PRESIDENZA DEL PRESIDENTE MARIO VALDUCCI

La seduta comincia alle 12,40.

(La Commissione approva il processo verbale della seduta precedente).

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso e la trasmissione televisiva sul canale satellitare della Camera dei deputati.

Audizione di rappresentanti della società Securiport.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sul sistema aeroportuale italiano, l'audizione di rappresentanti della società Securiport.

L'audizione è stata inserita nel calendario dell'indagine conoscitiva per permettere alla società Securiport di illustrare i sistemi tecnologici di controllo e di sicurezza negli aeroporti da essa sviluppati e già adottati negli Stati Uniti e, da ultimo, anche da parte dell'aeroporto internazionale di Francoforte.

Do la parola all'ambasciatore Jose Sorzano, presidente del consiglio di amministrazione della società e, successivamente, al vicepresidente, signor Whit Turner.

JOSE SORZANO, *Presidente del consiglio di amministrazione di Securiport*. Vi ringrazio per l'invito, che ci consente di presentarvi la tecnologia che è alla base della nostra attività.

Sono l'ambasciatore Jose Sorzano, presidente della Securiport; è qui con me anche il vicepresidente, Whit Turner.

Vorrei accennare brevemente ai nostri trascorsi. Sono stato ambasciatore americano presso le Nazioni Unite per cinque anni e poi direttore degli Affari della Sicurezza Nazionale per l'emisfero occidentale alla Casa Bianca. Whit Turner, invece, è stato pilota della marina militare e ha lavorato in varie agenzie governative negli ultimi venticinque anni, trattando temi di sicurezza nazionale. Da circa 25-30 anni, dunque, ci occupiamo di sicurezza nazionale.

La Securiport è una società nata dopo l'11 settembre, allo scopo di fornire ai Governi la tecnologia adeguata al fine di avere un sistema veloce, sicuro e affidabile per controllare le persone in ingresso e in partenza attraverso i propri confini.

La nostra tecnologia consiste in una serie di elementi: innanzitutto un *hardware front-end* e alcuni prodotti *software back-end*. Il nostro *hardware front-end* prevede, anzitutto, uno *scanner* di impronte digitali, un elemento che segna una grande differenza nella nostra tecnologia.

La tecnologia che abbiamo incorporato nel nostro sistema si basa sugli ultrasuoni. Le onde ultrasonore sono capaci di penetrare strati di diversa densità, a prescindere dal grado di sporcizia delle dita. Si tratta della stessa tecnologia che consente di effettuare le ecografie sulle donne in gravidanza. Quindi, anche se le dita sono molto sporche o lo stesso scanner è sporco, l'apparecchio riesce a cogliere comunque un'immagine estremamente nitida.

Per darvi una dimostrazione di come funzioni la nostra tecnologia, mi sporco il dito con un pennarello e poi lo pongo sullo *scanner*. Con una densità di 500 dpi *(dot per inch)*, che corrisponde allo standard utilizzato dall'FBI nelle sue indagini, come vedete l'immagine è stata catturata. Lo *scanner*, quindi, è riuscito a passare attraverso lo sporco.

Anche in caso di presenza di qualunque altro contaminante (sugo, grassi o sporco di ogni genere) l'acquisizione dell'immagine sarebbe ugualmente chiara. La possibilità di avere una riproduzione nitida e di buona qualità migliora l'accuratezza dell'identificazione; al contrario, peggiore è l'immagine e più lento è il processo di identificazione.

Una volta acquisita l'immagine dell'impronta digitale, si inserisce il passaporto in uno *scanner* apposito, che ha una biblioteca interna e analizza se il documento è in corso di validità, se l'inchiostro è regolamentare per un passaporto italiano, francese o brasiliano, se gli ologrammi sono nella posizione corretta e via dicendo. In questo modo, l'apparecchio riesce a stabilire innanzitutto se il documento è valido. Inoltre, lo *scanner* cattura le informazioni in maniera automatica, evitando all'operatore di digitarle e quindi velocizzando il processo. Alla fine, se il passaporto è valido, la macchina lo comunica e dà istruzioni all'operatore per acquisire la fotografia e quindi le impronte digitali e procedere all'identificazione.

