l'uscita dal paese e, nonostante venga descritto come un procedimento semplice nei filmati disponibili nel sito ufficiale[39], nasconde in realtà una serie di difficoltà dal punto di vista tecnico: la privacy di ogni singolo cittadino che si recherà in America, anche come semplice turista, rischierà di essere violata, dovendo egli sottoporsi a rilievi biometrici (foto e impronte) ai quali non potrà sottrarsi.
Nel database saranno immagazzinate informazioni sull'individuo in visita negli USA, precisamente nome completo, data e luogo di nascita, sesso, numero di passaporto, paese di residenza, ogni tipo di documento (ad esempio il visto, che è comunque richiesto all'ingresso del suolo americano) indirizzo completo di destinazione del viaggio e informazioni sulla permanenza e sul volo di ritorno oltre ai già citati dati biometrici.
Ovvio che con una tale scrupolosità nella raccolta dei dati i database del programma sono soggetti a rischio e mettono in pericolo la sicurezza di ogni singolo cittadino americano e non.
Ma non solo i terroristi hanno nel mirino gli archivi cui ha accesso l'US-VISIT, basta fare una considerazione: secondo i dati statistici pubblicati dall'Organizzazione Mondiale per il Turismo[40] (UNWO) nel 2004 nel nord america sono sbarcati 85.8 milioni di turisti e fra questi il 52% si è recato per motivi esclusivamente turistici, mentre solo il 16% come viaggio di lavoro. I dati raccolti sulla gente comune in una così grande quantità possono dunque essere usati per scopi commerciali.
Come si difendono gli USA, proprietari di tali dati, da attacchi di pericolosi terroristi, spionaggio industriale, criminali e da multinazionali senza scrupoli?

4.2. Analisi del sistema e delle misure di sicurezza

Innanzitutto diamo uno sguardo più critico all'intero sistema.
Il programma US-VISIT ha diversi scopi principali: aumentare la sicurezza dei cittadini e dei visitatori e assicurare la funzionalità del sistema di immigrazione degli USA ("*enhance the security of our citizens and visitors and ensure the integrity of the U.S. immigration system*") oltre che facilitare il legittimo scambio culturale e/o commerciale tra paesi tutelando la privacy.
Il progetto US-VISIT è stato sviluppato dal DHS (Department of Homeland Security), un organo federale la cui creazione è strettamente collegata ai fatti dell'11 Settembre 2001.
Il GAO nell'ultimo documento[41] sul DHS fa un confronto tra i provvedimenti per la sicurezza chiesti dallo stesso GAO in rapporti precedenti e quelli che sono stati effettivamente attuati al giorno d'oggi.
L'ente nel Settembre 2003 aveva segnalato al dipartimento che non fosse ancora stata definita una strategia riguardo non solo il numero preciso di persone che devono sottoporsi al trattamento o il numero di impronte da archiviare, ma non era stato comunicato l'intero assetto del progetto come ad esempio l'assegnamento di una carica per ogni personale all'interno del dipartimento (e la sua eventuale responsabilità in caso di manomissione o perdita dei dati).
Dopo circa 2 anni la strategia finale non è stata ancora ultimata, si parla, infatti, di un accordo per coordinare il lavoro del sistema US-VISIT con altre future iniziative facenti parte anch'essi del DHS (Security and Prosperity Partnership of North America and the Secure Border Iniziative) nate per

39 US-VISIT Videos and Brochures http://www.dhs.gov/dhspublic/interweb/assetlibrary/USVisit_English-High.wmv
40 Dati: 2004 Fonte: World Tourism Organization http://www.unwto.org/facts/menu.html
41 Data: 14 Feb 06 Fonte: GAO HOMELAND SECURITY Recommendations to Improve Management of Key Border Security Program Need to Be Implemented http://www.gao.gov/new.items/d06296.pdf

