nella sua comunicazione del 22 gennaio 2004 e la definizione di elementi per una cooperazione tra le autorità nazionali incaricate dell'attuazione dell'art. 13 (per l'Italia, il Garante) attraverso la rete *spam* Cnsa, cui si è fatto riferimento, e l'adozione di regole comuni per la trattazione di casi di *spam* transfrontaliero.

Il Consiglio dell'Unione, proprio in considerazione del grande impegno da assumere per contrastare lo *spam,* ha adottato nel mese di novembre alcune conclusioni che impegnano gli Stati ad un recepimento puntuale della direttiva 2002/58/CE ed in particolare del suo art. 13; ha richiesto poi alla Commissione di valutare se alcune disposizioni nazionali introdotte in attuazione della direttiva possano ritenersi confliggenti con l'applicazione armonizzata del principio del consenso preliminare (*opt-in*) da parte del destinatario e pertanto incidere sull'efficacia delle misure di contrasto allo *spam* transfrontaliero.

Analoga attenzione è stata posta all'intensificazione della collaborazione internazionale –in particolare, come ricordato, in sede Ocse ed *International Communication Union* (Itu)– finalizzata alla presentazione, attraverso la Commissione europea, di una posizione unitaria dei Paesi dell'Unione. Infatti, in altri Paesi la legislazione vigente si fonda sul diverso principio del cd. *opt-out* (la possibilità, cioè, per il destinatario di chiedere di non ricevere le comunicazioni commerciali) e pertanto quello che nell'Unione europea dall'entrata in vigore della direttiva 2002/58/CE (e nei singoli Paesi dalla data di trasposizione) è assoggettato a sanzione, in altri paesi può non costituire un comportamento vietato.

In questo quadro, il contributo del Gruppo art. 29 assume una notevole rilevanza. In particolare, il parere n. 5/2004 del 27 febbraio 2004 offre indicazioni su specifici elementi che riguardano le nozioni di "posta elettronica", "previo consenso" da parte degli abbonati e "commercializzazione diretta"; si prendono altresì in considerazione l'eccezione alla norma del previo consenso e il regime per le comunicazioni indirizzate alle persone giuridiche.

22.3. *Le conferenze tra autorità di protezione dei dati a livello europeo*

La Conferenza di primavera dei Garanti europei si è svolta a Rotterdam dal 21 al 23 aprile 2004 ed è stata dedicata alle politiche finalizzate a garantire l'efficacia della protezione dei dati. I temi al centro dell'incontro hanno riguardato il ruolo e l'azione di intervento delle autorità, le comunicazioni elettroniche, il rispetto delle norme sulla protezione dei dati personali e la cooperazione giudiziaria a livello europeo.

Il segretario generale dell'Autorità ha affrontato il tema delle strategie da mettere in atto per garantire l'effettiva attuazione delle norme in materia di *privacy*, non solo attraverso verifiche e controlli, ma anche mediante una costante azione di sensibilizzazione. Per quanto riguarda in particolare l'attività di verifica, soprattutto alla luce della direttiva 95/46/CE, si è altresì evidenziata l'opportunità di potenziare la collaborazione fra le autorità nazionali della protezione dei dati, anche in considerazione del carattere transnazionale delle problematiche che investono il settore della *privacy* (esempio tipico lo *spam*).

22.4. *Conferenze delle autorità su scala internazionale*

La 26ª Conferenza internazionale dei Garanti per la protezione dei dati personali, che si è tenuta a Wroclaw dal 14 al 16 settembre, è stata dedicata al binomio società della *privacy* società e della dignità.

Il Garante ha partecipato all'incontro attraverso quattro interventi nelle differenti sessioni di lavoro:

Mauro Paissan ha svolto una relazione sul delicato rapporto tra libertà di informazione e diritti della persona, evidenziando come il diritto di sapere, la libertà di comunicare e la trasparenza non possano cancellare il bisogno di intimità e il diritto di sviluppare liberamente la personalità;

Gaetano Rasi si è soffermato sugli aspetti economici della *privacy*, sottolineando come la tutela dei dati personali sia destinata a svolgere una funzione fondamentale per disegnare i futuri assetti del rapporto tra imprese e consumatori; in particolare, il trattamento –da parte delle aziende– di informazioni relative alla clientela improntato ai criteri di correttezza e trasparenza può sensibilmente migliorare la qualità del rapporto tra azienda e cliente;

Giovanni Buttarelli è intervenuto nella sessione dedicata al *marketing* politico, evidenziando gli aspetti legati alla necessità di ottenere un consenso preventivo, da parte degli interessati, all'invio di materiale propagandistico. Ciò, soprattutto perché la "pubblicità" elettorale, fondata sul trattamento di dati che riguardano identità personale e convinzioni politiche, tocca una sfera particolarmente delicata dell'individuo. Le nuove tecnologie utilizzate anche nella propaganda politica comportano la necessità di salvaguardare ancora più attentamente il diritto alla riservatezza. Ferma restando la libera circolazione delle idee e delle proposte politiche, è opportuno promuovere –anche in questo settore– un *marketing* responsabile. La proposta del segretario generale di operare in vista di una possibile risoluzione in occasione della prossima conferenze mondiale è stata condivisa.

Al Presidente Stefano Rodotà è stato affidato il compito di chiudere i lavori della Conferenza. Nella sintesi conclusiva, il prof. Rodotà ha affermato che fra i concetti di *privacy*, libertà e dignità esiste un legame sempre più stretto, in ragione del fatto che il trattamento di dati personali può determinare discriminazioni sulla base di convinzioni politiche, credenze religiose, condizioni di salute: la *privacy*, non più riconducibile al solo diritto ad essere lasciati soli, costituisce un elemento essenziale della società dell'uguaglianza. In particolare, il Presidente ha evidenziato quattro temi che –per le loro implicazioni rispetto ai valori fondanti di una società democratica e al rispetto della persona– necessitano di una riflessione approfondita: i rischi del progressivo passaggio da forme di sorveglianza mirata verso soggetti pericolosi ad una sorveglianza "generalizzata"; le trasformazioni del corpo –utilizzato come *password* attraverso i dati biometrici– determinate dall'impiego di strumenti elettronici che rendono possibile localizzare e seguire l'individuo in modo permanente; la conservazione di dati per periodi troppo lunghi che rende ciascuno "prigioniero" del proprio passato e dei controllori delle grandi banche dati; la necessità di una protezione integrale della persona anche nella dimensione elettronica. Questi temi proiettano la tutela dei dati al di là della semplice protezione della sfera privata, per farla divenire un elemento essenziale della cittadinanza del nuovo millennio.

Al termine dei lavori sono state approvate tre risoluzioni riguardanti l'aggiornamento automatico dei *software*, l'istituzione di un *forum* comune per le questioni attinenti alla cooperazione giudiziaria e di polizia e la definizione di uno standard-quadro ISO in materia di *privacy* (v. *Documentazione* par. 75).