Anche la fase *back-end* è estremamente importante. Essa si basa sull'uso di *software* che sono il cuore del processo. Tra questi innanzitutto l'AFIS *(Automatic Fingerprint Identification System)*, un programma che determina la corrispondenza tra un'impronta digitale e le numerose impronte acquisite e già memorizzate nel *database*. Questo *software* consente di stabilire se l'individuo in questione è già stato visto prima o meno, se è stato visto in entrata o in uscita nel Paese, se è nella lista delle persone sospette (la cosiddetta « *watch list* »).

Esiste, poi, un altro *software* che consente al Governo di inserire nella *watch list* tutte le persone indesiderate all'interno del Paese, che non possono entrare né uscire, per motivi di sicurezza nazionale o sulla base di informazioni dell'Interpol. Da ultimo, vengono memorizzate nel *database* tutte le informazioni: l'immagine acquisita dal passaporto, la riproduzione del visto, se richiesto per determinati passeggeri, tutte le informazioni personali, compresa la fotografia del volto e le impronte digitali, e le indicazioni riguardanti l'ingresso nel Paese e l'uscita dallo stesso.

Ritengo che, oggi, tutti pensino agli aspetti economici. Ebbene, la Securiport fornisce la tecnologia per l'installazione, l'addestramento degli operatori e il finanziamento necessario, quindi non c'è un impatto economico sul Paese che acquisisce il nostro sistema. La Securiport, infatti, incassa un'imposta che il passeggero paga acquistando il biglietto aereo.

Le informazioni acquisite sono di proprietà esclusiva del Paese. La nostra società installa la tecnologia e fornisce l'addestramento, ma tutte le informazioni delicate e confidenziali acquisite appartengono, ad esempio se si tratta dell'Italia, alle autorità italiane. Noi forniamo l'*hardware* e il *software*, ma sareste voi a criptare la tecnologia, per cui solo l'Italia avrebbe accesso ad essa.

Da un anno e mezzo lavoriamo in Germania: abbiamo installato la nostra tecnologia, come dimostrazione, all'aeroporto di Francoforte, che peraltro ha scritto per noi una lettera di raccomandazioni, che vi abbiamo inoltrato.

Vorrei dimostrarvi come funziona la nostra tecnologia e chiederò, dunque, al dottor Turner e al dottor Fagone di fingere di essere passeggeri in arrivo alla postazione dell'agente dell'immigrazione.

WHIT TURNER, *Vicepresidente di Securiport*. Io mi sono già registrato nel sistema, dunque sono già presente nei dati. Vedete con quale velocità e con quanta precisione viene rilevata la mia presenza. Il sistema automaticamente acquisisce l'immagine del passaporto e opera tutti i controlli di sicurezza su di esso. La risposta si basa su un codice cromatico, in

modo tale che risulti facile all'operatore capire qual è l'esito del controllo.

In questo caso, il documento viene considerato sconosciuto dal sistema, quindi si deve effettuare un controllo visivo (dopo faremo la dimostrazione con un altro passaporto che, invece, sarà riconosciuto dal sistema). Il programma importa tutte le informazioni contenute nel passaporto e le trasferisce automaticamente nel database. Se vi sono problemi, vengono segnalati: in questo caso, ad esempio, il *software* indica che parte dell'ultravioletto è difficile da leggere. Potete notare, infatti, che l'ultravioletto non è completo. Se è necessario, posso verificare visivamente e cogliere la presenza di un visto – ovviamente, nel vostro caso in italiano – in modo tale che venga acquisita automaticamente anche questa informazione e possa essere immessa nel *database* dei visti.

In questo caso, non ho attivato i visti italiani nella biblioteca, però qualunque documento (ad esempio, la patente o un permesso di soggiorno) viene riconosciuto automaticamente. Si possono immettere i dati relativi ai visti nei campi appositi, in maniera tale che restino registrati.

SALVATORE FAGONE, *Direttore per l'Europa di Securiport*. Questo non è un visto elettronico. È un visto libico, quindi i dati devono essere immessi manualmente.