controllare il flusso migratorio soprattutto dal vicino Messico, ma non è stato ancora attuata una vera e propria conduzione comune e tuttora non sappiamo come essi possano interagire.
Per quanto riguarda la struttura interna del dipartimento attualmente sono stati assegnati 102 su 115 cariche fisse (117 erano quelle previste inizialmente), il che sottolinea un notevole progresso, anche se per garantire la sicurezza dei cittadini un tale organo non dovrebbe avere posti vacanti all'interno del proprio sistema, in questo modo più facilmente violabile e soggetto a trafugazioni di dati.
Uno dei maggiori rischi sottolineati dal GAO nel suo rapporto del 2003 è la totale assenza di una tabella sui possibili rischi economici, informatici e sociali; nel Settembre 2005 il DHS ha programmato un piano dei pericoli previsti da tale sistema, come l'analisi, la manipolazione e il mantenimento dello stesso. Nonostante questo, il progetto attualmente sta sforando del 5% il costo previsto, cosi come il tempo di completamento totale è stato incrementato della stessa percentuale, fattori che compromettono la sicurezza, perché quando un progetto è in ritardo sulla tabella di marcia si tende a velocizzarne il completamento, aumentando il rischio di errori.
Sempre secondo il GAO i test globali del sistema, che comprendono un'analisi attenta del software, come ad esempio la valutazione delle performance (non va dimenticato che il sistema deve analizzare migliaia di dati da confrontare per ogni singola persona) e la sua vulnerabilità, erano stati del tutto assenti nei primi rapporti PIA (Privacy Impact Assessment).
Come specificato nell'ultimo documento[42] pubblicato dal DHS (datato Luglio 2005) questa richiesta è stata in parte risolta, tuttavia il 70% dei casi analizzati non hanno avuto riferimenti specifici riguardo dati della prova, in particolare il GAO denuncia una totale mancanza di trasparenza sulle verifiche effettuate e sulle condizioni effettive dei terminali su cui sono stati effettuati i test (che sembrano più ipotetici che reali).
Analizziamo in particolare questo dossier.
Chiariamo la ragione del perché vengono raccolti i dati personali: oltre che impedire a persone che possono nuocere alla sicurezza del paese, lo straniero che entra negli USA, secondo la propria posizione, può ricevere, estendere o regolarizzare il proprio stato di immigrazione. Inoltre può essere facilmente localizzata una persona avente diritto a condizioni speciali (ad esempio un rifugiato).
Il sistema oltre a confrontare le informazioni sui passeggeri con una lista di possibili terroristi o persone sospette (Watch List), tiene in considerazione confronti con organi che contengono database di impronte e foto digitali come il Department of State's (DOS) o il Consular Affairs Consolidated Database (CCD). Un ulteriore scopo dell'US-Visit è il controllo dell'immigrazione e a tal fine l'IDENT confronta le impronte con il database biometrico del CIS (il centro di immigrazione Americano) e altri database che controllano gli "extra-americani".
I soli che avranno accesso al database saranno impiegati del DHS e altre persone che controllano le varie infrastrutture (CBP, ICE, USCIS e DOS) e naturalmente gli organi federali per l'individuazione di possibili criminali.
Per quanto riguarda la sicurezza, il DHS mostra una struttura solida, sostenendo che ogni singola persona facente parte del progetto ha un proprio ruolo di responsabilità all'interno del sistema, inoltre sono previsti aggiornamenti e controlli tecnici ed una severa regolamentazione riguardo al sistema interno, soprattutto i suoi canali di comunicazione e le varie interfacce. I 3 organi principali ADIS (attestato del 10/2003), TECS (attestato del 2/2003), e IDENT (attestato del 5/2004) sono stati certificati e risultati idonei a questa procedura alla quale manca ancora il nuovo AIDMS,dove l'uso di alcuni dispositivi, come vedremo, rende problematica la sicurezza.
La certificazione del DHS dichiara che ogni impiegato è sufficientemente preparato alla sicurezza del sistema informatico e al suo mantenimento. Il programma prevede una serie di controlli tecnici per le macchine ma anche controlli psicofisici per i propri dipendenti per preservare l'integrità dei

42 Data: 1 Lug 05 Fonte: Privacy Impact Assessment http://www.dhs.gov/interweb/assetlibrary/privacy_pia_usvisitupd1.pdf

dati trasmessi. Tutti i soggetti che sono inclusi nel sistema di prescreening devono partecipare a seminari riguardanti la sicurezza e firmare un contratto di fiducia con l'ente.
Ogni scambio di dati durante il funzionamento deve essere documentato da entrambe le parti ed è vigilato da un trattato di sicurezza, l'Interconnection Security Agreement (ISA), per proteggere la privacy delle persone coinvolte e segnalare un'eventuale manipolazione dei dati.
Per ridurre il rischio nel traffico di informazioni biometriche, il DHS ha deciso di rendere la maggior parte di queste informazioni non riconoscibili ad occhio umano, permettendo il decrittaggio solo dai calcolatori. Questa può essere un'utile, ma non sufficiente, mossa anti-spionaggio contro chiunque tenti di corrompere il personale, da sempre punto debole in un sistema informatico; tuttavia è un provvedimento insufficiente, poiché gli impiegati hanno comunque accesso alle informazioni.
In particolare all'uscita dal paese il sistema rilascerà una ricevuta contenente una foto e solo in minima parte dati leggibili da umano, insieme ad un codice a barra contenente tutte le informazioni criptate secondo i principi dettati dal Federal Information Processing Standards (FIPS) usando chiavi specifiche che saranno cambiate giornalmente: è quindi molto limitato il rischio privacy in caso di smarrimento o trafugazione della ricevuta.
Anche se è possibile che le trasmissioni cifrate possano essere intercettate, secondo il DHS i dati rimarrebbero inaccessibili e la variazione giornaliera della chiave renderebbe il decrittaggio non autorizzato estremamente difficile.
Leggermente differente è il sistema di prescreening "veloce" introdotto con il nuovo AIDMS.
Ricordiamo che in questo caso il sistema prevede un utilizzo di RFID (Radio Frequency Identification), ovvero una tecnologia per l'identificazione automatica di persone attraverso un trasmettitore.
In questo caso l'ADSM creerà un codice per ogni individuo che attraversa il confine (RFID tag number) e lo collegherà alle informazioni esistenti ricevute dal TECS. Partiamo dalla considerazione che questi numeri non sono criptati; comunque sia, secondo il DHS, da essi non possiamo ricavare alcuna informazione sulla persona se non si ha accesso all'AIDMS, anche se ricordiamo che non ha ricevuto ancora la certificazione di sicurezza dallo stesso organo.
Secondo il dipartimento, tuttavia, non si correrebbe il rischio di essere riconosciuti o rintracciati, perchè il sistema utilizza una particolare frequenza e un piccolo raggio di azione, ma questo verrà smentito nell'approfondimento sui chip RFID a fine capitolo.

4.3. Ipotetici scenari di rischio tecnico

Possiamo a questo punto fare qualche ipotesi su qualche comune inconveniente tecnico, più o meno volontario.
Innanzitutto il sistema è essenzialmente un canale di passaggio e confronto tra dati, quindi dobbiamo distinguere i casi in cui sarà attaccato l'US-VISIT o i server contenenti gli archivi (database biometrici e Watch List).
Ad esempio il sistema di prescreening potrebbe prevedere un generatore ausiliario in caso di mancanza di corrente, tuttavia in determinate circostanze questo provvedimento può essere inutile, ed il programma diventerà inutilizzabile.
Non tutti sanno che pochi mesi prima che avesse luogo il famoso blackout in Italia nel Settembre 2003, nel Nord America si è verificato un evento simile, più grande territorialmente ma inferiore come numero di persone coinvolte rispetto a quello italiano (anche se città come New York e Detroit sono rimaste al buio).
Un tale evento, se prolungato, renderebbe aeroporti, porti e lo stesso US-VISIT oltre che fuori uso e attaccabili, e potrebbe permettere la compromissione dei dati degli archivi federali.

