COMITATO PARLAMENTARE DI CONTROLLO SULL'ATTUAZIONE DELL'ACCORDO DI SCHENGEN, DI VIGILANZA SULL'ATTIVITÀ DI EUROPOL, DI CONTROLLO E VIGILANZA IN MATERIA DI IMMIGRAZIONE

RESOCONTO STENOGRAFICO

AUDIZIONE

2.

SEDUTA DI MARTEDÌ 16 GENNAIO 2007

PRESIDENZA DEL PRESIDENTE **SANDRO GOZI**

INDICE

PRESIDENZA DEL PRESIDENTE SANDRO GOZI

La seduta comincia alle 14,35.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità del lavori della seduta odierna sarà assicurata anche attraverso impianti audiovisivi a circuito chiuso.

(Così rimane stabilito).

Audizione del professor Francesco Pizzetti, presidente dell'Autorità garante per la protezione dei dati personali.

PRESIDENTE. L'ordine del giorno reca, ai sensi dell'articolo 143, comma 2, del regolamento della Camera, l'audizione del professor Francesco Pizzetti, presidente dell'Autorità garante per la protezione dei dati personali, accompagnato dal dottor Giovanni Buttarelli, segretario generale.

Desidero ringraziare a nome del Comitato il professor Francesco Pizzetti per la sua presenza, che ritengo di grandissima rilevanza per la nostra attività. È mia ferma convinzione che debba esservi un rapporto forte e stretto, a livello politico, tra le attività che noi svolgiamo, soprattutto per quanto riguarda le competenze in area Schengen, e le attività che, in ambito italo-europeo, ricadono sotto la vostra competenza.

L'audizione di oggi, a nostro avviso, rappresenta il primo momento di un rapporto di cooperazione. Proprio per questo sarebbe opportuno che lei oggi ci delineasse un quadro generale non solo delle attività dell'Autorità garante che lei presiede, ma anche di come è nato e di come si è sviluppato il sistema di dati personali, di sicurezza, di garanzia delle libertà personali e di controllo per le esigenze di sicurezza, che rientra nell'ambito delle vostre competenze.

Credo che sarà anche molto utile sapere come il sistema si è evoluto, a livello europeo e italiano, dal 2001, ossia dal momento in cui le esigenze di sicurezza si sono fatte particolarmente rilevanti. È interessante conoscere come stiate procedendo nella ricerca di un nuovo equilibrio tra esigenze di sicurezza dei dati ed esigenze di sicurezza nella lotta a tutte le attività criminali – a cominciare dalle attività terroristiche – organizzate in Europa.

Vorremmo poi sapere quali sono, anche per voi, le differenze esistenti tra le attività comunitarie in senso classico e le loro ricadute nel sistema italiano, e le attività cosiddette di « terzo pilastro », cioè tutto ciò che attiene alla stretta cooperazione giudiziaria e di polizia.

Nel dettaglio, vorremmo conoscere le evoluzioni del sistema informativo Schengen, SIS-I e SIS-II. Su questo, come lei sa, abbiamo già sentito, in un'ottima audizione, il vicepresidente Frattini, ma sarebbe molto importante per noi avere una valutazione dal punto di vista dell'Autorità garante.

Un altro aspetto molto rilevante, per quel che riguarda la cooperazione delle polizie in Europa, è la possibilità di avere accesso ai dati personali di altre autorità e di altri Stati membri da parte della polizia di uno Stato, ovverosia il principio di disponibilità. Vorrei da lei una valutazione sulle reali possibilità di avere un forte principio di disponibilità, per accom-

pagnare ad una libera circolazione dei cittadini nello spazio Schengen un forte contrasto alla libera circolazione dei criminali.

Sempre per quanto riguarda le recenti evoluzioni, vorrei che lei evocasse il trattato di Prüm, di cui l'Italia non è ancora parte, ma rispetto al quale personalmente ritengo che il Governo dovrebbe attivarsi per diventarne parte pienamente contraente. Le chiedo quali sono le conseguenze per quanto riguarda i dati personali e, soprattutto, per quanto riguarda l'esigenza specifica relativa alla banca dati del DNA, nonché le possibilità di un inserimento di questo trattato internazionale in senso classico all'interno di un sistema giuridico più compiuto come quello comunitario.

L'ultimo punto riguarda lo sviluppo della cooperazione con gli Stati Uniti d'America, soprattutto in merito ai dati personali legati ai viaggi aerei. Mi riferisco alla questione relativa alla cooperazione tra l'Unione europea e gli Stati Uniti in materia di controllo dei passeggeri, nonché alla possibilità e ai rischi che derivano, a mio parere, dai recenti sviluppi in materia di controllo sulle transazioni finanziarie che riguardano i passeggeri dell'Unione europea che si recano nello spazio americano.

Questi, come lei capisce, sono grandi capitoli che magari potremo approfondire nel corso dei nostri lavori, ma sui quali oggi sarebbe utile che lei delineasse una panoramica.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Grazie, presidente. Ringrazio gli onorevoli deputati ed i senatori per la loro presenza e la Commissione per averci invitato. Il mio ringraziamento è particolarmente caloroso, perché, dopo una prima fase nella quale l'Autorità era stata presente con più audizioni, nelle persone del presidente, o del collega De Siervo, nell'ultima legislatura la Commissione si è avvalsa dell'apporto utilissimo, certamente prezioso e tecnicamente preparato, del segretario generale. Ad ogni modo, credo che sia una circostanza molto importante – ve ne siamo grati anche a nome del collegio – che abbiate chiesto la presenza del presidente dell'Autorità. Dico questo perché si tratta di una tematica rispetto alla quale il dato politico ha una rilevanza assoluta e crescente. Per dato politico intendo il valore più alto della politica, ossia ciò che tocca da vicino la vita quotidiana e la libertà reale, concreta e specifica di ciascuno di noi e di tutte le nostre comunità.

Come Collegio, consideriamo la vostra Commissione bicamerale uno dei nostri interlocutori naturali e istituzionali. La nostra idea è che, pur gelosi della nostra caratteristica di Autorità indipendente, abbiamo un dovere di rapporto costante con la comunità nazionale, anche perché essere Autorità indipendente non può significare operare nel vuoto di una « ipertecnocrazia ». E il rapporto con la comunità nazionale passa, innanzitutto e prima di tutto, per il Parlamento. Tra l'altro, e non a caso, caratteristica propria della nostra Autorità è di essere composta da quattro membri, tutti eletti dal Parlamento. Quindi, il nostro rapporto è con il Parlamento, ed è un rapporto preziosissimo, senza il quale la nostra attività, inevitabilmente, non può che soffrire.

Nell'ambito del Parlamento, credo che, al di là della relazione annuale, il nostro rapporto istituzionale debba intercorrere – tenendo conto delle varie attività e delle missioni che ci sono state attribuite dalle norme europee e dalla legge nazionale – con la Commissione giustizia, come tradizionalmente è sempre avvenuto (tra l'altro, siamo un'Autorità che tutela i diritti fondamentali e per i cui provvedimenti, caso unico nel sistema italiano, si può ricorrere al giudice ordinario); con la Commissione affari costituzionali, perché la pluralità delle attività di cui ci dobbiamo occupare coinvolge complessivamente i più diversi aspetti della collettività nazionale; con la Commissione che si occupa – e dirò poi perché nel corso di questa esposizione – delle strutture di sicurezza, perché tra gli altri compiti che ci spettano vi è quello di garantire i cittadini rispetto al corretto

funzionamento, mantenimento e utilizzazione delle banche dati (fra gli altri, dei servizi di sicurezza dello Stato); infine – correttamente avrei dovuto menzionare questa voce per prima – con voi, con la vostra Commissione, poiché il nostro radicamento è nel contesto europeo.