WHIT TURNER, *Vicepresidente di Securiport*. Se vi sono elementi, quali data di emissione e di scadenza, numero di ingressi consentiti nel Paese, uscite ed entrate e se esiste un'eccezione a quanto autorizzato, ciò viene subito portato all'attenzione dell'operatore.

Proseguendo con la nostra dimostrazione, analizziamo ora l'indice della mano sinistra del dottor Fagone. Come vedete, in ogni fase vi sono delle istruzioni per l'operatore. Si usa anche un codice cromatico, secondo il quale il verde significa che sono stati effettuati tutti i controlli sulla qualità dell'immagine acquisita del dito. I dati vengono immessi nel sistema se la qualità è sufficiente; in caso contrario, i dati non vengono immessi. In caso di discrepanze, il colore è il rosso e viene indicato il problema.

Ora, immettiamo i dati relativi al volo. Quando si completa l'elaborazione dei dati personali, se la persona passa attraverso questo sistema per la prima volta, verrà fatto un controllo sul *database* per vedere se le informazioni vi sono già contenute: numero di passaporto, nome e impronte digitali. Si possono presentare varie eventualità, per esempio che si tratti di una persona con due passaporti o due cittadinanze. In ogni caso, per ogni transazione di ingresso o di uscita, il sistema controlla le impronte, il nome, il numero del passaporto e fa un confronto con la *watch list*, dunque comunica all'operatore se il soggetto deve essere trattato in modo particolare. I messaggi pre-impostati hanno un tono cortese, ma possono comunque essere adattati alle proprie esigenze. Nel nostro caso, il sistema dice che occorre fare ulteriori valutazioni, quindi la persona in questione deve essere indirizzata ad un controllore responsabile.

Ora, per proseguire la nostra dimostrazione, assumo il ruolo del controllore responsabile, che ha il compito di analizzare ogni transazione. Nel caso il sistema rilevi dei dati relativi ad una persona pericolosa, la segnalazione sarà indicata dal colore rosso. Nel nostro esempio, il dottor Fagone è un soggetto nuovo, ma il sistema ha individuato un dato presente che corrisponde, l'impronta. Come possiamo vedere, però, non c'è corrispondenza, quindi prendiamo in considerazione gli altri dati o le credenziali della persona per accertarci della sua identità.

Analizziamo ora l'esempio di una persona ricercata che ha rubato un passaporto per cercare di uscire dal Paese. Io sono a Roma e il mio passaporto viene rubato da qualcuno che è in attesa di giudizio da parte di un tribunale italiano e cerca di lasciare il Paese. Il sistema verifica il passaporto e rileva che il documento è valido, quindi non esistono impedimenti. Naturalmente, il visto non è presente, perché si tratta di uscita dal

Paese, ad esempio verso l'Albania. Per la scansione dell'impronta userò queste due dita presenti nel sistema come appartenenti a un criminale. Il passaporto è regolare, ma l'impronta, ovviamente, rileva dei problemi. Come potete vedere, una volta terminata la transazione, il sistema mi segnala che manca la fotografia, che ora acquisiamo.

L'applicazione è progettata in modo tale che il suo utilizzo sia molto facile per l'operatore e che le possibilità di errore siano ridotte al minimo. Inoltre, le operazioni più impegnative (l'impostazione della qualità dell'immagine, il controllo dell'impronta) sono eseguite dal sistema e non dall'operatore. Nel nostro caso, si rileva un'anomalia, quindi il soggetto deve essere inviato a un supervisore.

Ora mi immedesimo nella figura del supervisore e vi mostro ciò che questi vede sul monitor. La persona sospetta arriva scortata e il supervisore esamina i suoi dati ipotizzando che, forse, possa essere presente sulla *watch list*. Esamina, quindi, le impronte e scopre che sono le impronte di un criminale, di cui viene indicato il nome; questo è uno dei punti di forza del sistema. Abbiamo un *database* in cui ci sono tutti i dati relativi ai viaggi di ogni soggetto, oltre alla *watch list,* in cui l'Interpol può immettere dati relativi a qualunque persona sospetta. Alcune informazioni, se per esempio la persona in questione soggiorna in un albergo nel quale è stato commesso un reato, possono essere immesse in modalità temporanea o permanente, Una persona ricercata può essere identificata dal sistema in entrata o in uscita dal Paese e ciò consente di intervenire alle forze dell'ordine.