Successivamente, nel Novembre 2003, si venne a sapere che il blackout fu provocato da una serie di imprevisti ad una centrale in Canada e che comunque non fu stato possibile comunicare in tempo utile il guasto ad organi che potevano contenere il fenomeno a causa di un bug[43] nel sistema basato su Unix (il General Electric Energy's XA/21).
Errori come buffer overflow, stack overflow ecc sono all'ordine del giorno anche nei sistemi più moderni e testati, non sarebbe una sorpresa trovarne nel programma del DHS, visto che lo stesso GAO, come detto, ha denunciato che non sono stati fatti sufficienti test, soprattutto non specifici su ogni calcolatore.
Come noi sappiamo, dal punto di vista informatico non esiste un sistema sicuro, soprattutto spesso il malfunzionamento del sistema è causato proprio da un errore nella programmazione del software (basti pensare al caso del sistema PATRIOT, in cui un errore di calcolo può causare il lancio di missili ingiustificato e causare più danni del presunto attacco).
Secondo l'ultimo PIA del DHS, ogni sistema è protetto sia da serrature che da personale armato, quindi inattaccabile dal punto di vista fisico.
Tuttavia proprio la presenza umana deve far riflettere: dove la macchina non può (o quasi) fallire interviene l'uomo; difatti queste apparecchiature sono controllate da impiegati che, in malafede o in buona fede che sia, possono trafugare o compromettere i risultati della macchina, oppure fornire informazioni su di essa a concorrenti o terroristi. Ne avrebbero tutto a vantaggio economico operando volontariamente, tuttavia anche involontariamente è possibile favorire un nemico. Un caso abbastanza recente ha riguardato l'intera "opera" di hacker come Kevin Mitnick, il quale basandosi sulla tecnica del social engineering[44], spacciandosi quindi come tecnico che chiedeva informazioni apparentemente innocue, provvedeva all'acquisizione di informazioni riservate direttamente dalle persone che avevano accesso al sistema. Ricordiamo che i dati hanno valori inestimabili e i "nemici" da cui il DHS deve difendersi hanno mezzi economici praticamente illimitati (multinazionali) e potere militare (terroristi).
Gli attacchi informatici sono in continua evoluzione, e nonostante questo anche i "classici" attacchi possono essere sempre utili. Ad esempio nel 2005 secondo una ricerca[45] Symantec ci sono stati circa 1402 attacchi DoS (Denial of Service) al giorno, e questa tecnica consiste semplicemente nello spedire pacchetti corrotti in modo tale da provocare un crash nella macchina bersaglio: se si avesse accesso ai computer di US-VISIT, potremo mandare in tilt i calcolatori contenenti i database biometrici.
Un altro archivio di dati che è coinvolto nell'US-VISIT sono i cosiddetti passaporti biometrici, nei quali ricordiamo che possono essere immagazzinate oltre ai normali dati biologici (nome, sesso, età) anche informazioni come impronte digitali e scansione dell'iride.
Attualmente solo un'immagine digitale, in formato JPEG, è immagazzinata nel chip RFID del passaporto.
Il chip RFID (simile fisicamente ad una SIM telefonica), utilizzato anche nel sistema AIDMS dell'US-VISIT, include una memoria minima di 32 KB di tipo EEPROM (Electrically Erasable Programmable Read-Only Memory), cioè una memoria che può mantenere le informazioni anche quando non alimentata. Come sappiamo le comunicazioni tra il chip e il lettore non sono criptate, e secondo 2400 testimonianze[46] raccolte, il raggio d'azione è ben oltre i 10 cm previsti (può arrivare fino a 10 metri, quindi intercettabile). Una recente ricerca[47] condotta dal Dipartimento Informatico dell'Università di Vrije, in Olanda, sottolinea la pericolosità di questo chip, che può essere facilmente infettato da virus e worms, con conseguenze disastrose.

43 Per maggiori informazioni http://www.securityfocus.com/news/8016
44 Per maggiori informazioni http://www.securityfocus.com/infocus/1527
45 Dati: 2005 Fonte: Symantec http://www.symantec.com/enterprise/images/theme/ent-threatreportix_chart_theme.jpg
46 Fonte: Frank Moss, deputy assistant secretary for passport services http://www.wired.com/news/privacy/0,1848,67333,00.html
47 Fonte: Department of Computer Science Vrije Universiteit Amsterdam RFID Viruses and Worms http://www.rfidvirus.org

La sicurezza riguardo questi chip è talmente scarsa da compromettere l'intero sistema US-VISIT: come sarà riconoscibile un soggetto pericoloso se può modificare a piacimento il proprio passaporto, inserendo foto e dati falsi?
Per tutelarsi, il governo americano vuole introdurre a partire dall'Ottobre 2006[48] passaporti biometrici "schermati" in modo da scoraggiare possibili manomissioni e sarà prevista una più ferrea procedura nella lettura dei dati, chiamata BAC (Basic Access Control): il passaporto sarà munito di un codice PIN (Personal Identification Number) che, prima della lettura dei dati al suo interno, dovrà essere digitato sulla tastiera del lettore RFID. Inoltre sarà criptato ogni dato scambiato al momento della lettura tra il chip e la macchina interrogatrice.
Tuttavia la soluzione è totalmente inadeguata in questo caso, poiché se questo esempio non verrà seguito dagli altri stati mondiali, al momento dell'introduzione del passaporto biometrico si potranno verificare irregolarità già esposte: è noto che il sistema US-VISIT è operativo solo per i cittadini stranieri e non per quelli americani provvisti di tale sicurezza aggiuntiva e necessaria.