Nella risoluzione sull'aggiornamento automatico dei *software* i Garanti hanno preso atto con preoccupazione che le società produttrici di *software* fanno sempre più ricorso a meccanismi non trasparenti che permettono una serie di operazioni: trasferire nel *computer* degli utenti, a loro insaputa, aggiornamenti di *software* per raccogliere i dati personali memorizzati; assumere il controllo, almeno parziale, del *computer* terminale limitando la capacità dell'utente, quale titolare del trattamento, di

far fronte agli obblighi ed alle responsabilità previsti dalla legge per garantire la sicurezza dei dati trattati; modificare o provocare malfunzionamenti nel *software* installato senza la possibilità di individuarne la causa. I Garanti hanno, pertanto, invitato le aziende produttrici di *software* a prevedere che le procedure per il rilascio dei dati da parte degli utenti Internet, finalizzate anche all'aggiornamento *on-line* del *software*, siano trasparenti ed associate ad un'informativa adeguata. Tale aggiornamento dovrebbe avvenire, inoltre, solo dopo aver ottenuto il consenso dell'utente, impedendo nel contempo che possano verificarsi accessi non controllati al *computer*.

La risoluzione sulla cooperazione giudiziaria e in materia di polizia chiede l'istituzione di un *forum* comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia, nell'ambito, cioè, del cosiddetto Terzo Pilastro del Trattato di Amsterdam. Tale risoluzione poggia sulla necessità, avvertita nelle diverse sedi istituzionali europee, che gli Stati membri dell'Unione europea intensifichino ulteriormente la cooperazione giudiziaria e di polizia in ambito penale per assicurare un livello elevato di sicurezza in un'area di libertà, sicurezza e giustizia, garantendo al contempo un equo bilanciamento fra l'esigenza di sicurezza e la difesa delle libertà civili, compresi i diritti di protezione dei dati, la cui tutela è sancita dalla Carta dei diritti fondamentali dell'Unione europea. Tuttavia, le autorità per la protezione dei dati personali si trovano nella situazione di non poter esercitare la loro attività consultiva in materia a causa dell'assenza di una struttura di coordinamento. I Garanti hanno pertanto invitato il Consiglio e la Commissione, da un lato ad incorporare l'attività consultiva in materia di protezione dei dati nella struttura del Consiglio dell'Unione europea, dotandola delle necessarie risorse umane ed organizzative prima della fine del 2004 e, dall'altro, a creare i presupposti giuridici per l'armonizzazione delle attività di controllo nell'ambito del Terzo Pilastro.

Con la terza risoluzione, la Conferenza ha invece raccomandato all'Organizzazione internazionale per la standardizzazione (ISO), la definizione di uno o più *standard* globali in materia di protezione dei dati e *privacy*. I Garanti hanno chiesto, in particolare, l'individuazione di uno *standard* tecnologico fondato sulle prassi di leale informazione e sui principi di parsimonia, necessità ed anonimizzazione nell'uso dei dati, tale da supportare l'attuazione di norme di legge in materia di *privacy* e protezione dei dati, se già esistenti, e la formulazione di tali norme ove esse non siano ancora definite. Lo *standard*, si legge nella risoluzione, dovrebbe poggiare sul rispetto di tre parametri. In primo luogo, offrire criteri di valutazione e verifica che facilitino il rispetto delle normative nazionali ed internazionali da parte dei titolari. In secondo luogo, indicare se le misure volte alla tutela della *privacy* impiegate da sistemi utilizzati per la gestione di dati personali siano realmente efficaci. Infine, garantire che i dati personali siano trattati sempre nel rispetto dei parametri in base ai quali sono stati inizialmente raccolti, indipendentemente dai passaggi e dal numero di soggetti che possono intervenire nella gestione e nell'interscambio di tali dati personali. La Conferenza ha, inoltre, sottoposto all'ISO le sue preoccupazioni; le medesime sono state recepite, conducendo alla sospensione delle iniziative in corso miranti alla definizione di "*standard privacy*" per le tecnologie dell'informazione, avviate senza consultare le autorità di protezione dati.

La Conferenza internazionale che, nel 2005, tornerà a riunire le autorità garanti dei diversi Paesi, avrà ad oggetto le sfide legate alla protezione dei dati personali nel mondo globalizzato.

In particolare, la discussione si concentrerà sul carattere universale del diritto alla *privacy* pur nel necessario rispetto delle diversità. Ciò, ponendosi in una linea di continuità con le riflessioni iniziate nel corso della Conferenza internazionale *"One*

world, One privacy" (Venezia, settembre 2000) che hanno portato all'adozione della "Carta di Venezia". Già in tale occasione, infatti, le autorità –alla luce del riconoscimento della *privacy* come diritto fondamentale della persona e quale elemento costitutivo della libertà del cittadino– hanno evidenziato la necessità di perseguire regole comuni universalmente condivise per la salvaguardia di tale diritto.

22.5. *La cooperazione tra autorità garanti nell'Unione europea: il Gruppo* ex *art. 29*

Nel 2004 l'attività del Gruppo *ex* art. 29 si è incentrata, come nel passato, su tematiche attinenti agli ordinari ambiti di applicazione delle direttive 95/46/CE e 2002/58/CE soffermandosi, in particolare, su iniziative che, alla luce delle esigenze rappresentate dalle autorità giudiziaria e di polizia al fine di migliorare la raccolta e lo scambio di informazioni per la lotta al terrorismo ed alla criminalità, hanno potenzialmente un grande impatto sulla tutela della riservatezza e sul diritto alla protezione dei dati personali affermato solennemente come diritto fondamentale (già dalla Carta dei diritti fondamentali e ora) dal Trattato che adotta una Costituzione per l'Europa, firmato a Roma il 29 ottobre 2004 (articoli I-51 e II-68).

Il Gruppo, proprio per tener adeguatamente conto dei cambiamenti legati, da un lato, all'allargamento dell'Unione europea con l'adesione di dieci nuovi Stati e, dall'altro, al riconoscimento del diritto alla protezione dei dati come diritto fondamentale, ha deciso di avviare una riflessione approfondita sul proprio ruolo e sulle prospettive di lavoro futuro. Si è giunti così all'adozione di un documento di ampio respiro che disegna un programma di lavoro di medio-lungo termine e si affianca al programma di lavoro del Gruppo, che ha cadenza annuale. A giudizio delle autorità europee, i due binari da percorrere sono il miglioramento dell'attuazione dei principi comunitari in materia di protezione dei dati attraverso iniziative concrete, in parte già in corso, e la definizione ed il potenziamento della cooperazione fra il Gruppo stesso e le istituzioni comunitarie (in particolare la Commissione europea, il Parlamento europeo e il Consiglio dell'Unione), oltre che con le autorità chiamate a far rispettare le regole poste a garanzia di tale diritto (il Garante europeo per la protezione dei dati e, in particolare, le autorità comuni di controllo Europol, Schengen, Dogane ed Eurojust).