In quest'ambito, la nostra collocazione nello spazio di sicurezza, libertà e giustizia – oggi definita anche dagli atti dell'Unione europea, ma in realtà sempre esistente nella costruzione della comunità europea – è per noi una parte assolutamente rilevante.

Inevitabilmente ci troviamo ad operare nel vuoto, senza il vostro aiuto e il vostro costante supporto, senza un'istituzione nazionale con la quale poter colloquiare nel rispetto più rigoroso dei diversi ruoli istituzionali. Aggiungo a tal proposito – e poi passo agli aspetti più sostanziali – che è particolarmente importante per il Parlamento che questo rapporto si concretizzi attraverso il ruolo della vostra Commissione bicamerale. Infatti man mano che il processo di integrazione europea procede, in mancanza della ratifica del Trattato costituente per l'Unione, i Parlamenti nazionali rischiano sempre più di essere marginalizzati, spostandosi il potere decisionale alle istituzioni europee. Ovviamente tutti siamo lieti che in larga misura si spostino i procedimenti di codecisione nel rapporto fra Consiglio, Commissione e Parlamento ma, molte volte, proprio in questi settori, lo stesso Parlamento europeo è interpellato solo nella procedura di consultazione più che in quella di codecisione. Quindi il ruolo dei Parlamenti nazionali – prezioso comunque, perché in ogni caso le comunità nazionali si esprimono attraverso il loro Parlamento – in questo contesto è particolarmente importante.

Oggi cercherò di essere molto generico – lo anticipo, e mi scuserete –, perché mi sembra più importante dare un quadro complessivo del contesto nel quale ci muoviamo come Autorità, e nel quale siamo (noi e voi) nell'attuale fase storica europea.

Mi avete posto alcune specifiche domande, alle quali cercherò ovviamente di dare puntale risposta. Lo avete fatto attraverso l'introduzione del presidente, che ringrazio di nuovo, anche per la specificità dei quesiti, e attraverso i colloqui intercorsi fra le nostre strutture tecniche.

In particolare, mi avete chiesto chiarimenti sul SIS-II, il PNR e la SWIFT e notizie sul trattato di Prüm, per sapere a che punto è la situazione rispetto a queste tematiche. A tutti questi quesiti cercherò di dare puntuale risposta, ma prima di tutto vorrei riprendere il filo di un'affermazione che ho già fatto.

Noi, come Autorità indipendenti, in Europa – e in particolare in Italia – nasciamo e viviamo con una sorta di doppia missione. Da un lato, nasciamo e viviamo dentro quello che potremmo chiamare « primo pilastro », ossia come una struttura europea e nazionale essenziale per evitare che la protezione dei dati, attuata con legislazioni nazionali difformi, crei una sorta di barriera occulta alla libertà di circolazione dei beni, delle persone e delle cose e, quindi, mini le quattro libertà fondamentali del primo pilastro. Dall'altro, nasciamo tutte – ma quella italiana in particolare – dentro un contesto essenziale per garantire che l'integrazione tra i vari paesi e le diverse comunità, necessaria per dare piena attuazione proprio alle libertà fondamentali del primo pilastro e, oggi, sempre più necessaria per creare lo spazio comune di sicurezza, libertà e giustizia, non si trasformi in un accrescersi della pericolosità per le nostre comunità.

Questo, ovviamente, implica un rafforzamento delle nostre strutture di sicurezza e la messa in circolazione dei dati utilizzati, classificati e raccolti a fini di sicurezza (qui uso il termine « sicurezza » nell'accezione più generale). Questa attività è indispensabile per evitare che l'Europa trasformi la libertà di circolazione in libertà di criminalità. D'altra parte, perché si mantengano saldi i principi della nostra democrazia e la tutela dei diritti fondamentali dei cittadini, questa attività consente alle nostre strutture di sicurezza, appartenenti a paesi diversi, provenienti da tradizioni giuridiche e culturali diffe-

renti, di poter collaborare con una certa fiducia reciproca, nella convinzione che ci sono soggetti che tutelano i dati raccolti e l'uso delle banche dati secondo regole comuni.

Detto in modo più esplicito, questa attività nasce per garantire che i dati siano raccolti per proteggere i cittadini europei e non per essere usati contro di loro dalle strutture di sicurezza, che ovviamente sono indispensabili per garantire, appunto, la nostra sicurezza; nasce, altresì, e si sviluppa per garantire che le diverse strutture di sicurezza, con tradizioni differenti fra di loro, possano collaborare con una ragionevole fiducia, basandosi sul fatto che i dati che ciascuna struttura raccoglie e che, attraverso le comuni banche dati europee, mette in circolazione in tutta l'Unione europea, siano verificati e credibili, che possano essere utilizzati dalle diverse strutture di sicurezza degli altri paesi con adeguata e sufficiente fiducia, in ordine alle modalità della loro raccolta, della loro tenuta e messa in comune.

Da questo punto di vista, per la parte che ci sta interessando oggi, la nostra Autorità ha un doppio ruolo, particolarmente importante: quello di garantire ai nostri cittadini che i dati raccolti siano usati per loro e non contro di loro, e quello di garantire alle nostre strutture di sicurezza nazionale, che devono lavorare in comune, la ragionevole affidabilità che le diverse strutture di sicurezza seguano regole condivise e uniformi, che operino secondo modalità verificate e, in qualche misura, accertate da soggetti terzi.

Quello che capita quotidianamente, in ordine all'uso di dati che provengono da tradizioni diverse, ci dice quanto questo aspetto sia importante. Come ho detto, come Autorità italiana nasciamo geneticamente con questo duplice aspetto. Non dobbiamo mai dimenticare che l'Autorità italiana viene istituita nel 1996 ed entra in funzione nel 1997, come ultimo passo essenziale perché l'Italia possa entrare a pieno titolo nello spazio comune Schengen. Tale spazio è, in quel momento, una cooperazione rafforzata – istituita fin dal 1985, poi realizzata con una Convenzione del 1990 fra Benelux, Francia e Germania – finalizzata a liberalizzare la circolazione fra le frontiere e ad anticipare la libera circolazione delle persone. Questo farà sì che il trattato di Amsterdam del 1999 comunitarizzi quella parte di Schengen che serve a liberalizzare le frontiere.

Se pensate che noi abbiamo ratificato Schengen già nel 1993 – ma solo nel 1997 siamo entrati nell'area Schengen – e che per poter entrare in area Schengen è stata necessaria l'approvazione della legge istitutiva della nostra Autorità, che costituisce la garanzia complessiva che il sistema Schengen richiede, vi renderete conto di come noi nasciamo dentro la duplicità di aspetti che ho richiamato.