48 Fonte: RFID JOURNAL http://www.rfidjournal.com/article/articleview/1951/1/132

5. Sicurezza sui voli: un problema legale o morale? Il caso del CAPPS

a cura di Valerio Borsò

5.1. Introduzione

L'attentato al World Trade Center di New York dell'11 settembre 2001 ha "aperto gli occhi" all'America ed in generale ai governi dei paesi sviluppati riguardo al terrorismo. L'apparato di sorveglianza predisposto non ha saputo arrestare il volo di due aerei dirottati ed usati come missili kamikaze contro due edifici Newyorkesi. La strage è stata di proporzioni gigantesche: migliaia di morti e altrettanti feriti, danni irreparabili alle torri, crollate a causa del cedimento della struttura portante interna sotto la potenza dell'impatto e delle fiamme.
Ciò ha portato ad intensificare i controlli su tutto l'apparato aeroportuale incentivando la creazione di programmi governativi di sicurezza con lo scopo di monitorare le attività aeree ed aumentare i livelli di sicurezza dei controlli.
A che prezzo tutto questo? Quanto sono approfonditi questi controlli, quanto si intacca della privacy personale di un passeggero che si imbarca su un volo da un aeroporto americano? E la legge tanto ostentata sulla privacy a cui gli americani sono così attaccati che fine ha fatto?

5.2. Sicurezza o Privacy?

Una delle risposte alla necessita di incrementare la sicurezza dei trasporti aerei è stato il C.A.P.P.S. (e suoi successori come C.A.P.P.S. II e Secure Flight) un sistema di pre-screening dei passeggeri (Computer Assisted Passenger Prescreening System).
Ogni persona che si imbarchi su di un volo deve, secondo quanto previsto nel progetto C.A.P.P.S., fornire un documento di identità e/o un passaporto: normali controlli di sicurezza. Ma a sua insaputa ogni imbarco viene registrato in un database (a cui il software del C.A.P.P.S. ha accesso ed attinge informazioni) e con questo i suoi dati. Coi dati raccolti viene assegnato ad ogni persona un livello di rischio. Più alto sarà il livello, Più pesanti saranno i controlli. Il sistema mira a bloccare, rallentare o consentire gli imbarchi su aerei statunitensi e quindi cercare di diminuire il rischio che possa ripetersi la terribile strage delle Twin Towers da parte di organizzazioni terroristiche.
Recentemente il Governo degli Stati Uniti d'America ha ampliato lo spettro di ricerca del software, permettendone l'utilizzo non solo per la ricerca di terroristi "stranieri" ma anche per quei terroristi interni al territorio americano[49].
I passeggeri, ovviamente, non sono al corrente di tale ricerca, solo chi ha l'accortezza di documentarsi sull'argomento può trovare informazioni riguardo l'utilizzo dei sistemi computerizzati di pre-screening. Inoltre è impossibile risalire alla provenienza delle fonti da cui il C.A.P.P.S. prende informazioni, quindi la trasparenza nell'operazione di identificazione è praticamente ridotta a zero. Tutto questo implica che una eventuale contestazione da parte di una persona contro le intromissioni del sistema risulti poco agevole, anche perché le informazioni primarie raccolte dal C.A.P.P.S. possono appartenere a organi governativi come l' FBI, NSA o simili, o addirittura a enti pubblici e commerciali (come banche, società di carte di credito ecc).

Questo sistema di computer sofisticati, di connessioni sicure e protette, di server di appoggio per la ramificazione della rete e collegamenti ai database esterni da cui vengono tratte le informazioni necessarie, hanno un costo decisamente elevato. I 164 milioni di dollari spesi complessivamente non sono l'unico prezzo da pagare: dovrebbe essere preso in considerazione soprattutto il prezzo, non quantificabile in dollari, che ogni cittadino americano o estero si trova a pagare a causa di tali

49 da una recensione dell' EFF; Electtronic Frontiere Foundation

ricerche sulla propria persona, ricerche che violano i diritti costituzionali sulla privacy e sul trattamento dei dati personali.
Ogni cittadino quindi ha due strade da seguire: o rinunciare alla propria privacy per permettere al governo e agli organi istituzionali di garantire una maggiore sicurezza contro eventuali organizzazioni terroristiche, o combattere contro questa intrusione, cercando mezzi per smuovere l'opinione pubblica ed in generale sensibilizzare il resto delle persone noncuranti del problema.