Il Gruppo ha chiesto di essere pienamente informato riguardo alle iniziative in corso di predisposizione (da parte delle istituzioni comunitarie) che possono avere un impatto sulla protezione dei dati personali, in modo da poter fornire il proprio contributo di conoscenza e competenza sin dalle fasi iniziali di formazione delle proposte di azione comunitaria. Ha in parallelo considerato opportuno sollecitare un miglioramento della cooperazione delle autorità di protezione dei dati per affrontare tematiche non più limitate agli aspetti tipici del mercato interno, ma che coinvolgano altri settori e politiche comunitarie sì da richiedere un esame ed un'azione comune da parte delle diverse autorità. Quest'ultimo punto, in particolare, riveste crescente importanza alla luce del rilievo assunto dalle questioni cosiddette di Terzo Pilastro anche in rapporto al difficile contesto internazionale. Il Gruppo è infatti intervenuto prendendo posizione con sempre maggiore frequenza anche su queste tematiche (ad esempio l'obbligo per i vettori aerei di fornire i dati *Passenger Name Record* (*Pnr*) dei passeggeri dei voli transoceanici (sul quale più compiutamente si sofferma il par. 22.6), quello di conservazione dei dati concernenti comunicazioni elettroniche, pur parzialmente sottratte all'ambito comunitario, nonché di introdurre in passaporti, visti, permessi di soggiorno elementi biometrici, foto digitalizzata ovvero scannerizzata del volto, impronte digitali).

Il programma di lavoro annuale per il 2004 ha, a sua volta, concentrato molte iniziative d'azione sui temi evidenziati dalla Commissione europea nel rapporto sull'applicazione della direttiva 95/46/CE e, segnatamente, in materia di semplificazione dei requisiti delle notificazioni, armonizzazione dei requisiti in materia di informativa, semplificazione dei trasferimenti internazionali, migliore e più coordinata attuazione di alcuni principi della direttiva.

Come illustrato in dettaglio nel par. 22.6, il Gruppo ha continuato a dedicare speciale attenzione alle richieste degli Stati Uniti di ottenere da parte delle compagnie aeree i dati personali dei passeggeri in viaggio da e verso il loro territorio. Alle richieste degli Stati Uniti si sono aggiunte quelle di alcuni altri Stati, segnatamente il Canada e l'Australia.

Sono stati al riguardo adottati, in rapida successione, cinque pareri, 3 rivolti alle richieste USA (pareri 2/2004, 6/2004 ed 8/2004) e due, rispettivamente a quelle australiane e canadesi (pareri 1/2004 e 3/2004).

In tema di trasferimento dei dati personali verso Paesi terzi, si segnala altresì la decisione adottata il 28 aprile dalla Commissione europea, sulla scorta del parere espresso in precedenza dal Gruppo, in merito all'adeguatezza della protezione dei dati personali nell'Isola di Man. Nel corso del 2004 è stata effettuata, sempre da parte della Commissione, la valutazione del funzionamento delle due decisioni di adeguatezza adottate nel 2000, relative alla Svizzera ed al cd. *Safe Harbor* (concernente il trasferimento dei dati verso gli Stati Uniti).

Entrambe le valutazioni sono state fatte precedere da uno studio affidato a consulenti esterni e le relative conclusioni sono state adottate il 20 ottobre 2004. I documenti di lavoro e gli studi su cui si fondano sono stati resi pubblici.

Per quanto riguarda il particolare il funzionamento dell'accordo sul *Safe Harbor*, il documento della Commissione conclude che, a suo avviso, pur evidenziandosi talune difficoltà applicative, non vi sono ragioni per rivedere la decisione del 2000. La Commissione ritiene apprezzabile l'aumento del numero delle società che hanno aderito al *Safe Harbor*, anche se considera necessario acquisire in futuro elementi sulla loro consistenza. Lo studio al quale la Commissione ha fatto riferimento per formulare le proprie valutazioni, svolto dal Crid (Centro di ricerca su informazione e diritto) dell'Università di Namur sotto la guida del prof. Poullet, fornisce un'approfondita ed articolata valutazione del funzionamento del sistema ed evidenzia vari aspetti problematici che vanno dal ruolo, non sempre pienamente svolto, delle autorità statunitensi preposte alla verifica del rispetto dei principi da parte delle società aderenti, alla mancanza di *privacy policy* sui siti delle stesse società, con la sensazione di una scarsa conoscenza delle implicazioni che l'adesione all'accordo determina e, quindi, di una ancora più scarsa informazione degli interessati in merito alla possibilità di far valere i loro diritti di accesso, di verifica, di rettifica e cancellazione. Altro aspetto messo in luce dallo studio consiste nella possibilità che in taluni casi la legislazione adottata negli Stati Uniti a seguito degli eventi dell'11 settembre abbia introdotto obblighi di comunicazione dei dati per le società aderenti.

Un caso segnalato specificamente dallo studio riguarda anche il possibile conflitto tra le normative statunitense ed europee con riguardo all'invio delle comunicazioni commerciali (*opt-out* vs. *opt-in*).

Alla luce di queste riflessioni, il Gruppo ha deciso nella sua ultima riunione del novembre 2004 di affidare ad un gruppo ristretto l'analisi attenta delle valutazioni offerte dallo studio del Crid.

Il Gruppo ha inoltre continuato ad approfondire il lavoro sulle cd. "soluzioni contrattuali", che consentono alle imprese di trasferire dati personali nel rispetto dei principi della direttiva anche quando il Paese di destinazione non abbia una legisla-

zione adeguata, prevedendo le idonee garanzie attraverso lo strumento contrattuale.

Da un lato, anche sulla scorta di un precedente parere del Gruppo, è stato approvato dalla Commissione europea un ulteriore modello di clausole contrattuali *standard* (in *Documentazione* par. 46). Le imprese saranno libere di scegliere se utilizzare l'uno o l'altro gruppo di regole. Il modello cd. "alternativo", cui si è fatto cenno anche nella *Relazione 2003*, è stato presentato dalla Camera di commercio internazionale e da altre organizzazioni commerciali ed è stato successivamente modificato in più parti su suggerimento del Gruppo, al fine di assicurare che le clausole contrattuali tipo proposte offrano un livello di tutela paragonabile a quelle approvate in virtù della decisione della Commissione n. 497/2001/CE.

Dall'altro lato, sono proseguiti i lavori per il riconoscimento e la possibile introduzione di un diverso sistema che consenta, in particolare, il trasferimento fra società appartenenti ad uno stesso gruppo multinazionale. Questo sistema, basato su ipotizzate "norme vincolanti d'impresa" (cd. *binding corporate rules*) era stato già analizzato dal Gruppo in un documento di lavoro (WP del 3 giugno 2003) al fine di valutare in quali termini e in base a quali condizioni questi speciali "codici di condotta" possano offrire, appunto, le "garanzie sufficienti" menzionate dall'art. 26(2) della direttiva.