Schengen nasce inizialmente come un accordo tra cinque paesi, poi diventa una cooperazione rafforzata e viene successivamente integrata, con il trattato di Amsterdam del 1999, nell'Unione europea. Dall'accordo del 1985 alla convenzione del 1990, e fino al 1999 – come vedete, l'Europa è sempre lenta nel suo processo –, l'Italia arriva *in articulo mortis*, ossia l'anno prima che si arrivi alla comunitarizzazione. Non credo che si possa dubitare che proprio questa è la spinta che porta finalmente ad attuare la direttiva 95/46/CEE, che già l'Unione europea si era data nel primo pilastro, per la protezione dati e per mettere l'Italia – anche per quanto riguarda la protezione dati sulla libera circolazione delle merci –, con l'istituzione dell'Autorità garante, in regola col resto dell'Unione europea.

Oggi naturalmente non parleremo di primo pilastro, ma essenzialmente di terzo pilastro; non parleremo dunque degli aspetti più strettamente legati alla direttiva europea 95/46, che riguarda la protezione dei dati dentro quella che ancora, purtroppo, dobbiamo chiamare CEE. Come ho detto, oggi parleremo soprattutto di terzo pilastro.

Il sistema Schengen, dunque, chiarisce fin dall'inizio questa ambivalenza e duplicità di ruolo delle Autorità, che a livello europeo è chiarissima. In assenza della ratifica del trattato costituente dell'Unione europea, siamo costretti purtroppo a par-

lare di primo e di terzo pilastro. Quando ci muoviamo a livello di Unione europea è facile cogliere, anche attraverso differenti aspetti procedurali nel processo decisionale, se si è dentro il primo o il terzo pilastro; in verità, sta diventando sempre meno facile, ma è ancora possibile.

Come dicevo, la duplicità di ruolo si riflette anche all'interno della nostra attività nazionale e, al riguardo, vorrei toccare subito un punto che, se credete, riprenderemo in seguito. Anche all'interno del compito che abbiamo come Autorità nazionale, indipendentemente dal nostro rapporto con il contesto europeo, in realtà noi ci muoviamo su un doppio binario. Uno dei principi fondamentali del sistema di protezione dati, tradotto in diritto fondamentale dei cittadini, è che il cittadino abbia il diritto di sapere se qualcuno possiede dati che lo riguardano – quello che chiamiamo il diritto di accesso – e di chiedere la rettifica dei dati che lo riguardano, se sbagliati.

Questo diritto è affievolito nei settori che fanno riferimento alla giustizia, alla polizia e alla sicurezza. In questo contesto si ripete, a livello nazionale, qualcosa di simile a quello che avviene a livello europeo. Tuttavia il nostro ruolo di Autorità, che è fortissimo quando dobbiamo garantire al cittadino che il suo diritto di accesso sia effettivo (il cittadino ricorre all'Autorità che, con un provvedimento che è penalmente sanzionato se non eseguito, intima di dare accesso al cittadino istante), non è meno importante nel settore della sicurezza, della giustizia e della polizia. Rispetto a questi settori, nei quali il cittadino ha un diritto di accesso affievolito, sorge infatti il nostro dovere – disciplinato nel codice – di svolgere una specifica attività di vigilanza, anche attraverso attività ispettive e di controllo, su come sono tenute e organizzate le banche dati.

In questi stessi settori – in particolare in quello della sicurezza e della polizia, perché in quello della giustizia c'è il normale ricorso ai mezzi di interpello del giudice, che i nostri codici di procedura prevedono – quel diritto di accesso che il cittadino singolarmente non vede tutelato, può essere rafforzato rivolgendosi a noi. Sostituendo il cittadino, infatti, noi andiamo a verificare se la tenuta dei dati che lo riguardano avviene in modo corretto e legittimo o meno.

Questo ruolo della Autorità – è un primo aspetto che vorrei riuscire ad esprimere con chiarezza – trova pienezza proprio nella sua duplice natura. Noi non siamo solo Autorità chiamate a tutelare il cittadino individualmente, quando fa ricorso a noi rispetto al rifiuto che gli sia stato opposto di fargli conoscere i dati che lo riguardano; in certi settori, sia che ci muoviamo a livello europeo, sia che ci muoviamo a livello nazionale, noi abbiamo un compito di vigilanza generale, attraverso attività di carattere ispettivo, di carattere collaborativo, attraverso prescrizioni, sulla tenuta delle grandi banche dati del sistema italiano ed europeo.

Questo è il motivo per cui, nell'ambito italiano, abbiamo avviato un'attività ispettiva sul CED del Dipartimento della pubblica sicurezza, che si sta svolgendo da due anni e che sta dando una serie di risultati assai utili. Questo è il motivo – scusate se lo ripeto anche in questa sede, ma siete parlamentari a pieno titolo – per cui non mi stancherò mai di chiedere che i Ministeri dell'interno e della giustizia approvino i famosi decreti nei quali devono indicare, a norma del codice le banche dati di giustizia e di sicurezza di cui si avvalgono per garantire i compiti istituzionali delle amministrazioni di loro specifica competenza.

Tornando a noi, abbiamo detto che « nasciamo » con Schengen. Schengen, come ho detto, è fin dall'inizio un insieme di regole o forme di accordi che nel tempo cessano di essere puramente internazionali e diventano in qualche modo riconducibili all'Unione, in particolare nel cosiddetto terzo pilastro.

Tuttavia, per rispondere alla vostra domanda, non possiamo limitarci a questa parte della vicenda, ma dobbiamo fare un salto ulteriore. Siamo arrivati finora al 1999, alla ricezione dentro l'*acquis communautaire* di Schengen; ma il 1999, come

sappiamo, è un anno che ha la particolarità di venire a ridosso del 2001, cioè a ridosso di una situazione che vedrà una forte accelerazione dei problemi relativi alla sicurezza. Non è casuale che, già nel dicembre 2001, un Consiglio europeo – che segue quello di Tampere, ma sembra essere passato un decennio, anziché un anno solo – decide di dar vita a quello che oggi chiamiamo il SIS-II.

In sostanza, sebbene la banca dati Schengen (SIS, *Schengen Information System)* contenga una serie di dati utili a garantire la libera circolazione fra le frontiere – i dati che si pensavano utili nel 1985, e che si sono ritenuti sufficienti nel 1999 –, improvvisamente nel 2001 si decide strategicamente di trasformarla in una banca dati completamente diversa.

Quando parliamo di SIS-II, parliamo di una scelta che venne fatta nel 2001, e che – pensate a come sono lenti i tempi europei – solo a dicembre del 2006 si trasforma in atti regolamentari pubblicati sulla *Gazzetta Ufficiale*. Poiché sono tre gli atti che istituiscono il SIS-II, siamo ancora in attesa della pubblicazione sulla *Gazzetta* del terzo atto, una decisione di terzo pilastro che completi la base normativa di questa nuova realizzazione del sistema di sicurezza Schengen.

Nel 2001 si comincia a pensare a questa accentuazione del sistema della banca dati Schengen a causa di una esigenza accresciuta di sicurezza. Ebbene, siamo al 2007 e non abbiamo ancora completato il procedimento giuridico-formale di realizzazione di quella scelta strategica del 2001.

Quando mi chiedete cos'è il SIS-II, vi rispondo che è un sostanziale mutamento della banca dati Schengen, nota da tempo come SIS, che corrisponde ad una scelta strategica che risale ormai a cinque anni fa e che troverà attuazione, se tutto andrà bene, nel 2008. Uno strumento, quindi, che ha tempi necessariamente molto lunghi, le cui caratteristiche tecniche sono in sostanza di duplice natura: immettere nella banca dati un numero di informazioni molto più rilevante di quanto non fosse nel SIS di prima generazione; creare non più, come il SIS di prima generazione, una rete fra le banche dati SIS dei vari paesi, ma una vera (fisica) banca dati nella quale affluiscono i dati forniti dalle banche dati SIS nazionali.