5.3. Indagine sull'affidabilità del programma

Si calcola statisticamente che circa 600 milioni di passeggeri ogni anno si imbarchino su velivoli statunitensi, e quindi ognuno di essi, nel caso che il C.A.P.P.S. fosse entrato in funzione, sarebbe dovuto essere sottoposto allo stesso trattamento da parte del C.A.P.P.S.. Assumiamo che il software abbia una affidabilità del 99% nell'identificare un terrorista tramite le informazioni raccolte nelle banche dati esterne (valore secondo esperti prossimo alla vera percentuale di efficacia del sistema), e che 1000 di questi passeggeri siano realmente terroristi. Utilizzando questi dati otteniamo che circa 6 milioni di persone saranno segnalate dal programma come terroristi o affini. Ma, dato che se su 6 milioni di persone solo mille erano implicate in atti terroristici veri e propri, ogni persona segnalata dal sistema ha solo lo 0.01% di probabilità di essere realmente un soggetto pericoloso, mentre il 99,99% verrà indagato ingiustamente[50].
Ogni nominativo inserito in questa "lista nera", viene poi divulgato alle autorità competenti come sospetto terrorista. Quindi i controlli sulla sua persona aumenteranno a seconda del grado di pericolosità a lui associato: questo implica che le generalità di una stessa persona possano coincidere in città grandi, come ad esempio New York e Los Angeles, il risultato è che persone innocenti possano essere trattenute o indagate ingiustamente, a causa di un errore nella fase di calcolo del rischio da parte del software.
Riguardo il grado di sicurezza dei dati raccolti dal C.A.P.P.S. contro attacchi esterni al sistema o da abusi il discorso risulta controverso. In un rapporto del G.A.O.[51] viene illustrata l'importanza di una serie di elementi di sicurezza (polizze di sicurezza, certificazioni autenticate sul livello di sicurezza del sistema, un piano di controllo dei rischi ecc. ecc.) atti a garantire che i dati accumulati nei database del C.A.P.P.S. non siano suscettibili ad attacchi hacker o addirittura da abusi illeciti di tali dati da parte di persone interne al sistema. Dal suddetto rapporto emerge che il livello di sicurezza del software e delle sue banche dati non sia riconosciuto da certificati di alcuna sorta; che il T.S.A. sembri ancora temporeggiare; e che al febbraio 2004 il programma non abbia un adeguato livello di sicurezza[52]. I difetti riscontrati dal GAO nell'analisi del C.A.P.P.S. non riguardano solo questo sistema ma sono problemi che affliggono ogni sistema che tratta dati sensibili.

5.4. C.A.P.P.S. e Costituzione Americana

Tutte le proteste sollevate contro il progetto del C.A.P.P.S. sono basate su fatti concreti, i più importanti (tralasciando gli aspetti di ordine etico e morale) sono inerenti ai confitti sulla legittimità in relazione alla carta costituzionale delle indagini svolte dal sistema.
Il primo conflitto con l'apparato legislativo si ha con l'infrazione dell'articolo riguardante il diritto a viaggiare liberamente sancito all'interno della costituzione. Come già detto, il C.A.P.P.S. a fronte dei dati raccolti può bloccare o rallentare significativamente i trasporti per determinate persone che risultano "potenzialmente" pericolose; inoltre sarà difficile per il malcapitato capire come mai gli è impossibile viaggiare (risalire quindi ad un sistema di Pre-Screening). In questo modo chiunque risulti nelle liste (e come già visto non è detto che chiunque ne faccia parte possa essere

50 elaborazione inclusa nella Nota del 30/9/2003 spedita al dipartimento della difesa statunitense
51 Febbraio 2004, rapporto sulla sicurezza dei voli, C.A.P.P.S.
52 idem nota 51

effettivamente un soggetto pericoloso) vede precludersi un diritto costituzionale solo a causa di un software che ha generato un "sospetto di colpevolezza" sulla propria persona e sulle attività da lui condotte.
Così recita il primo emendamento della costituzione americana (1971), uno dei più importanti della Costituzione stessa, in cui viene sancito il diritto di ogni persona ad esercitare il diritto di stampa, associazione, religione e parola ovunque e senza che nessuno possa impedire tale attività: *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."*[53]. Il C.A.P.P.S. come già sappiamo attinge informazioni da fonti (più o meno attendibili) sulle attività personali di ogni passeggero: abitudini alimentari, religiose, professionali ecc. Sostanzialmente però il C.A.P.P.S. non vieta a nessuno di lavorare liberamente, o di non esprimere le proprie opinioni in libertà, da dove viene quindi questa pesante infrazione al primo emendamento? Virgine Lawinger, attivista politico di Milwaukee è stato ingiustamente trattenuto in aeroporto a causa delle sue idee politiche prima di poter accedere al volo; due giornalisti sono stati interrogati da agenti F.B.I. solo a causa della loro propensione politica e pacifista[54]; questi, e molti altri, sono esempi di come l'inserimento della propria persona in una lista nera del software possano minare diritti costituzionali dichiarati intoccabili.
Ma il caso di infrazione grave è quello al 4° emendamento: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*[55]. Risulta in effetti chiaro che il metodo di investigazione e raccolta dati del C.A.P.P.S. non lo rispetti assolutamente. Infatti le persone sono per lo più ignare della raccolta dei loro dati personali visto che la fase di assegnazione del livello di rischio e raccolta dati da parte del C.A.P.P.S. è assolutamente segreta condotta semplicemente al fine di raccogliere dati statistici, e quindi senza una chiara fonte di sospetto sulla persona indagata. Dato il livello di affidabilità del C.A.P.P.S. poi non solo i terroristi vengono indagati ma anche innocenti che vedono letteralmente "rubare" le proprie informazioni, un po' come subire una perquisizione in casa propria in modo arbitrario e senza un mandato regolamentare.

53 Citazione da: Costituzione Americana, 1° Emendamento
54 Justin Jouvenal 28/7/2003
55 Citazione da: Costituzione Americana, 4° Emendamento

6. L'Europa e la privacy per la sicurezza aerea

Come l'Europa si muove nei confronti degli Usa riguardo lo scambio di dati dei passeggeri
a cura di Cristina Puccinelli

6.1. Introduzione

Come già visto nei capitoli precedenti questa tesina si pone l'obiettivo di spiegare quale sia l'impegno degli USA per aumentare la sicurezza aerea al momento dell'imbarco attraverso sistemi di prescreening che possano accedere ad ogni forma di dati personali del passeggero. Questo capitolo in particolare si focalizza su un altro grande paese, su cui gli Stati Uniti d'America puntano per poter difendersi via informatica da possibili attacchi: L'Unione Europea. La UE in questo frangente non ha messo a punto programmi come il CAPPS od il CAPPS II, ma allo stesso tempo non rimane indietro con l'analisi dei dati personali dei passeggeri aerei. Proprio per questo gli Usa hanno chiesto all'Unione Europea uno scambio di dati dei passeggeri diretti negli Stati Uniti in modo da cautelarsi.