Le "norme vincolanti d'impresa" sarebbero infatti veri e propri codici di condotta elaborati nell'ambito di un gruppo di imprese e validi per tutte le società che di tale gruppo fanno parte.

Basandosi sull'esperienza maturata in alcuni Stati membri e sugli approfondimenti scaturiti nel corso di un seminario internazionale svoltosi a l'Aja, il Gruppo ha recentemente adottato un documento in cui si individuano gli elementi essenziali per presentare ad una autorità di protezione dei dati la richiesta di autorizzazione (*model checklist*). Giova ricordare che, a differenza delle clausole contrattuali, sulla base delle disposizioni della direttiva la Commissione europea non è competente ad adottare una decisione vincolante in materia ed i singoli Stati (più precisamente le autorità nazionali di protezione dei dati) restano liberi di rendere o meno operanti le "norme vincolanti d'impresa" sul proprio territorio.

Dopo l'adozione di uno specifico documento di lavoro sull'uso dei sistemi biometrici (WP 80 del 1° agosto 2003), il Gruppo ha adottato l'11 agosto 2004 un parere sull'inclusione di elementi biometrici nei visti e permessi di soggiorno, che esprime dubbi sulla proporzionalità delle misure proposte rispetto alle finalità individuate dai proponenti e forti preoccupazioni in relazione al quadro più ampio in cui la proposta si colloca.

Come già evidenziato, infatti, occorre guardare in modo unitario ad una congerie di proposte formulate da Consiglio e/o Commissione, che prevedono un crescente impiego della biometria (impronte digitali e scannerizzazione del volto in particolare) rendendone obbligatorio l'inserimento nei documenti rilasciati a stranieri e cittadini (passaporti, carte d'identità, visti, permessi di soggiorno), prevedendo la creazione a livello europeo di grandi basi di dati in cui anche questi elementi vengono inseriti (Sis II, Sistema informazione visti-Vis) ed intensificando la possibilità di scambiare queste informazioni con una pluralità di Stati ed organismi esteri (in proposito si veda in allegato, anche il Regolamento (CE) n. 2252/2004 del Consiglio sulle caratteristiche di sicurezza e gli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri).

Il Gruppo, nel suo parere, ricorda che tali proposte hanno un forte impatto sui diritti umani fondamentali ed in particolare sul diritto alla protezione dei dati personali; pertanto, richiama l'attenzione sulla necessità di esserne preliminarmente informato e che le stesse proposte siano adeguatamente rese pubbliche nei confronti

dei Parlamenti e della società civile e che ai relativi lavori sia data trasparenza, anche attraverso il coinvolgimento delle autorità di protezione dei dati. Nel parere, infatti, il Gruppo ricorda l'obbligo di rispettare in particolare il principio di proporzionalità e la necessità di definire con chiarezza le finalità del trattamento dei dati biometrici. Il parere individua anche le cautele da adottare al fine di rendere "affidabile" il trattamento di tali dati e richiede precise garanzie in ordine allo stesso; chiede inoltre di ricevere informazioni approfondite sulla sicurezza del sistema scelto e sulle modalità di incorporazione dei dati nel *chip*.

Esprime infine forti preoccupazioni riguardo alla previsione della possibile creazione di un *database* centralizzato a livello europeo e ricorda che il ruolo delle autorità di supervisione deve essere mantenuto adeguato alle novità che si vogliono introdurre per evitare un abbassamento del livello di tutela.

Come già segnalato nella *Relazione* 2003, il Gruppo ha adottato il parere 4/2004 (WP 89 del 11 febbraio 2004) sul trattamento dei dati effettuato attraverso la videosorveglianza, che individua regole e garanzie precise sull'installazione di telecamere fornendo un quadro uniforme e armonizzato in materia a livello europeo. Il parere contiene un "decalogo" sulle cautele ed i principi da osservare, principi che si applicano anche ai trattamenti non soggetti espressamente alle disposizioni della direttiva europea (ad esempio, trattamenti effettuati per scopi di sicurezza pubblica o per il perseguimento di reati, oppure trattamenti effettuati da una persona fisica per scopi esclusivamente privati o familiari).

È stato altresì adottato un parere in tema di comunicazioni commerciali non richieste (parere 5/2004 WP 90 del 27 febbraio 2004), al fine di fornire una interpretazione comune dell'art. 13 della direttiva 2002/58/CE riguardo ad alcuni aspetti che potrebbero dare luogo a soluzioni divergenti in sede di recepimento o di applicazione della normativa nei diversi Stati membri.

Altro importante parere del Gruppo (parere 9/2004 del 9 novembre 2004) riguarda una proposta legislativa presentata da quattro Stati dell'Unione il 28 aprile 2004 (Doc. 8958) tendente ad imporre ai fornitori di servizi di comunicazione elettronica l'obbligo di conservazione dei dati di traffico trattati ai fini della fornitura del servizio o comunque disponibili.

La proposta, in discussione presso il Consiglio dell'Unione, nella sua forma attuale prevede la conservazione preventiva in maniera indiscriminata, per un periodo di tempo limitato solo nel minimo, di tutti i dati di traffico (telefonico, Internet, comprensivo della posta elettronica).

I Garanti hanno ritenuto tale proposta in contrasto con i principi fondamentali in materia di protezione dei dati e con la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Il Gruppo ha richiamato i precedenti pareri espressi, ha rinnovato la richiesta che sia previamente valutato, come previsto dalla stessa Convenzione, se l'ipotizzata interferenza nella vita privata abbia un'adeguata base giuridica e se risponda a criteri di necessità nel quadro di una società democratica, rammentando la necessità del rispetto dei principi in materia di protezione dei dati –in particolare dei principi di proporzionalità, pertinenza, finalità– per la conservazione dei dati di traffico anche per finalità giudiziarie e di polizia (v. art. 15 della direttiva 2002/58/CE).

Si segnala anche un primo documento di lavoro adottato dal Gruppo (WP 86 del 23 gennaio 2004) sui dispositivi proposti dal consorzio *Trusted Computing Group* per incentivare la sicurezza delle transazioni elettroniche attraverso strumenti non solo *software,* ma anche *hardware* e, soprattutto, il documento di lavoro adottato il 17 marzo 2004 (WP 91) sul trattamento dei dati genetici.

Nel documento di lavoro, come già rappresentato nella *Relazione 2003*, il

Gruppo ha preferito affrontare il progresso tecnologico nel campo della genetica e le sue ripercussioni nella sfera della riservatezza scegliendo un approccio analitico volto ad individuare i settori in cui maggiori sono le preoccupazioni in relazione al trattamento dei dati genetici.

22.6. *Il trasferimento dei dati* Pnr *dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea*

Uno dei temi più delicati e controversi a livello europeo ed internazionale resta il trasferimento dei dati *Pnr* dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea (v. già la *Relazione 2003*). Infatti, come sottolineato anche da un recente intervento del commissario europeo Frattini, la richiesta da parte delle autorità pubbliche di Paesi terzi di ottenere dalle compagnie aeree europee i dati dei passeggeri ai fini di prevenzione del crimine non solo deve essere valutata alla luce del rispetto del diritto fondamentale alla protezione dei dati personali, ma è collegata anche alla delicata questione della protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia nell'Unione europea (cd. Terzo Pilastro), che risulta tuttora frammentaria e non armonizzata.