In sostanza, il sistema SIS-II ha il duplice compito di incrementare significativamente il numero di informazioni contenute e di creare un luogo fisico nel quale questi dati sono raccolti e gestiti. Questo luogo fisico e questo nuovo sistema centralizzato devono essere messi sotto la responsabilità della Commissione europea.

Terza importante innovazione del SIS-II è che si decide strategicamente che a questa nuova grande banca dati – molto più grande di quanto non sia il SIS attualmente in vigore – potranno accedere una serie di strutture operanti nel settore di sicurezza, libertà e giustizia che, ad oggi, hanno invece o la necessità di costituire proprie banche dati, o l'impossibilità di accedere ai dati contenuti nel sistema SIS. Parlo di Europol, delle strutture di controllo alle frontiere, di Eurojust; insomma, parlo di una serie di strutture di sicurezza che si sono accresciute in questi anni e fanno parte del programma di integrazione complessivo del sistema europeo in corso di sviluppo.

Quando parliamo del SIS-II, parliamo di una cosa molto seria e importante, che cambierà significativamente il sistema di informazioni a disposizione delle varie strutture operanti nello spazio di sicurezza, libertà e giustizia. Uno strumento che costituirà un'enorme nuova banca dati, che ricadrà sotto la competenza e la vigilanza della Commissione, che per la tutela della correttezza della gestione della banca dati vedrà la competenza dell'EDPS, cioè il Garante europeo della protezione dei dati e che vedrà le Autorità nazionali non diminuire i loro ruoli e i loro compiti, ma piuttosto aumentarli. Sarà, infatti, sempre più importante vigilare, all'interno delle frontiere nazionali, in primo luogo che i dati immessi in questo sistema siano corretti ed in secondo luogo che i dati tratti da questo sistema siano utilizzati correttamente. È ovvio che più i dati aumentano, più la pericolosità di una loro

immissione o utilizzazione in violazione delle norme che disciplinano il sistema potrà determinare danni e pericoli per i cittadini.

Quando parliamo di SIS-II, parliamo di un sistema ancora non operativo, la cui operatività, come ho detto, è prevista – proprio dal Consiglio europeo del 4 e 5 dicembre che si è appena svolto –, se tutto andrà bene, nel 2008.

Quando nel 2001 – scusate se la mia spiegazione è articolata ma è la complessità della storia europea che mi spinge a questo – si decide di passare dal sistema SIS al sistema SIS-II, lo si fa avendo come obiettivo, innanzitutto, quello di implementare la sicurezza (mi assumo la responsabilità di quanto affermo, sapendo che probabilmente tecnici illustri come Buttarelli accoglieranno con gelo queste affermazioni). Lo si fa, però, sostenendo che, in ogni caso, è necessario passare dal SIS, quello pensato nel 1990, al SIS-II, ossia alla nuova banca dati europea (questa volta davvero europea), perché l'ingresso di dieci nuovi paesi – oggi già diventati dodici – all'interno delle frontiere dell'Unione europea obbliga ad un mutamento del sistema di conservazione dei dati. Nel 2001 si afferma, dunque, che quando l'Europa sarà diventata a 25 (oggi a 27) non sarà più possibile utilizzare il sistema SIS.

A questo punto, potete chiedere giustamente come si debba agire, dal momento che il SIS-II fino al 2008 non entrerà in funzione, se tutto andrà bene. Questo è uno dei problemi che il Consiglio europeo di un mese fa ha dovuto affrontare. Si sta cercando, sotto la spinta dell'autorità di controllo – oggi guidata da un presidente portoghese, ma in passato presieduta anche dal nostro segretario generale – e soprattutto del Governo portoghese, di adottare immediate misure tecniche che consentano comunque di estendere il SIS oggi vigente, in attesa che diventi operativo il SIS-II, anche ai paesi nuovi membri.

Sulla possibilità di realizzare questo obiettivo non siamo in grado ad oggi di darvi rassicurazioni. È ovvio che il rallentamento determinerà qualche complessità, dal momento che i nuovi paesi entrati, avendo noi chiesto loro di avere i requisiti Schengen per entrare nell'Unione, si aspettano di avere anche i vantaggi Schengen.

Di conseguenza, quanto più ritardiamo la libera mobilità fra le frontiere dei nuovi paesi entrati, che hanno già pagato i costi di Schengen – ad esempio, tutti hanno un'autorità di protezione e garante dei dati –, tanto più il problema politico cresce. Per questa ragione il Consiglio europeo del 4 e 5 dicembre ha deliberato di cercare una soluzione affinché, in attesa del SIS-II, comunque si onori il patto assunto con i paesi nuovi entrati.

Finora ho parlato di SIS-II in divenire e di SIS attuale, ma l'ho fatto per semplificare. Devo dirvi, infatti, che già oggi il SIS del 1990 è diventato SIS+1, come peraltro compare sui documenti. Nella documentazione del Consiglio europeo di dicembre, troverete la proposta portoghese del SIS+1 *for all*, per tutti.

Cosa significa SIS+1 ? Nel 2004, sotto Presidenza spagnola, non a caso dopo l'attentato di Madrid, la Spagna ottenne – con una propria proposta, poi diventata regolamento – di implementare una serie di dati da immettere nel vecchio SIS. Il SIS, dunque, già dal 2004 non è più quello originario del 1990, ma è un SIS cresciuto, più panciuto, che contiene dati relativi anche a veicoli e una serie di elementi che il primo SIS non prevedeva.

Per riassumere questa vicenda e passare ad altri profili, l'antico sistema Schengen è stato pensato e creato prima fra cinque paesi, poi esteso a quasi tutti i paesi. Come sapete, fuori dal sistema Schengen ci sono oggi la Gran Bretagna e l'Irlanda, mentre al suo interno vi sono la Norvegia e la Svizzera, che sta entrando ormai a pieno titolo: Schengen è quindi un sistema a geometria variabile. È un sistema pensato nel 1990, dichiarato in via di obsolescenza nel 2001, realizzato come base giuridica nel 2007, la cui entrata a regime è prevista nel 2008. Dal 2004 il sistema è stato cambiato in SIS+1 e contiene maggiori dati, proprio per aumentare

la soglia di sicurezza. Questo ci dice come il processo di cui ci stiamo occupando sia complesso.

Passiamo ad altri profili, che sento il dovere di segnalarvi. Al di là del SIS, mi avete posto altre domande. Mi avete chiesto informazioni sul trattato di Prüm e sulle sue implicazioni. Consentitemi, prima di arrivare al trattato di Prüm, di richiamarvi due profili, che ho già toccato, ma che voglio sottolineare. La necessità di accrescere le misure di sicurezza non ha solo nel SIS e nel suo progetto l'unico fondamento. Nel corso di questi anni, in particolare a partire dal 2001, sono aumentati i sistemi di raccolta dati da usare a fini di sicurezza o della messa in comune di dati. Possiamo parlare di una serie di processi; tra i più significativi vi è il sistema VIS, finalizzato a mettere in comune tutti i dati in possesso dei paesi dell'Unione relativamente alla richiesta di visti di entrata nell'Unione (un sistema che non è ancora realizzato), ma potremmo parlare anche di altri profili.