6.2. Stati Uniti ed Unione Europea: primi passi sullo scambio di dati

Quando gli Stati Uniti annunciarono il 19 Settembre 2001 che entro il 5 Marzo 2003, tutte le compagnie aeree internazionali, avrebbero dovuto fornire l'accesso elettronico a tutti i dati dei passeggeri di volo, subito si levò da parte di queste ultime un veto in quanto questo scambio di dati avrebbe leso le normative europee tuttora vigenti. Questi dati, secondo quanto richiesto dagli Stati Uniti, comprendevano il nome, l'indirizzo, il numero di volo, il numero della carta di credito ed il pasto scelto dal passeggero. Dati tutti annotati nel PNR (Passenger Name Record – Registro Nomi Passeggero, vedi in seguito).

> *"Since 5 February, 2003, the U.S. requires in-flying airlines to give access, upon request, to the data processed by their reservations and departure control systems, and in particular to Passenger Name Records (PNR). This requirement raises difficulties for the application of European law on data protection and specific provisions on the EU Regulation on Computerised Reservation Systems."*[56]

L'Unione Europea interpellata quindi dalle proprie compagnie di volo, riguardo queste dichiarazioni risalenti ai mesi successivi l'attacco al World Trade Center, dichiarò che l'uso dei dati dei propri passeggeri da parte degli Stati Uniti, avrebbe violato le norme sulla sicurezza e sulla privacy esposte dalle proprie leggi e mise in discussione il fatto che la segretezza dei loro cittadini fosse adeguatamente protetta. Per l'appunto la Legge europea di protezione dei dati personali prevede l'accesso da parte delle autorità soltanto nei casi in cui esista una base di probabile sospetto del passeggero, inoltre richiede che i dati raccolti per uno scopo non vengano usati per un altro fine, soprattutto se le informazioni riguardano la religione, l'affiliazione etnica o politica della persona.
Alla fine, sia gli Stati Uniti sia l'Unione Europea dichiararono, sempre nel 2003, di cooperare per formulare una disposizione riguardo il trattamento di dati personali che possa essere accettata dalle compagnie di volo senza violare le leggi esistenti.

> *"On 17-18 February 2003, a high-level meeting between representatives of the European Commission and U.S. Customs (now Customs and Border Protection), took place to try to find a mutually satisfactory solution, providing legal certainty. After the*

56 Passenger Name Record fact sheet – Unione Europea – link: http://ec.europa.eu/comm/external_relations/us/sum06_03/pnr.pdf

meeting, both sides issued a Joint Statement containing certain undertakings by U.S. Customs with regard to how they will handle the transmitted personal data."[57]

La Commissione Europea abrogò una disposizione ad interim in cui era scritto che i cittadini europei acconsentivano a non far rispettare le leggi sulla privacy, fin quando non fosse stato trovato un accordo. Nello scambio, gli Stati Uniti avrebbero offerto chiarificazioni sul metodo di "trattare" i dati personali.

"In order to establish a legally sound basis for the transfers, both sides agreed to work together towards a bilateral arrangement involving the adoption by the European Commission of a Decision under Article 25.6 of the Directive on Data Protection (95/46) in response to additional undertakings by the U.S. side about the manner in which data would be handled and protected in the U.S. Such a Decision, stating that the European Commission finds that the U.S. authorities ensure an "adequate" level of protection, would be binding on all Member States. The process by which this could be achieved requires the involvement of Data Protection Authorities, Member States and the European Parliament."[58]

Solo come nota complementare, l'articolo 25.6 della direttiva 95/46/CE sopraccitata del parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, afferma che "*La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona."*

Riprendendo il discorso precedente, è da notare che questa "satisfactory solution" era già stata proposta il 5 febbraio 2003, quando gli Stati Uniti richiesero il permesso, come già detto, di poter accedere ai dati dei passeggeri europei tramite il PNR. Questo requisito solleva in un certo senso le responsabilità dei due paesi e delle compagnie aeree.

"On 13 June 2003 the Article 29 Data Protection Working Party adopted Opinion 4/2003 on the level of Protection ensured in the U.S. for the Transfer of Passenger Data. In this Opinion the Working Party identifies the areas where improvements to the present U.S undertakings are still necessary in order to meet the adequacy standard set by the Directive."

Fino a pochi giorni fa, come si può leggere nell'ultimo paragrafo di questo capitolo riguardante l'Europa, lo scambio di dati continuava in quanto il livello di protezione adottato poteva venir modificato per rispondere agli standard di protezione europei senza eccessivi problemi.
Dopo questo spaccato generale, analizzerò più nel dettaglio gli aspetti legali di questi movimenti, il PNR europeo e come finora sono state portate avanti le discussioni fra gli Usa e l'Unione Europea.

6.3. Aspetti Legali

Riporto qui sotto alcuni articoli della Direttiva 95/46/CE che impone in generale i requisiti per il trattamento di dati personali:

"ARTICOLO 1

57 idem nota 56
58 idem nota 56

Oggetto della direttiva

1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

2. Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1."[59]

La direttiva 95/46/CE viene applicata nel caso in cui i dati delle persone fisiche identificate o identificabili (ARTICOLO 2: *"si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"*) sono sotto trattamento delle autorità competenti (ARTICOLO 2: *"Trattamento: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione"*).
Ciò deve essere compiuto in modo specifico, esplicito e legittimo (*"ARTICOLO 6: a) trattati lealmente e lecitamente; b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità."*) in modo che la raccolta di dati sia sufficiente, relativa e non eccessiva rispetto agli scopi per cui i dati sono raccolti e soprattutto devono essere esatti ed immagazzinati soltanto fin quando necessario (ARTICOLO 6: *"c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati; d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati"; e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici"*).
Per concludere, questi sono i principali articoli riguardanti l'acquisizione di dati personali ed il conseguente trattamento, ma innumerevoli altri ne conseguono da questi che per ovvi motivi di sintesi ho preferito non inserire.
L'unico che però, di quelli successivi e non riportati, mi ha fatto riflettere (è soltanto una mera opinione personale) è l'ARTICOLO 8 che riguarda il trattamento di dati che attinenti a particolari categorie:

"Gli Stati membri vietano il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale."