Il Gruppo ha dedicato grande attenzione al tema, occupandosi non solo del sistema proposto dalle autorità statunitensi, su cui si era già espresso nel corso del 2002 e del 2003, ma anche dalle analoghe richieste provenienti dall'Australia e dal Canada, nella convinzione che i comuni obiettivi di lotta al terrorismo debbano essere perseguiti nel rispetto dei diritti fondamentali ed in particolare del diritto alla protezione dei dati personali.

Per quanto riguarda gli Stati Uniti, il Gruppo è tornato ad evidenziare, nel parere 2/2004, le lacune del sistema statunitense, proponendo una serie di miglioramenti atti a garantire che il trasferimento dei dati dei passeggeri avvenga nel rispetto dei principi stabiliti dalla normativa europea in materia di protezione dati. Fra questi, il Gruppo ha segnalato, in particolare, il principio di finalità, in base al quale i dati del *Pnr* dovrebbero essere utilizzati soltanto per contrastare il terrorismo ed altri specifici reati ad esso connessi; il principio di proporzionalità nei dati richiesti, evitando il trasferimento di dati superflui; la conservazione dei dati per un periodo limitato; il divieto di trattare dati sensibili; il diritto dei passeggeri ad essere adeguatamente informati e ad essere messi in condizione di esercitare agevolmente i propri diritti (accesso, rettifica). Inoltre, il Gruppo ha chiesto che le garanzie per i passeggeri non si basino meramente su impegni unilaterali privi di vincolatività giuridica per la controparte americana e tali da non creare diritti che i terzi (in questo caso i cittadini europei) possano far valere negli Usa in caso di controversie.

Anche il Parlamento europeo, condividendo molte delle critiche espresse dal Gruppo, nel marzo 2004 ha approvato due risoluzioni con cui, sottolineando gli insoddisfacenti risultati del negoziato tra autorità statunitensi e Commissione europea, invitava quest'ultima ad ottenere garanzie reali affinché fosse rispettato il diritto alla protezione dei dati personali dei cittadini europei, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Ue.

La Commissione ha però deciso di procedere con la propria iniziativa contenuta nel "pacchetto *Pnr*", adottando una decisione relativa all'adeguatezza della protezione accordata dagli Stati Uniti ai dati personali dei passeggeri aerei, fondata su impegni unilaterali (cd. "*undertakings*") delle autorità statunitensi. A tale iniziativa ha fatto seguito l'approvazione di un accordo internazionale da parte del Consiglio dei ministri dell'Ue,

con cui si impone alle compagnie aeree europee di consentire alle autorità doganali statunitensi l'accesso diretto ai dati contenuti nei propri sistemi di prenotazione (cfr. al riguardo i documenti riprodotti nei par. 43-45 in *Documentazione*).

Entrambi gli atti sono stati approvati a maggio 2004, nonostante le preoccupazioni espresse dal Gruppo art. 29 e la richiesta del Parlamento europeo, presentata ad aprile alla Corte di giustizia delle Comunità europee, di un parere preliminare sulla compatibilità con l'ordinamento comunitario del proposto accordo internazionale.

Ai sensi del "pacchetto *Pnr*", le autorità doganali statunitensi sono autorizzate ad accedere direttamente ad un novero molto ampio di dati (34 elementi, fra cui indirizzi, numeri di telefono, indirizzi di posta elettronica, numeri di carte di credito, informazioni contenute nei programmi "*frequent flyer*") e a conservare per almeno tre anni e mezzo le informazioni relative ai dati di tutti i passeggeri (al contrario del sistema australiano, approvato dai Garanti europei, in cui i dati vengono conservati solo in presenza di un reato o di una indagine per un presunto reato). I dati possono essere trattati per finalità che esorbitano dalla lotta al terrorismo ed essere ulteriormente trasmessi ad altre autorità, anche di Paesi terzi.

Allo stato, sono accessibili dati "neutri" e sensibili; con riguardo a questi ultimi, gli *undertakings* prevedono specifici impegni da parte delle autorità statunitensi a non farne uso. In futuro, i dati sensibili (riguardanti la salute, le convinzioni religiose o politiche, ecc.) non saranno più accessibili grazie ad un apposito sistema di filtraggio.

Infine, i diritti dei passeggeri europei ad essere informati, ad accedere ai propri dati ed eventualmente a rettificarli non sono sembrati adeguatamente garantiti: fra l'altro, sia per l'assenza di un organo di ricorso veramente indipendente, sia per la dubbia vincolatività giuridica degli impegni assunti dalle autorità statunitensi.

Pertanto, il Parlamento europeo ha deciso di presentare un ricorso alla Corte di giustizia delle Comunità europee (che si aggiunge a quello, decaduto a seguito della firma dell'accordo, presentato in sede pregiudiziale e del quale si è fatto cenno nella *Relazione 2003*) per far annullare la decisione della Commissione e l'accordo internazionale. Secondo il Parlamento europeo, non soltanto la soluzione raggiunta non tutelerebbe adeguatamente i diritti dei passeggeri, ma la stessa Commissione avrebbe oltrepassato le proprie competenze e non avrebbe assicurato la dovuta partecipazione del Parlamento al processo decisionale.

Tale ricorso è stato condiviso nel merito anche dal Garante europeo della protezione dati (la cui attività è iniziata di recente), il quale ha presentato nel novembre scorso alla Corte di giustizia una richiesta di intervento a sostegno delle posizioni del Parlamento europeo.

Nelle more della pronuncia della Corte, il Gruppo art. 29 si è adoperato per tutelare il più possibile i diritti dei passeggeri. Nel giugno 2004 è stato approvato il parere 6/2004 in cui, in relazione all'attuazione da parte delle compagnie aeree del "pacchetto *Pnr*", si è auspicato un rapido passaggio dal meccanismo che consente alle autorità statunitensi di accedere direttamente ai sistemi di prenotazione (cd. sistema *"pull"*) ad un meccanismo in cui siano le stesse compagnie aeree a filtrare i dati ed inviarli (sistema *"push"*), nonché a fornire l'informazione completa e chiara ai passeggeri.

Per approfondire tali temi, il Garante ha ospitato a Roma un incontro fra le autorità di protezione dati europee e i rappresentanti delle compagnie aeree. In seguito a questo incontro, il Gruppo art. 29 ha approvato il parere 8/2004, in cui si propongono modelli di informativa da fornirsi ai passeggeri dei voli transatlantici da parte delle compagnie aeree, degli agenti di viaggio e dei sistemi di prenotazione via *computer* facenti parte del circuito di prenotazione dei voli.