Nell'ambito di questo processo, in corso dal 2001 in poi, devo riferirvi di un altro profilo di particolare importanza. Mi riferisco alla decisione che la Spagna è riuscita ad imporre nel 2004, facendo approvare una direttiva, nota in gergo come direttiva APIS (direttiva 2004/82/CE), compresa nella legge comunitaria per il 2005 e che dovrebbe essere in corso di recepimento da parte del Consiglio dei ministri italiano nei prossimi mesi.

L'APIS è l'obbligo – rivolto alle compagnie che operano dai paesi esterni all'Unione europea e portano viaggiatori dentro le frontiere dell'Unione – di comunicare in anticipo rispetto alla partenza dei voli, la lista dei passeggeri e i dati tradizionalmente in possesso delle compagnie aeree sui passeggeri (nome, cognome, dati che si consegnano al *check-in*).

Questo ci dice come anche l'Europa si ponga il problema di implementare la raccolta dei dati, da poter utilizzare. Dentro questo contesto, al quale ho accennato – lasciando da parte Europol, Eurojust, Eurodac ed altre strutture di cui, se riterrete, potremo occuparci –, si colloca anche il Trattato di Prüm. È un trattato molto recente, derivante da un accordo stipulato tra Germania, Francia ed altri paesi (tra cui, se non sbaglio, anche la Spagna) il 27 maggio 2005, che ha dichiaratamente – nel suo stesso titolo – l'obiettivo di implementare le misure antiterrorismo. Il trattato è finalizzato alla messa in comune, da parte dei paesi contraenti, di una nuova serie di dati che questi paesi si impegnano a raccogliere e mettere reciprocamente a disposizione.

Come capite, siamo dentro un contesto singolarmente omogeneo ed articolato. Da una parte il SIS-II implementa la raccolta dei dati e l'accesso agli stessi; dall'altra, in attesa che il SIS-II si realizzi, si attua il SIS+1 e poi la direttiva APIS.

Tornando a Prüm, la specificità più significativa del trattato è che esso prevede la raccolta e la messa a disposizione di dati biometrici identificativi e del DNA della persona, non come campione fisico, ma come tracciato.

Al trattato di Prüm l'Italia ha già dichiarato di voler aderire – il nostro ministro dell'interno ha dichiarato ufficialmente la volontà di adesione dell'Italia – e aderiranno, nel corso dei prossimi mesi, altri 4-5 paesi. Proprio in queste ore, in considerazione del fatto che entro pochi mesi il trattato avrà un numero di paesi contraenti sufficiente per delineare una cooperazione rafforzata, è stato proposto dalla Presidenza tedesca che il trattato di Prüm (come accadde a suo tempo a Schengen) sia accolto all'interno della legislazione dell'Unione europea, ovviamente dapprima come cooperazione rafforzata.

L'eventuale ingresso – uso il termine « eventuale » quasi eufemisticamente, poiché tutte le dichiarazioni politiche del nostro Governo in questo momento sono inequivoche in questo senso – dell'Italia dentro il trattato di Prüm, tanto più se esso è destinato a diventare una cooperazione rafforzata, porrà all'Italia il tema della realizzazione ufficiale di una banca dati DNA, a fini di polizia e di sicurezza, della quale oggi nel nostro ordinamento non c'è base giuridica, e porrà ovviamente nuovi, importanti e complessi compiti di

controllo di questi dati, sia nella fase della loro raccolta all'interno del paese, sia in quella della loro utilizzazione, sia nella definizione di chi ha diritto di accedervi, sia nella messa a disposizione fra le diverse strutture di polizia e di sicurezza aderenti alla cooperazione rafforzata.

Come dicevo all'inizio, siamo in un processo storico estremamente importante, complesso, articolatissimo, attorno al quale si stanno disegnando le caratteristiche dell'Unione europea (vorrei dire come essa è già oggi, più ancora che come essa sta per diventare) e siamo obbligati a seguirlo con molta attenzione.

Inoltre, mi avete chiesto notizie su PNR e SWIFT. Qui siamo dentro una tematica differente, quella dei rapporti fra Unione europea e Stati Uniti. Una tematica che, per quanto riguarda la protezione dati, è sempre stata complessa. Come sapete, gli Stati Uniti hanno una visione della protezione dati del tutto diversa da quella propria dell'Unione europea. Noi consideriamo la protezione dei dati un diritto fondamentale del cittadino, un diritto che secondo la tradizione europea lo Stato deve garantire; gli Stati Uniti considerano i dati dei cittadini un bene la cui eventuale utilizzazione in modo illecito dà diritto al cittadino di ricorrere al giudice. Nel sistema e nella mentalità americana, i dati sono disciplinati dalle normali regole civilistiche che disciplinano i rapporti tra i cittadini. Non che non sia un diritto fondamentale, ma non c'è la pretesa che sia lo Stato a proteggerlo.

Diversa è la posizione europea, chiarita nella direttiva 95/46/CE ma prima ancora nella Carta europea dei diritti dell'uomo, ribadita poi nella Carta dei diritti fondamentali dell'Unione europea e specificata in modo ancora più chiaro nel Trattato costituente europeo. Il filo rosso che lega questa posizione è che in Europa i cittadini hanno il diritto che lo Stato protegga i loro dati. È un diritto fondamentale che i cittadini possono vantare rispetto alla loro comunità, quindi non è affidato soltanto al rapporto contenzioso *one to one* davanti a un giudice civile.

Il rapporto tra Stati Uniti e Unione europea è molto complesso su questa tematica, perché noi – può sembrare strano ma è così – consideriamo inadeguata la protezione dei dati personali assicurata nel territorio americano. Il sistema pubblico americano non si fa carico di quel tipo di protezione dati che noi, invece, assicuriamo ai nostri cittadini dentro il territorio europeo.

A questo, dopo l'11 settembre, si è aggiunto un altro e diverso profilo, molto più complesso, perché le autorità americane – in modo crescente – pretendono, chiedono e ottengono, di conoscere e utilizzare i dati dei cittadini europei, a fini di sicurezza e di difesa del territorio americano.

Si passa, quindi, nel contenzioso (lo dico in forma atecnica) fra Stati Uniti ed Europa, da una difficoltà di rapporti di « primo pilastro » – per usare questa terminologia un po' convenzionale – ad una, più complessa e più delicata da gestire, difficoltà di rapporti di « terzo pilastro », sul sistema della sicurezza.

Il PNR è una pretesa americana, che l'Unione europea è stata forzata ad accogliere qualche anno fa e poi forzata a rinnovare, sia pure transitoriamente, a settembre, e che dovrà essere rinegoziata nel corso del 2007. Secondo tale pretesa, le autorità americane possono entrare direttamente nelle banche dati delle compagnie aeree che gestiscono voli da/per gli Stati Uniti o che ne sorvolano il territorio, al fine di acquisire i dati dei passeggeri.

Ovviamente gli americani chiedono l'accesso a questi dati indiscriminatamente, ma noi siamo particolarmente sensibili – per usare un eufemismo – al fatto di dover accettare che le autorità americane non chiedano, ma acquisiscano direttamente questi dati, anche quando riguardano i cittadini europei, e comunque quando riguardano compagnie che operano in partenza dal territorio europeo.