Vi faccio vedere rapidamente il procedimento seguito dal sistema nel caso di una persona già presente nello stesso. Il soggetto arriva e si immette il passaporto nello *scanner*, operazione che richiede, di solito, quindici secondi. Nel sistema dal vivo appaiono automaticamente i dati sulle impronte e il sistema effettua la ricerca automaticamente.

Si tratta di un sistema molto veloce. Se una persona passa per la prima volta il sistema richiede uno o due minuti, a seconda che ci sia o meno un problema di comunicazione, ma è comunque molto rapido e consente di acquisire tutte le informazioni necessarie. Inoltre, se vi è qualcosa sul passaporto che rende difficile o impossibile la lettura – penso ai Paesi che hanno i passaporti scritti a mano – il documento viene ingrandito. Quindi, l'operatore può leggere con maggiore facilità i dati e trasferirli senza doverli digitare sulla tastiera personalmente.

Vorrei parlare, ora, della gestione della *watch list* e del *database*. Questa è una funzione del supervisore, il quale può cercare chiunque, in base al cognome, al numero del volo, alla nazionalità. I criteri di ricerca sono tantissimi e, a partire da questi, si può impostare una ricerca di gruppi di persone. Ad esempio, possiamo chiedere al sistema di indicare tutti i soggetti arrivati con Air France la settimana scorsa e magari di ridurre la ricerca solo ai maschi e, tra questi, a coloro che hanno la nazionalità di determinati Paesi.

Si tratta, dunque, di uno strumento di ricerca potentissimo, poiché contiene dati esaurienti sui viaggi di tutte le persone transitate. Il sistema rende possibile, inoltre, la rimozione dei soggetti e dei loro dati dal *database*.

Vi mostro un esempio del *watch list manager*, la funzione che gestisce questo elenco con lo scopo di supervisione. Il *watch list manager* consente di applicare molte modalità di inserimento delle persone nella lista, in modo da evidenziare caratteristiche diverse. Prendiamo il caso di determinati soggetti immessi nel sistema senza che vi siano particolari segnalazioni; questa funzione permette di assimilare tutti i dati (come l'impronta) per poterli, poi, individuare nel *database* e aggiungerli, quindi, alla *watch list*.

Il sistema consente di recuperare l'elenco di tutte le persone che sono sulla *watch list*. Questo tipo di operazione segue lo standard di trasferimento elettronico e biometrico automatico dei dati usato da tutte le forze di polizia del mondo. Di conseguenza, le informazioni possono es-

sere aggiunte, si può cercare chiunque ed è possibile anche cancellare dei soggetti dal *database*.

Un fattore essenziale e di grande valore in un sistema di questo genere è la sicurezza, perché si tratta di informazioni sensibili. Abbiamo previsto una serie di misure di sicurezza. Innanzitutto il *database* è criptato, e i codici sono stabiliti dai committenti. Noi possiamo entrare nel sistema soltanto su vostra richiesta per aggiornarlo o per una supervisione.

Se per qualunque motivo si verifica un'anomalia, il progettista del *software* viene direttamente da voi e lavora al sistema, esclusivamente se autorizzato e in presenza di un funzionario che assiste all'intervento.

Per quanto riguarda la sicurezza, forniamo anche le autorizzazioni di accesso a diversi livelli di *login*. Pertanto, chi lavora in aeroporto e si occupa degli arrivi e delle partenze è autorizzato a fare solo questo: il personale non può utilizzare videogiochi né entrare nel *database*, ma può usare solo le funzioni che sono necessarie per svolgere la mansione che gli compete. Gli operatori, ai quali vengono prese anche le impronte, hanno un loro nome, un *login* e una *password*.

Qualunque transazione effettuata da un soggetto resta a lui associata: anche questa è una misura di sicurezza. A mano a mano che si innalzano i livelli di accesso, le persone vengono autorizzate e contrassegnate da un sistema di autenticazione.

Il sistema, in definitiva, garantisce un livello di controllo molto elevato.

A questo punto, penso di lasciare spazio alle domande che, senza dubbio, avrete da porre.