Come già detto, il sistema statunitense è solo il primo di una serie di analoghe e

sempre più numerose iniziative che hanno finora interessato Canada, Australia, Sudafrica e Corea del Sud.

Il Gruppo, pur nella convinzione che una soluzione multilaterale sia preferibile e più aderente al principio di non discriminazione, ha esaminato nel corso del 2004 le richieste dell'Australia e del Canada.

Il sistema australiano prevede il trasferimento di un numero più limitato di dati personali che sono raccolti per finalità di lotta al terrorismo e reati connessi e sono conservati solo in casi specifici. Inoltre, i diritti dei passeggeri sono garantiti a livello sia normativo, sia istituzionale. Per queste ragioni, il Gruppo ha espresso un parere sostanzialmente favorevole (parere 1/2004 del 16 gennaio 2004) ad una dichiarazione di adeguatezza da parte della Commissione dopo che saranno chiariti e risolti alcuni aspetti controversi.

Per quanto riguarda il Canada, il parere 3/2004 dell'11 febbraio 2004 ha evidenziato una serie di problemi che dovranno essere risolti prima che si possa dare avvio al trasferimento di dati.

Bisogna, infine, sottolineare come la dimensione internazionale della questione del trasferimento dei dati dei passeggeri abbia spinto diverse organizzazioni internazionali, quali l'Ocse e l'Icao, ad occuparsi del tema al fine di trovare adeguate soluzioni multilaterali (v. *infra*).

22.7. *Cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Nel 2004 si è evidenziata la tendenza ad un ulteriore incremento delle iniziative legislative adottate a livello comunitario per rafforzare la cooperazione tra le autorità nazionali di polizia e giudiziarie. Tali iniziative, come si è visto, spesso implicano lo scambio di informazioni personali e, talvolta, la creazione di nuove basi di dati europee ovvero l'ampliamento della possibilità di accesso ai dati dei sistemi di informazione esistenti a soggetti nuovi rispetto a quelli previsti nelle convenzioni istitutive.

È necessario che queste attività rispettino al contempo le esigenze richieste da un'effettiva cooperazione tra forze di polizia e autorità giudiziarie e il diritto fondamentale alla tutela dei dati personali (solennemente introdotto dalla Carta dei diritti fondamentali e dal Trattato per una Costituzione europea) e si svolgano quindi nei limiti consentiti dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Attualmente, le iniziative dell'Ue che comportano la raccolta, la conservazione o lo scambio di dati personali ai fini dell'applicazione della legge sono numerose: tra gli esempi più significativi vi sono misure per consentire lo scambio di informazioni e la cooperazione rispetto ai reati terroristici, la semplificazione dello scambio di informazioni e di "*intelligence*" tra i servizi repressivi degli Stati, l'accesso ai dati ed agli archivi da parte degli organi giudiziari e le forze di polizia, lo scambio di dati sui passeggeri di voli aerei, nonché proposte per richiedere la conservazione dei dati delle comunicazioni. Vi sono poi, come ricordato, le diverse proposte volte ad introdurre elementi biometrici nei documenti rilasciati dagli Stati Ue a cittadini e stranieri, con la previsione di larghe basi di dati a livello europeo che si aggiungerebbero a quelle già esistenti, moltiplicando i rischi e gli effetti di un erroneo inserimento di dati o di accessi non autorizzati.

Questi ed altri sviluppi, quali il suggerimento di trasformare in futuro l'Europol in un'agenzia investigativa, possono avere rilevanti implicazioni anche per i diritti degli individui.

Per il modo della loro elaborazione e per la frammentarietà delle competenze in materia in seno all'Unione, molte delle nuove iniziative dell'Unione europea che riguardano dati personali sono al momento sottratte al controllo delle autorità di protezione dei dati poiché non rientrano in modo netto in uno dei tradizionali pilastri dell'Ue. Nonostante i ripetuti inviti del Parlamento europeo, queste attività hanno continuato ad essere svolte solo in gruppi di lavoro a composizione specializzata, senza il coinvolgimento adeguato delle istituzioni e degli organismi che a livello nazionale e comunitario hanno responsabilità in materia –con la conseguenza che spesso possono sfuggire sia alla tempestiva valutazione del Gruppo articolo 29, sia all'esame delle autorità di controllo esistenti nel cd. Terzo Pilastro (Schengen, Europol, Dogane)– senza, peraltro, un'adeguata base giuridica fondata sull'elaborazione di principi di protezione dei dati validi per i trattamenti proposti.

Già da tempo le autorità di protezione dei dati avevano segnalato il progressivo venir meno di "momenti istituzionalizzati" che favorissero la necessaria valutazione dell'impatto che tali misure erano destinate a produrre sui diritti fondamentali della persona e, più specificamente, sulla tutela dei dati personali. Infatti, i gruppi di lavoro il cui mandato specifico nel Consiglio dell'Ue era la protezione dati, rispettivamente nel Primo e Terzo Pilastro, sono stati soppressi fin dal 2002 e solo nei primi mesi del 2004 il Garante europeo per la protezione dei dati ha iniziato la sua attività, peraltro limitata ai trattamenti effettuati dalle istituzioni comunitarie "nei settori di competenza del diritto comunitario".

Considerato che i pilastri dell'Ue con l'adozione del Trattato firmato a Roma il 29 ottobre 2004 sono destinati a convergere e la protezione dei dati personali ha assunto il rango di diritto fondamentale, in occasione della Conferenza delle autorità incaricate della protezione dei dati svoltasi a Rotterdam nel 2004, è stato deciso che i rappresentanti delle autorità che operano a livello comunitario si riuniscano per coordinare la loro attività e cercare di svolgere un ruolo adeguato ai bisogni rappresentati.

Alla prima riunione di questo gruppo "di pianificazione", che ha avuto luogo nel giugno 2004, hanno partecipato il Garante europeo della protezione dei dati, i presidenti delle autorità di controllo comune e la presidenza del Gruppo art. 29.

La situazione si è evoluta nel settembre 2004 in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati a Wroclaw, quando una sessione a porte chiuse delle autorità europee ha approvato una risoluzione in cui si chiede che le istituzioni dell'Ue promuovano un *forum* nel quale le autorità europee incaricate della protezione dei dati possano discutere le implicazioni a livello di protezione dei dati degli sviluppi del Terzo Pilastro. Fino alla creazione di tale *forum*, le iniziative del Terzo Pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune, saranno esaminate da un gruppo di lavoro delle autorità europee incaricate della protezione dei dati.

Le autorità di controllo hanno pertanto deciso, avvalendosi della struttura di segreteria comune prevista per assistere i lavori delle autorità Schengen, Europol e Dogane, di prevedere alcune riunioni congiunte, invitando anche il Garante europeo per la protezione dei dati e l'autorità di controllo istituita per Eurojust, ove informarsi e discutere, al momento informalmente, delle iniziative esistenti ed eventualmente definire proposte unitarie da presentare agli organismi competenti, avvalendosi anche delle aperture che sembrano presenti nel nuovo programma per il rafforzamento dell'area di libertà, sicurezza e giustizia per il periodo 2005-2009.