È un problema complesso, perché è evidente che la lotta al terrorismo e la sicurezza sono obiettivi comuni. È evidente che non ci può essere antagonismo su un problema fondamentale come la

garanzia della sicurezza dei cittadini, ma è anche evidente che c'è una difficoltà di rapporto con le autorità americane, ed occorre trovare un sistema accettabile anche per noi. Quello attuale non è accettabile perché le autorità americane accedono direttamente ai dati e non è possibile a nessuno, in Europa, valutare la fondatezza delle richieste. Non è accettabile inoltre perché i dati a cui gli americani possono accedere sono numerosissimi (più di 34 tipologie). Può essere che ci siano casi o situazioni, personali o temporali, nelle quali tutti questi dati sono necessari, ma è difficile pensare che questi dati possano essere chiesti in qualunque situazione, per qualunque tipo di cittadino, quale che sia la situazione oggettiva di pericolo. In terzo luogo, non è accettabile perché noi, come autorità europee, non abbiamo alcuna possibilità di verificare o controllare come i dati sono utilizzati dalle autorità americane e viene quindi meno proprio il cuore del nostro ruolo. Infatti anche quando il cittadino ha una garanzia affievolita perché, per ragioni di sicurezza o di giustizia, i suoi dati sono utilizzati senza che egli debba dare il consenso o possa conoscere esattamente quali di essi sono utilizzati, devono esserci autorità che lo garantiscano circa il modo con cui le banche dati sono usate, la legittimità della raccolta e dell'utilizzazione. Oggi, rispetto agli Stati Uniti non possiamo fare nulla di tutto questo.

L'altro fronte che si è aperto attualmente è il caso SWIFT, non meno delicato. La SWIFT è una cooperativa di istituti finanziari – sono più di 7.800 gli istituti finanziari che vi aderiscono – che ha il compito fondamentale quanto specifico di mantenere traccia delle transazioni finanziarie che avvengono in giro per il mondo prevalentemente attraverso bonifici. Si tratta di una struttura essenziale, in quanto struttura di garanzia dell'interscambio finanziario. La società, che ha sede in Belgio, ha da tempo istituito un archivio di sicurezza, chiamato *Mirror*, negli Stati Uniti.

È una regola di qualunque gestione di banche dati che ognuna di esse abbia sempre un archivio di sicurezza posto in un'altra parte del territorio. La scelta della SWIFT, nel 1997, è stata ragionevole: avendo l'archivio principale in Belgio, ha deciso di fare l'archivio di sicurezza negli Stati Uniti, in un altro continente. Sennonché, da alcuni anni, le autorità americane, utilizzando un potere vincolante proprio del diritto americano e prendendo atto che questo archivio di sicurezza è sul territorio americano, hanno obbligato la SWIFT a creare una sorta di archivio separato, nel quale la società è tenuta – per ordine vincolante dell'autorità, secondo il diritto americano – a inserire i dati di transazioni finanziarie che abbiano le specifiche caratteristiche richieste dalle autorità americane. L'accesso a questo archivio separato da parte delle autorità americane è rimesso totalmente alle scelte delle autorità stesse, senza alcuna possibilità di controllo, né di verifica.

È ovvio che questo ci pone due tipi di problemi. Il primo è un problema di carattere generale, che riguarda il trasferimento dei dati dal mondo europeo a quello americano, tenendo conto che noi riteniamo – a torto o a ragione, ma non è questa la discussione che dobbiamo aprire – che la protezione dati negli Stati Uniti sia meno efficace di quanto non lo sia in Europa. Il secondo problema, più delicato, nasce dal fatto che una quota parte di questi dati sul territorio americano è conoscibile dalle autorità americane per ragioni di sicurezza certamente, ma comunque senza che a noi sia data alcuna possibilità di verificare come, quando, secondo quali modalità, per quali finalità e con quali garanzie rispetto ai soggetti titolari delle transazioni finanziarie.

Comprenderete che si tratta di una problematica delicatissima, anche da un punto di vista giuridico perché incrocia problemi di primo e di terzo pilastro, problemi di sicurezza e problemi di tutela dei diritti fondamentali; e che fa tremare avendo a mente che oggi sappiamo solo di due problematiche relative all'uso dei dati fra l'uno e l'altro sistema, ma le ragioni che spingono all'utilizzazione dei dati per motivi di sicurezza sono tali, e così mol-

teplici, che, negli stessi Stati Uniti, come avete letto sui giornali dell'altro ieri, si continuano a individuare nuovi casi in cui le autorità americane usano i dati dei cittadini. Nessuno, quindi, può rimanere indifferente a quello che giustamente il vicepresidente Frattini ha sottolineato essere un grande problema di relazioni tra le due sponde dell'Atlantico, che, ovviamente, va risolto dentro un contesto di carattere generale ed unitario.

Detto in altri termini, quella differenza culturale e giuridica che finora ha caratterizzato il sistema di protezione dati sulle due sponde dell'Atlantico, da un lato, e quella complessità nei rapporti tra le due sponde dell'Atlantico circa le politiche di sicurezza, dall'altro, se non messa a regime dentro un contesto convenuto, definito e rispettoso delle tradizioni e dei valori di entrambe le comunità, rischia di creare una serie di difficoltà e di tensioni che credo nessuno si possa o si debba augurare.

Questo è un altro dei problemi di fronte ai quali oggi ci troviamo: ci si trova l'Unione europea, ma anche noi Autorità nazionali. È chiaro che questo fa parte proprio degli aspetti più gelosi (che non possiamo assolutamente rinunciare a tutelare) della nostra missione, quando parliamo di protezione dei dati.

Potrei parlarvi di molte altre cose. Potrei dirvi, ad esempio, cosa sono le autorità comuni di controllo, sostanzialmente « collegi» a cui partecipano le Autorità nazionali, che hanno il compito di verificare la correttezza della tenuta delle banche dati messe in comune. Potrei tornare a parlarvi dei compiti a cui dobbiamo assolvere (e speriamo di farlo in modo sempre più incisivo) di vigilanza sulle banche dati del nostro paese, vuoi per motivi nazionali, vuoi per garantire i nostri cittadini, vuoi per motivi europei. Noi abbiamo infatti il dovere di garantire che il sistema SIS italiano sia perfettamente a regime, nell'ambito del sistema CED; abbiamo il dovere di garantire che tutte le banche dati utilizzate per ragioni di sicurezza e di giustizia, sia all'interno del territorio nazionale, sia nel contesto europeo, corrispondano alle regole convenute e disciplinate dal legislatore nazionale o da quello europeo.

Tuttavia, credo di aver già abusato più di quanto la vostra cortesia e la vostra pazienza avrebbero consentito. Nel rinnovarvi il ringraziamento sentito per questa occasione che ci avete dato, restiamo a vostra completa disposizione per ogni approfondimento rispetto ai temi che ho toccato e ribadiamo l'auspicio che ci possano essere ulteriori occasioni nelle quali abbiate la compiacenza di ritenere utile ascoltarci. Grazie.

PRESIDENTE. Grazie, presidente, anche per la completezza della sua esposizione. Avrei anch'io delle domande da porre, ma prima vorrei dare la parola ai colleghi.

TITTI DI SALVO. Intervengo semplicemente per esprimere un apprezzamento, non formale né rituale, per l'esposizione del presidente Pizzetti.

Sono contenta che verrà redatto un resoconto della seduta, che consentirà di approfondire la mole di informazioni e di valutazioni che ci sono state proposte, che – naturalmente parlo per me – hanno bisogno di un'ulteriore riflessione.