A seguire, sono stati elencati vari aspetti della persona per i quali è vietato il trattamento dei dati. Non sono tanto questi ciò che reputo importante, ma l'articolo in se per se, che elenca il modo per

59 http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:IT:HTML

cui non bisogna applicare la raccolta di dati. E' da notare che sono proprio alcuni di questi aspetti che i programmi di prescreening USA vanno a ledere.

6.4. Cosa è il PNR – Passenger Name Record

Il PNR è l'acronimo di Passenger Name Record, che letteralmente significa "Registro nomi passeggeri" ed è un generico nome dato ai files creati dalla compagnie aeree al momento della prenotazione, in cui vengono annotati i dati per ogni viaggio effettuato. Questi dati vengono successivamente registrati in un Database generale e ciò permette ad un qualsiasi agente di una compagnia aerea di avere accesso ad ogni tipo di dato riguardante il volo di un determinato passeggero: voli di partenza e di ritorno, voli di scambio ecc ecc.
Oltre a questi dati prettamente riguardati il volo, il PNR comprende molti altri campi, come dichiarato dall' Unione Europea *"There are approximately 20-25 possible fields of PNR data, some of which include subsets of information, expanding the total to approximately 60 fields and sub-fields"* che comprendono eventuali prenotazioni di alberghi, di noleggio auto, o di altri servizi o viaggi speciali fatti attraverso agenzie.
Secondo EPIC, sono raccolti anche altri dati che esulano del tutto dal viaggio quali: *"health, paid price, banking co-ordinates, telephone number of a person to be contacted in the event of problem, place of lodging in the country of destination, name of people with whom the person travels. In certain cases it might contain the history of the preceding voyages and the choice of meal."*
Secondo un esempio esempio, sempre fornito da EPIC: *"A passenger, usually, may choose "no pref, baby, child, pure vegetarian, vegetarian (lacto), fruit, raw, seafood, high fiber, diabetic, low calorie, low fat/low cholesterol, low protein, low sodium, no lactose, Asian vegetarian, Asian, Hindu, kosher, Musli, Bland." The specifications "Asian vegetarian, Asian, Hindu, kosher, Musli, Bland" make obvious that these data must be regarded as a category of "special sensitive data" because they could reveal the religious or ethnic background of the passenger."*
E ciò dà da pensare su quanto quest'acquisizione di dati vada oltre la sola prenotazione aerea.

6.5. Unione Europea Oggi

Proprio pochi giorni fa è stato pubblicato un articolo riguardante lo scambio di dati dei passeggeri fra Stati Uniti ed Europa. Ho preferito riportare l'articolo, di un giornale quotidiano toscano, perché esplica in modo chiaro e conciso la situazione che si è venuta ad instaurare negli ultimi mesi e come la UE porterà avanti la questione dello scambio dei dati.
Da il Tirreno del 31/05/2006 [Didascalia foto di un A320: Vietato fornire dati sui passeggeri diretti in Usa]

> *"Bocciata l'intesa con la Ue. A rischio i voli per gli Usa.*
>
> *La Corte Europea ha annullato la decisione delle istituzioni comunitarie sul trasferimento di dati personali dei passeggeri di voli transatlantici alle autorità Usa. Il provvedimento […] aveva trovato l'opposizione del Parlamento Europeo preoccupato del mancato rispetto della privacy. La bocciatura della Corte è motivata dal fatto che le "decisioni non sono fondate su basi giuridiche appropriate" e non entra nel merito dei motivi addotti dall'assemblea di Strasburgo. I Giudici Europei hanno inoltre deciso di mantenere in vigore l'attuale sistema di trasferimento dei dati fino al 30 settembre prossimo per "ragioni di certezza del diritto e per proteggere le persone interessate".*
>
> *Nel Frattempo, Ue e Usa dovrebbero trovare una soluzione alternativa. "non possiamo immaginare che dopo il 30 settembre non vi sia più una regolamentazione europea nello*

scambio di informazioni sui passeggeri", ha affermato il vicepresidente della Commissione Franco Frattini sottolineando che la Commissione sta lavorando "per garantire la continuità" e puntando sul fatto che la Corte "non ha criticato la sostanza dell'iniziativa, ma lo strumento giuridico scelto" per attuarla. Per far fronte alla bocciatura, Frattini ha annunciato che presenterà già dopo domani [02/06] delle proposte concrete al Consiglio dei ministri interni e giustizia dei 25 riuniti a Lussemburgo. Prudente la reazione del Parlamento Europeo che, dopo aver chiesto alla Corte del Lussemburgo un pronunciamento, ora si mostra soddisfatto a metà. I membri della competente commissione hanno esaminato la sentenza, con gli esperti giuridici, in una riunione a porte chiuse. E non manca chi fa notare che il giudizio della Corte potrebbe spostare ora la competenza della decisione sul trasferimento dei dati dalla sede comunitaria ai singoli stati Ue."

Direi che non ci resta che attendere.