Un canale particolare di dialogo si è aperto con la *House of Lords*, il cui sottocomitato specializzato ha richiesto un parere sulla protezione dei dati nel Terzo Pilastro, ed è stato rafforzato il legame esistente con il Parlamento europeo, Commissione libertà e diritti dei cittadini, che ha voluto incontrare più volte i rap-

presentanti delle autorità in previsione della discussione di alcune delle iniziative menzionate. Va ricordato in proposito che a partire dal 1° gennaio 2005 il Parlamento ha acquisito il diritto alla codecisione in materie quali le politiche di visti, asilo, immigrazione e le altre politiche connesse alla realizzazione del principio della libera circolazione delle persone e sarà quindi necessario il suo accordo per la loro adozione.

Ma certamente la novità più positiva in materia è legata alla nomina del nuovo Commissario italiano come vice presidente e responsabile del settore Libertà, sicurezza e giustizia. Fin dalla presentazione del suo programma davanti al Parlamento europeo il Commissario Frattini ha infatti chiarito che intende far garantire il pieno rispetto del diritto alla protezione dei dati personali e favorire il dialogo con le autorità di protezione dei dati per le materie affidate alla sua competenza.

A rafforzamento di questo impegno il Commissario ha incontrato le autorità di controllo comuni nella loro riunione congiunta del 21 dicembre pronunciando un apprezzabile discorso disponibile in rete che contiene precise linee di azione ed impegni in materia e che dovrebbe servire da guida anche per i successivi interventi dei rappresentanti della Commissione.

22.8. *L'attività del Garante nell'Autorità di controllo comune Schengen*

Il Garante è autorità nazionale di controllo per l'Italia con il compito di esercitare un controllo indipendente dell'archivio della sezione nazionale del Sistema d'informazione Schengen (Sis) e verificare che l'elaborazione e l'utilizzazione dei dati inseriti non leda i diritti della persona interessata, ai sensi dell'art. 114 della Convenzione; in tale veste entra a comporre l'Autorità di controllo comune (Acc).

Fra le attività di maggior rilievo dell'Acc, alle cui riunioni il Garante ha partecipato attivamente fin dall'inizio nella persona del segretario generale, prima vice presidente poi nel biennio 2002-2003 presidente dell'Autorità, va ricordata quella di verifica e controllo del funzionamento della parte centrale del Sis e di vigilanza sulla corretta applicazione delle disposizioni della Convenzione, attività che viene svolta anche attraverso l'indicazione, ove necessario, degli aggiustamenti e delle prassi corrette da adottare. Considerato che ad una persona può essere rifiutato l'accesso al territorio Schengen (e non più solo al territorio nazionale) sulla base di informazioni contenute nel sistema, resta di immediata ed ovvia importanza assicurare che le informazioni siano ad esempio accurate ed aggiornate.

L'attività dell'Acc continua ad essere di particolare rilievo e, al riguardo, va notata la crescente attenzione prestata dal Consiglio dell'Unione europea ai pareri dalla stessa espressi, come ad esempio mostra la recente Decisione relativa alla "lotta contro la criminalità connessa con veicoli". Il testo approvato ha recepito largamente le osservazioni critiche formulate dall'Acc rispetto alla proposta iniziale e non prevede più di allargare l'accesso diretto al Sis a soggetti diversi da quelli già autorizzati, limitandosi a richiedere da parte delle autorità competenti il tempestivo inserimento nel sistema di una segnalazione ogniqualvolta vengano denunciati furti di veicoli o di carte di circolazione e l'informazione degli uffici nazionali della motorizzazione.

Nel corso del 2004 gran parte dell'attività dell'Acc ha continuato ad essere concentrata sui problemi legati allo sviluppo del Sistema informativo Schengen, il cd. Sis II.

In estrema sintesi, vi sono due aspetti che preoccupano fortemente l'Acc, il primo concernente le informazioni che il Sis deve contenere (anche a fronte delle diverse proposte per introdurre nuove categorie di informazioni e nuovi tipi di dati); l'altro,

in merito all'accesso al Sis e all'uso dei dati nel sistema. Con queste proposte, peraltro frutto e sintomo di un approccio normativo frammentario, si tende ad trasformare il Sis in un sistema di indagine e non più solo di informazione, mutandone quindi radicalmente le finalità rispetto a quelle definite dalla Convenzione del 1990.

L'Autorità ha ricordato nel parere adottato il 19 maggio che l'ampliamento delle categorie di informazioni registrabili nel sistema, il possibile inserimento di dati biometrici, la modifica di alcuni meccanismi di accesso e utilizzazione dei dati proposti a livello tecnico, possono essere praticati, ma devono essere fondati su un'appropriata base giuridica. L'Acc ha rimarcato l'assenza di tale base ed ha ricordato il necessario rispetto del testo attuale della Convenzione, la quale individua esattamente le categorie di dati inseribili e le autorità che possono accedere ai dati, fissandone i limiti. Anche i compiti delle autorità di supervisione e controllo sono disegnati in relazione alle attuali funzionalità del sistema.

Qualunque cambiamento, inclusi quelli definiti con il recente regolamento del Consiglio del 29 aprile 2004 (v. *Documentazione* par. 49), deve essere considerato ed "equilibrato" rispetto al disegno dell'intero sistema. L'Acc ha chiesto pertanto che le proposte siano previamente e adeguatamente discusse considerando anche quale sarebbe il loro impatto sui diritti fondamentali della persona e sul rispetto dei principi in materia di protezione dei dati, in particolare il principio di proporzionalità delle modifiche richieste. In questa valutazione, deve essere anche considerato il rischio che il Sis, incorporando nuove funzioni e nuove categorie di dati, possa duplicare inutilmente sistemi di informazioni già esistenti in seno all'Unione. L'Acc si è dichiarata disponibile ad assistere con la sua competenza le istituzioni comunitarie ed ha comunque richiesto una puntuale informazione sui lavori in corso, per poter essere in grado di formulare indicazioni in tempo utile rispetto all'adozione degli atti.

I timori dell'Acc si fondano sull'osservazione del modo in cui i lavori per il Sis II vengono portati avanti. Sarebbe infatti logico far precedere lo sviluppo tecnico del sistema sia da decisioni politiche che ne fissino le finalità e le relative modalità di funzionamento, sia dalla definizione di un idoneo quadro giuridico che modifichi le disposizioni attualmente vigenti specificando le finalità del sistema e stabilendo le norme necessarie per definire le modalità di accesso e gli altri elementi essenziali. Invece, in mancanza di decisioni appropriate, le proposte formulate dalla Commissione cercano di costruire un sistema basato sulla massima flessibilità tecnica, prevedendo il maggior numero di funzioni e di accessi. *"Pertanto"*, si legge nel parere dell'Acc, *"la messa a punto del sistema avviene sotto l'impulso delle mutevoli istanze provenienti dal settore giustizia e affari interni dell'Ue, anziché sulla base di obiettivi espressi e definiti all'interno di un quadro giuridico preciso"*.