Approfitto della parola che mi è stata concessa per scusarmi del fatto di dovermi allontanare dall'aula. Oggi, come tutti i colleghi sanno, c'è stata una sovrapposizione di impegni.

Per quanto mi riguarda, approfitterò molto della disponibilità di approfondimento, una volta che gli atti trascritti consentiranno una maggiore valutazione.

GIOVANNI MAURO. Anch'io vorrei ringraziare il presidente Pizzetti per la sua relazione, ricca di contenuti e interessante. Naturalmente, la disponibilità espressa all'inizio del suo intervento non può che farci piacere e spingerci a collaborare, nell'ambito delle rispettive competenze.

In Senato abbiamo già approvato la legge comunitaria, che credo approderà alla Camera questa settimana. Nel provvedimento si è inserito un ulteriore ele-

mento, che ritengo dovrà essere oggetto di reciproca valutazione. Mi riferisco alla scelta di collegare la possibilità di asilo – dato giuridicamente oggettivo – anche all'orientamento sessuale delle persone. Credo che questo apra un nuovo capitolo che dovrà essere affrontato, in quanto assolutamente innovativo.

Poiché nel mondo vi sono paesi nei quali lo Stato infligge pene ai suoi cittadini a causa del loro orientamento sessuale, si è stabilito che, non potendo noi condividere questi atteggiamenti, si possa dare asilo a coloro che sono perseguitati, nei propri paesi di origine, per via dell'orientamento sessuale.

Naturalmente, nel dare attuazione a questa norma, la tutela dei dati dovrà essere ancora più pregnante. Se si adotta questa previsione normativa, sarà bene che le nostre banche dati e tutto il sistema di tutela si attrezzino in questa direzione.

So che si tratta di un tema assolutamente nuovo, ma credo che avremo occasione di parlarne e – spero – di poterci confrontare su queste nuove esigenze che si prospettano.

MERCEDES LOURDES FRIAS. Vorrei anch'io ringraziare il presidente Pizzetti per la chiarezza della sua esposizione, grazie alla quale anche una profana come me è riuscita a capire i termini della questione. Vorrei porre una domanda sull'ultima parte della sua relazione, riguardante PNR e SWIFT. A tal proposito, si prospettano due piani di valutazione, uno politico e uno giuridico.

Quanto all'aspetto politico, penso che concedere ciò che chiedono gli Stati Uniti – lei ha utilizzato la parola « pretesa » – non sia altro che un'inspiegabile subalternità nei confronti di chi comanda. Tuttavia, questo è un commento personale, di cui mi assumo la responsabilità.

Sul piano giuridico, invece, pongo una domanda. Penso che sia un dato di grande civiltà questa assunzione di responsabilità da parte dello Stato nel garantire il diritto alla protezione dei dati. A dire il vero, a volte si arriva all'eccesso che anche per iscriversi a un corso sia necessaria l'autorizzazione al trattamento dei propri dati, pena l'esclusione.

Come è possibile, dal punto di vista giuridico, che i cittadini europei non abbiano protezione nei confronti di uno Stato altro, considerato che questo diritto viene garantito localmente ? Non è una grossa contraddizione ? C'è qualcosa che si può fare in questo senso, agendo giuridicamente ?

PRESIDENTE. Presidente Pizzetti, vorrei approfondire quello che lei ha detto sul trattato di Prüm e sulla cooperazione, soprattutto in materia di lotta contro il terrorismo. Mi sembra che anche con lo sviluppo del trattato di Prüm, che porta ad una cooperazione rafforzata, rimanga comunque una zona grigia nell'attività degli Esecutivi, che giustifica ancora di più l'azione di Comitati come il nostro, che cercano di svolgere un'attività di vigilanza e controllo in quelle zone che oggi sfuggono sia al Parlamento europeo – il trattato di Prüm, nonostante l'evoluzione che lei ci ha descritto, sfugge al controllo del Parlamento europeo – sia al controllo dei Parlamenti nazionali. Al riguardo vorrei conoscere la sua valutazione. Esiste questa zona grigia ? È una zona grigia che va coperta, oppure è un problema non particolarmente rilevante ?

In secondo luogo, lei parlava di una *condicio sine qua non*, dal punto di vista dell'aumento di efficacia nella lotta contro il terrorismo: l'aumento di fiducia tra le amministrazioni nazionali. Alla luce di questa considerazione, per quanto riguarda il cosiddetto principio di disponibilità, cioè il libero accesso ai dati delle autorità investigative di uno Stato membro rispetto ai dati posseduti dalle autorità investigative di un altro Stato membro, come vede le recenti evoluzioni ? Quali tempi prevede ? Potremo arrivare all'obiettivo di affermare questo principio di disponibilità in tempi ragionevoli, oppure no ?

Infine, è chiaro che c'è un equilibrio giuridico – oltre che politico – instabile, per certi aspetti, fra il sistema di protezione dati americano e il sistema di protezione dati italiano ed europeo, e certa-

mente la situazione che lei ci descrive è complessa. Tuttavia, la necessità di rafforzare, su basi più equilibrate, la cooperazione fra noi e gli Stati Uniti rimarrà sempre una priorità nei prossimi anni. Come vede le evoluzioni prossime ?

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Chiedo scusa se non sarò esaustivo nel rispondere alle vostre domande. Sul diritto di asilo, per quel che ci risulta – e ringrazio il segretario generale, che è sempre molto preciso nella conoscenza di questi profili –, la specificazione sottolineata lo riguarda puntualmente. Avendo una Costituzione ispirata al principio di non discriminazione, noi consideriamo il fatto che un cittadino sia discriminato nel suo paese di origine per motivi sessuali come un elemento ulteriore, che rafforza la domanda d'asilo. Da questo punto di vista, se ho compreso bene, la norma è in favore del richiedente asilo.

Ovviamente è giustissima la sua osservazione, ma è altresì necessario che la presa in considerazione di un elemento così sensibile, di cui non neghiamo la possibilità di uso ai fini della valutazione della domanda di asilo, non si trasformi poi in una occasione di discriminazione.

GIOVANNI MAURO. Proprio perché diventa un elemento costitutivo per la concessione del diritto di asilo.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Mi auguro che in sede di attuazione della norma il Ministero dell'interno, che ha competenza sul diritto di asilo, presti la dovuta attenzione, propria dell'amministrazione, e poi ci interpelli e ci chieda il parere – a me pare sia giusto chiederlo a un'Autorità che ha come specificità istituzionale quella di essere esperta in protezione dati – su come conciliare le due esigenze: una in favore dell'asilante per evitare che il dato sensibile si trasformi in un danno per colui che si vede accolta la domanda d'asilo all'interno dell'ordinamento, e l'altra per garantire la sicurezza del dato.

La ringrazio molto della segnalazione, che ancora di più ci spingerà ad essere attenti, come Autorità.

Sul PNR, informo la Commissione che la nostra attenzione è assolutamente alta. Do anche una prima risposta alla domanda finale del presidente nella mia personale convinzione – ma credo sia una convinzione largamente condivisa – che il bene della sicurezza sia di tale rilevanza per tutte le comunità, americana ed europea, da richiedere assoluta attenzione ed evidenza. Da questo punto di vista, fa parte dei valori del costituzionalismo moderno prima di tutto la difesa della vita della persona. È chiaro che, al di là di ogni differenziazione di tipo ideologico che possiamo avere, nessuno che sia inserito nella tradizione culturale del costituzionalismo moderno può considerare, neanche per un istante, secondario il diritto alla sicurezza, che è il diritto innanzitutto alla protezione della vita della persona minacciata.