7. Conclusioni

7.1. L'informazione riguardo ai rischi sulla privacy

Durante la stesura della tesina, il problema che ci è sembrato più grave è che nel panorama della discussione pubblica ad ogni livello manca completamente l'attenzione verso i temi del rispetto della privacy e in particolare dei sistemi di prescreening che la violano.
Riteniamo che la creazione di un sistema di così alta rilevanza e complessità e con un così importante impatto sociale debba necessariamente essere accompagnato da un'informazione e una discussione approfondite.
Al contrario il governo americano adotta una politica comunicativa allarmistica propagandando come obbiettivo primario la lotta al terrorismo. Questa esasperata semplificazione pone in secondo piano ogni aspetto relativo alla difesa della privacy e in generale dei diritti civili, tacciando come nemico degli Stati Uniti chiunque si opponga alle politiche adottate.
In scelte su temi di così grande importanza non si è data rilevanza all'opinione pubblica, tentando in primo luogo di rendere più celata e ambigua possibile la discussione. Il risultato è che l'approvazione in sede ufficiale di tanti provvedimenti fondamentali è passata nel silenzio.
Questo clima di disinformazione si è creato anche a causa del disinteresse dei mass media che non hanno prestato all'argomento l'attenzione che merita.

7.2. Il nostro giudizio sulla sicurezza dei sistemi

Dalle nostre ricerche possiamo concludere che con le tecnologie attuali i sistemi di prescreening non possano raggiungere la sicurezza necessaria e che sia impossibile garantire la loro impenetrabilità e quindi la riservatezza dei dati personali. Esiste quindi il rischio concreto che le informazioni raccolte siano usate per scopi pericolosi per la società. Ci risulta anche difficile pensare che la sicurezza informatica possa in futuro raggiungere la perfezione, visto che tendenzialmente rendendo più complicato un sistema, si ha come effetto negativo di renderlo più vulnerabile e non più sicuro.
D'altra parte non ci sentiamo in grado di esprimere un giudizio su coloro i quali spingono per la creazione di tali sistemi. Non sappiamo infatti se questa spinta avvenga in mala fede e con obbiettivi nascosti che mirano alla creazione di un sistema di sorveglianza per la limitazione delle libertà civili, oppure se si tratti di errori provocati dall'eccessiva fiducia nella tecnologia.

7.3. La risposta al terrorismo

Non può funzionare contro il rischio delle organizzazioni terroristiche una risposta da parte dei governi occidentali basata sull'offesa. Utilizzare contro il terrorismo l'arma dello stesso terrorismo porta solamente all'inasprimento del conflitto. Non può esistere un sistema che renda una nazione immune dagli attentati, sia per la “semplicità” con cui essi possono essere realizzati sia per la determinazione che hanno i terroristi.
Per questo pensiamo che l'ingente spesa economica destinata ai sistemi di prescreening e in generale alla prevenzione del terrorismo sarebbe potuta, con migliori risultati, essere destinata a un intervento di aiuto diretto ai paesi da cui il terrorismo nasce. Per evitare il fenomeno del terrorismo bisogna infatti cercare nel disagio sociale le motivazioni che portano a questi gesti estremi, cercando di eliminare le basi dell'odio e facendo terra bruciata intorno a quei signori della guerra che fomentano il terrorismo.

8. Bibliografia

Siti governativi

Sito ufficiale della TSA (Transport Security Administration)
http://www.tsa.gov

Sito ufficiale del DHS (Department of Homeland Security)
http://www.dhs.gov

Sito ufficiale dell'Unione Europea
http://www.europa.eu/

Associazioni per la difesa della privacy

EPIC (Electronic Privacy Information Center)
http://www.epic.org

ACLU (American Civil Liberties Union)
http://www.aclu.org

Privacy International
http://www.privacyinternational.org

Electronic Frontier Foundation
www.eff.org/

Privacy Activism
www.privacyactivism.org

Quotidiani e media

Washington Technology
http://www.washingtontechnology.com/

The Age
http://www.theage.com.au

Earth Web News
http://news.earthweb.com

BTNonline.com
http://www.btnonline.com/

FCW.com
http://www.fcw.com/

Sueddeutsche.de
http://www.sueddeutsche.de/

China Daily
http://www.chinadaily.com.cn/english

BBC News
http://news.bbc.co.uk

La Repubblica
http://www.repubblica.it/

Il Tirreno
http://www.iltirreno.quotidianiespresso.it/

Su US-VISIT

Pagina di EPIC su US-VISIT
http://www.epic.org/privacy/us-visit/

Pagina del DHS sul progetto US-VISIT
http://www.dhs.gov/dhspublic/display?theme=91

Sul database biometrico

Privacy International sul database biometrico
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-73837

EPIC sulla biometria
http://www.epic.org/privacy/biometrics/

Pagine di Wikipedia

Pagina di Wikipedia su CAPPS
http://en.wikipedia.org/w/index.php?title=Computer_Assisted_Passenger_Prescreening_System&oldid=55167271

Pagina di Wikipedia su US-VISIT
http://en.wikipedia.org/w/index.php?title=United_States_Visitor_and_Immigrant_Status_Indicator_Technology&oldid=49362424

Pagina di Wikipedia su RFID
http://en.wikipedia.org/w/index.php?title=Radio_Frequency_Identification&oldid=56102533

Altre fonti consultate

Sito del GAO (General Accounting Office)
http://www.gao.gov

Sito del Web Application Security Consortium
http://www.webappsec.org/

Sito del Center for Responsive Politics con i dati sul finanziamento delle campagne elettorali
http://www.opensecrets.org/

Pagina della borsa di New York (New York Stock Exchange) sulle quotazioni di Accenture
http://www.nyse.com/about/listed/lcddata.html?ticker=acn

Sito di Bruce Schneier (Schneier on Security)
http://www.schneier.com/blog

Testo della Costituzione Statunitense
www.usconstitution.net/