PRESIDENTE. Vorrei farvi una prima domanda che riguarda il tema dei costi – prima ci avete detto che non c'è un costo ma, in realtà, esso grava sul passeggero – legati alla possibilità di inserire questo sistema negli aeroporti.

Ho letto nella documentazione che avete presentato (se ho ben interpretato quanto è stato scritto) che negli Stati Uniti d'America è previsto un costo – definito la « tassa dell'11 settembre » – di 10 dollari su ogni biglietto. È chiaro che non si tratta di un costo marginale per un passeggero italiano o europeo. Dunque, vorrei sapere come è stato affrontato questo aspetto nel caso dell'aeroporto di Francoforte che si colloca, per l'appunto, in ambito europeo.

Vorrei, inoltre, sapere se questi impianti sono presenti in tutti gli aeroporti statunitensi.

Infine, voi avete parlato di una banca dati presente anche in un aeroporto di nuova installazione. Penso alle informazioni relative ai ricercati e quant'altro. Poiché quando si affronta questo tema si pongono problemi di riservatezza e di *privacy* relativamente al trasferimento delle informazioni, vorrei capire se esistono accordi tra i diversi Paesi – tra Stati Uniti e Italia sicuramente – per l'utilizzo di questi dati.

JOSE SORZANO, *Presidente del consiglio di amministrazione di Securiport*. In primo luogo, i costi del sistema dipendono dal volume di traffico dei passeggeri e dal tipo di volo, se internazionale o nazionale e via dicendo. Solitamente, il nostro sistema è usato soltanto per i passeggeri di voli internazionali in arrivo in un Paese, i quali devono passare attraverso il controllo dei passaporti.

Abbiamo rilevato che il volume del traffico è un fattore che determina l'ammontare della tassa supplementare sul biglietto. Gli Stati Uniti hanno adottato delle tasse per la sicurezza e abbiamo rilevato che il costo aggiunto al biglietto dalle compagnie aeree varia di giorno in giorno. Chiunque legga un biglietto aereo non riesce a capire l'ammontare delle varie tasse.

Abbiamo anche rivolto, al riguardo, delle domande alle autorità competenti in diversi Paesi nei quali abbiamo presentato la nostra tecnologia, e anche loro non sono in grado di scomporre le varie sovrattasse. Certamente, nei voli internazionali, ad esempio se si va da Washington a Roma con un biglietto di *business*, si spendono

migliaia di dollari e l'aggiunta di 5-10 dollari non viene notata rispetto all'importo del biglietto stesso.

Come ho detto prima, tutto dipende dal volume dei passeggeri e dall'investimento di capitali effettuato dall'aeroporto in cui viene installata la tecnologia; sono, poi, le autorità nazionali a dover stabilire un prezzo ragionevole.

Per quanto riguarda la domanda relativa all'aeroporto di Francoforte, in quel caso abbiamo installato la tecnologia per dimostrarne l'impiego e fare emergere il suo valore e la sua affidabilità, con l'idea di avvicinare Lufthansa. Vi abbiamo fornito i risultati del test effettuato (durato quasi due anni), non per l'identificazione dei passeggeri, ma per l'accesso alle varie zone riservate dell'aeroporto. La scorsa settimana abbiamo parlato con Lufthansa, azionista dell'aeroporto di Francoforte, per avanzare una proposta che sembra essere ben accetta. Inizieremo ad acquisire le informazioni sui passeggeri con la nostra tecnologia. Dunque, come spiegato in precedenza, il passeggero in arrivo al *gate* di Francoforte con destinazione, ad esempio, Washington presenterà visto e passaporto; dopodiché si procederà all'acquisizione dell'immagine e delle impronte digitali. Durante le nove ore di durata del volo, tutti i dati vengono trasferiti a Washington, dove vengono elaborati. Se non ci sono impedimenti, il passaporto del passeggero Lufthansa sarà stato già autorizzato. In questo modo, si snellisce il folle processo attraverso il quale normalmente si entra negli Stati Uniti. Lufthansa ha accettato la nostra proposta e ora stiamo lavorando per attuare questa nuova tecnologia.