Sono d'accordo sul fatto che è assolutamente necessario per ciascuno dei protagonisti – ed io, ovviamente, essendo un europeo parlo per l'Unione europea – trovare un contemperamento corretto fra i diversi valori costituzionali (tutti di primissimo livello e irrinunciabili) e in particolare tra il diritto alla protezione dei dati e la sicurezza. Quando si parla di ricerca di un equilibrio, ovviamente si parla di un contemperamento, cioè di una messa in opera degli accorgimenti che consentano di assicurare il pieno rispetto dell'uno, senza un sacrificio inammissibile o inaccettabile dell'altro.

Personalmente, credo non ci siano difficoltà insormontabili, purché si accetti un dialogo fra pari e un dialogo tra soggetti che si riconoscono non solo come cittadini dello stesso mondo, ma anche come cittadini dello stesso sistema culturale e di tradizione valoriale. La mia convinzione è che molte volte la protezione dei dati trovi la sua particolare realizzazione nella garanzia che il dato sia usato non contro di me, ma per proteggermi. È un problema di vigilanza, di adeguatezza, di finalità.

Per quale scopo questi dati vengono raccolti ? Per la sicurezza. Sono necessari ?

Questa è una valutazione che non possono fare le Autorità, ma che le Autorità hanno il diritto di chiedere ai soggetti politici di fare con attenzione, nella consapevolezza che ogni dato raccolto è un potenziale pericolo anche se si raccoglie per difendere la persona.

Soprattutto, chi può conoscere, trattare, utilizzare i dati ? E come si proteggono ? In Italia abbiamo avuto amare esperienze, anche recenti, dei danni gravissimi che si possono fare acquisendo illecitamente dati, utilizzandoli contro le persone per proteggere le quali i dati stessi erano stati raccolti. Certe attività di dossieraggio che hanno utilizzato, come purtroppo sappiamo, banche dati pubbliche – finalizzate, al contrario, alla sicurezza della comunità – dimostrano la pericolosità di questo sistema.

Credo che, da questo punto di vista, se si accetta un dialogo fra pari, nel rispetto complessivo dei valori in gioco, non dovrebbe essere così difficile trovare un equilibrio ragionevole. In questo senso, mi preme dire alla Commissione bicamerale che noi siamo così attenti che ospiteremo, nella sede della nostra Autorità, il 22 e il 23, il sottogruppo del *working party*, ossia del sistema delle Autorità europee che lavora congiuntamente – nell'ambito della direttiva di primo pilastro – sul PNR. D'altro canto, una fortunata coincidenza ha fatto sì che il vicepresidente Frattini abbia avuto un colloquio con me in presenza del Collegio: sostanzialmente abbiamo assicurato al vicepresidente la massima attenzione allo sforzo – che lui, su mandato della Presidenza tedesca e credo del Consiglio europeo, sta svolgendo e implementerà ulteriormente – di negoziare un accordo accettabile con gli Stati Uniti.

Ho trattato non di politica, ma di problemi giuridici, nel senso di valori alti che sono in gioco. La sicurezza non è un valore solo politico; nessuno di noi potrà mai chiedere ad una mamma di accettare tranquillamente il rischio che suo figlio « salti » in metropolitana, perché il problema di tutela del valore fondamentale viene prima. Il nostro mestiere – nostro di tecnici della protezione dati, vostro di politici – è quello di trovare il punto di equilibrio fra valori che per i nostri concittadini non sono rinunciabili. Credo di poter assicurare che la nostra attenzione è massima, da questo punto di vista.

Il principio di adeguatezza è per noi il punto di riferimento essenziale. Perché serve un certo dato ? A quale scopo ? In quale contesto verrà utilizzato ? Credo che questi quesiti debbano muovere la nostra azione.

Un altro tema di particolare importanza è stato richiamato dal presidente (e anche di questo lo ringrazio), e riguarda il principio di disponibilità. Non ho detto, ma avrei voluto farlo – se avessi dovuto essere assolutamente esaustivo avrei dovuto abusare ancora di più della vostra pazienza –, che fra i meriti indubbi della Commissione europea, nel periodo più recente, c'è stato anche quello di accompagnare le proposte (relative, per esempio, all'implementazione del SIS-II ed altre) con una proposta di decisione quadro, relativa al principio di protezione dati e al principio di disponibilità proprio nel terzo pilastro.

Il disegno strategico è quello di implementare la raccolta dei dati e di accompagnarla con una normativa sul principio di disponibilità. Se, infatti, non posso scambiare i dati, perché dovrei raccoglierli ? E soprattutto, se non li posso scambiare, perché raccogliere i dati dovrebbe servire ad aumentare la sicurezza europea e non solo quella nazionale ? Il principio di disponibilità, dunque, è essenziale, ma, poiché rendendo più facile la circolazione dei dati esso aumenta i pericoli, tale principio richiede anche la decisione quadro sul principio di protezione dati nel terzo pilastro. Questo trasferisce nel terzo pilastro una serie di regole che sono consolidate per noi, nel contesto europeo, ma che nel terzo pilastro, come avete visto dalla mia esposizione, sono distribuite su autorità di controllo diverse, secondo modalità differenti, con livelli di garanzia diversi.

Registro che le proposte della Commissione sia in materia di disponibilità sia in

materia di protezione dati stanno incontrando non poche difficoltà nel processo di approvazione. Alla proposta del principio di disponibilità si oppone in molti casi una resistenza da parte delle stesse forze di polizia. Del resto, vi ho detto che il nostro ruolo è anche quello di rassicurare le forze di sicurezza, preoccupate del fatto che siano messi in circolazione dati fra soggetti che poi possono non aiutare a perseguire il crimine, ma osteggiare la lotta alla criminalità. È per questo che le autorità garanti hanno anche questo ruolo, quindi si trasformano in tutori dei diritti, ma anche in uno strumento di sicurezza.

Il principio di protezione dati nel terzo pilastro sta appunto incontrando difficoltà. È qui, non ultima, una delle ragioni del trattato di Prüm: considerato che è così difficile arrivare a una normativa condivisa fra tutti i paesi membri sul principio di disponibilità, ci si muove con la cooperazione rafforzata dentro il trattato. Quindi, il trattato di Prüm, che fa molta impressione per il profilo DNA, da un punto di vista teorico è ancora più rilevante, essendo un'anticipazione ulteriore del principio di disponibilità.

Nel ringraziarvi ancora, comunico che siamo a disposizione per tutto il tempo che vorrete dedicarci.

PRESIDENTE. Grazie, presidente. Oggi l'abbiamo già fatta lavorare abbastanza.

Accolgo il suo invito: il Comitato sarà un interlocutore politico costante dell'Autorità garante. Anche in futuro, dunque, l'aspettiamo per affrontare altri aspetti più specifici.

Dichiaro conclusa l'audizione.

La seduta termina alle 15,55.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE
DELLA CAMERA DEI DEPUTATI

DOTT. COSTANTINO RIZZUTO

Licenziato per la stampa
il 13 febbraio 2007.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

€ 0,30

15STC0002040