Infine, all'ultima domanda rispondo che questa tecnologia non viene usata in tutti gli aeroporti statunitensi. Gli aeroporti statunitensi, al momento, non dispongono delle stesse capacità di scansione dei passaporti, ma dispongono di uno *scanner* per le impronte digitali: spesso però, se il dito è sporco, l'immagine acquisita non è di buona qualità. Secondo le statistiche, solo per l'88 per cento dei passeggeri che attualmente passano attraverso gli *scanner* ottici negli Stati Uniti la scansione va a buon fine. Esiste, dunque, un *gap* del 12 per cento. Credo che l'uso della tecnologia ad ultrasuoni consenta di migliorare questa percentuale.

WHIT TURNER, *Vicepresidente di Securiport*. Negli ultimi dieci anni, in tutto il mondo, sono state effettuate numerose valutazioni della tecnologia ad ultrasuoni per l'acquisizione di impronte digitali. In questo periodo, soltanto tre persone – in totale – non sono state registrate correttamente, in quanto non hanno potuto essere sottoposte alla scansione; in tutti e tre i casi si è trattato di persone che erano rimaste ustionate a seguito di incidenti e che avevano subito un trapianto di pelle.

L'ultrasuono, invece di fare semplicemente una foto del dito e di tutto ciò che si trova tra il dito e il sensore, acquisisce una cifra tridimensionale ultrasonica. Per cui si acquisiscono i dati X e Y, ma anche il dato Z, vale a dire la profondità, tanto che è stato possibile acquisire anche le impronte di categorie di persone dalle dita, per così dire, « difficili » (penso alle donne asiatiche, ai bambini, agli anziani e altri soggetti, come i muratori, i cassieri, ecc.).

Dieci anni fa, quando vigeva il sistema americano dei visti Ident (da me supervisionato), ho ritenuto fosse necessario passare ad una tecnologia migliore, quale l'Ultrascan. Se si arriva a perdere, infatti, un'alta percentuale di viaggiatori, il rischio è che il *database* diventi incompleto; inoltre, vengono meno i deterrenti e la fiducia degli operatori. Le persone con le dita leggermente sporche non passano nemmeno il controllo. Quando il numero delle persone da scansionare è molto alto, se non si ha un *database* aggiornato e una tecnologia altamente affidabile, si rischia di non essere efficienti.

PRESIDENTE. Avete detto che sui voli interni non viene mai utilizzata questa tecnologia. Nemmeno sul personale degli aeroporti ?

JOSE SORZANO, *Presidente del consiglio di amministrazione* di *Securiport*. Di-

pende dalle richieste e dalle necessità del Paese. In alcuni Paesi registriamo anche i passeggeri dei voli nazionali. Ci occupiamo anche delle informazioni relative ai passeggeri dei traghetti, ai controlli di frontiera, non solo negli aeroporti. Anche in questi casi installiamo la nostra tecnologia addebitandone i costi ai viaggiatori.

PRESIDENTE. Vorrei chiedere se questo tipo di sistema è stato correlato alle regole relative all'acquisizione di informazioni biometriche sulla base delle indicazioni europee. Inoltre vorrei chiederle se questa tecnologia è stata testata unitamente ai sistemi europei di acquisizione di queste impronte biometriche, come, ad esempio, il *border control system*.

JOSE SORZANO, *Presidente del consiglio di amministrazione di Securiport*. Credo che dovremo fornirvi questa risposta in un secondo tempo. Sono stato professore universitario alla Georgetown University e, a volte, quando uno studente mi poneva una domanda per la quale non avevo una risposta, non inventavo ma gli chiedevo di lasciarmi del tempo. Ora, faccio a voi la stessa richiesta: lasciateci del tempo per documentarci e vi risponderemo.

Se mi può fornire un appunto a proposito di questo test, potrò rispondere in modo accurato ed esatto.

PRESIDENTE. Ringrazio i rappresentanti della società Securiport per il loro intervento e dichiaro conclusa l'audizione.

La seduta termina alle 13,20.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

DOTT. GUGLIELMO ROMANO

Licenziato per la stampa
il 20 luglio 2009.

Gli interventi in lingua straniera sono tradotti a cura degli interpreti della Camera dei deputati

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

€ 0,35

Stampato su carta riciclata ecologica

16STC0004470