Preoccupazioni analoghe sono state rappresentate anche dal Parlamento europeo che si è dimostrato molto sensibile alle sollecitazioni provenienti dalle autorità di protezione dei dati personali.

L'Acc ha inoltre proseguito l'attività di verifica sulle modalità dell'inserimento nel Sis delle segnalazioni di stranieri al fine di non ammetterli sul territorio Schengen, per valutare se vi siano discrepanze fra gli Stati Parte nell'applicazione e/o nell'interpretazione dell'art. 96 della Convenzione. Nel corso dell'anno, le autorità nazionali di controllo hanno richiesto, sulla base di un modulo appositamente predisposto, specifiche informazioni sulle procedure seguite dagli uffici che sono abilitati ad inserire i dati nel sistema (per l'Italia: oltre ad alcuni uffici centrali del Ministero dell'interno, le questure) e hanno svolto colloqui che hanno interessato anche il Sis nazionale (N-Sis) ed il Sirene.

Di queste attività, che sono state svolte in maniera coordinata in tutti gli Stati

Schengen, è stata data ampia informazione all'Acc la quale predisporrà un documento riassuntivo e, ove necessario, linee-guida. Una seconda parte dell'indagine, consistente in una ispezione agli archivi per verificare in concreto la correttezza degli inserimenti ed il rispetto delle regole in materia di trattamento e conservazione dei dati, sarà svolta, sempre con modalità coordinate, nei primi mesi del 2005.

A completamento di quanto detto, si può segnalare, anche se non direttamente legata all'attività dell'Acc, la visita di valutazione che gli esperti del Consiglio dell'Unione europea hanno svolto in Italia nel mese di settembre 2004 per gli aspetti relativi alla protezione dei dati. Di essa si è già reso conto nel par. 6.3; è opportuno evidenziare qui le preoccupazioni manifestate dagli esperti per l'alto numero di segnalazioni inserite ai sensi dell'art. 96 con il conseguente invito a verificarne la qualità.

22.9. *Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso*

L'Autorità comune di controllo ha presentato il 23 novembre scorso la seconda relazione di attività che copre il biennio da novembre 2002 ad ottobre 2004 (v. *Documentazione* par. 54).

Nella relazione, l'Acc ha ricordato come, in un periodo fortemente caratterizzato dalle misure adottate per combattere il terrorismo dopo i tragici eventi dell'11 settembre 2001 negli Stati Uniti e, recentemente, dagli attentati di Madrid nel marzo 2004, l'Autorità stessa nei suoi pareri e nelle iniziative attuate abbia dimostrato che è possibile, e per nulla incompatibile, sostenere l'obiettivo comune della lotta al terrorismo internazionale e alla criminalità organizzata, salvaguardando nel contempo i diritti dei singoli.

L'Acc ha anche evidenziato che risulta sempre più evidente che il campo della cooperazione di polizia e giudiziaria necessita di norme chiare e specifiche sulla protezione dei dati, con la formulazione di un parere indipendente e di un'attività di controllo armonica.

Relativamente all'attività svolta nel corso del 2004, si segnala in particolare la vigilanza sulle modalità di applicazione dell'accordo Europol-Stati Uniti per la trasmissione di dati personali.

Secondo i dati acquisiti dall'Acc lo scambio della maggior parte delle informazioni tra l'Ue e le autorità di polizia statunitensi sembrerebbe essere avvenuto in base ad accordi bilaterali esistenti tra gli Stati Uniti e singoli Stati membri. L'Autorità, tuttavia, ritenendo che il volume di informazioni scambiate tra Europol e Stati Uniti aumenterà, ha deliberato di concentrare le ispezioni future dell'Europol sull'esame dei dati di natura personale trasmessi nell'ambito dell'accordo, per assicurare che vi sia conformità alle disposizioni pertinenti. Inoltre, l'Acc cercherà di coordinare l'attività di vigilanza, collaborando con le autorità nazionali incaricate della protezione dei dati personali negli Stati membri e con il *Chief Privacy Officer* presso il Dipartimento della sicurezza interna negli Stati Uniti.

La conduzione d'ispezioni *in loco* delle attività dell'Europol costituisce peraltro uno dei modi adottati dall'autorità di controllo comune per ottemperare al suo mandato. L'Acc ha al riguardo definito gli obiettivi ed i criteri che guideranno le ispezioni future (di regola annuali), anche alla luce della considerazione che il ruolo dell'Europol si sta sviluppando rapidamente, con un numero sempre maggiore di dati trattati.

Nel marzo 2004 è stata effettuata una nuova ispezione, incentrata sulla qualità dei dati trattati negli archivi per fini di analisi. Come risultato, il *team* d'ispezione ha riscontrato che, nel complesso, la qualità dei dati è soddisfacente, almeno per

quanto riguarda la rispondenza dei dati negli archivi con quelli forniti dagli Stati membri. Tuttavia, è stata confermata la percezione di un'incapacità generale da parte degli Stati membri di valutare correttamente i dati trasmessi ad Europol (verificando la fonte, l'affidabilità e così via). L'Acc ha sottolineato che, per risolvere questo problema, occorre migliorare la cooperazione tra Stati Membri ed Europol.

Altro tema rilevante riguarda le squadre investigative comuni: l'Acc sta attualmente valutando la portata del sostegno in materia di analisi fornito dall'Europol.

Una decisione del Consiglio ha introdotto regole comuni per queste squadre ed ha previsto la possibilità che le stesse includano "funzionari di organismi costituiti ai sensi del Trattato sull'Unione europea": una definizione che interessa dunque anche il personale dell'Europol. I particolari riguardanti la partecipazione di questo organismo a squadre investigative comuni sono stati definiti in un successivo Protocollo ai sensi del quale il suo personale parteciperebbe solamente con "funzioni di supporto". Tuttavia, sempre in base al Protocollo, gli agenti dell'Europol verrebbero comunque inseriti nella catena di comando e le informazioni detenute negli archivi sarebbero condivise con i componenti della squadra; inoltre, le informazioni da questa raccolte sarebbero a loro volta inserite nelle banche dati dell'Europol.

L'Acc ha chiesto all'Europol di essere informata in merito alle decisioni riguardanti il tipo di sostegno che sarebbe offerto alle squadre investigative comuni. Ed in particolare sul modo in cui l'organismo intende utilizzare i suoi servizi di analisi ed ha intenzione di vigilare per assicurare il rispetto della Convenzione.

L'attività del comitato ricorsi

Nel 2004 l'Europol (in base a dati dallo stesso forniti) ha ricevuto circa dieci richieste di accesso (un dato relativamente stabile negli ultimi due anni) mentre risultano in aumento i casi di contenzioso.

Nell'ultimo anno il comitato ha deciso in merito a due ricorsi e attualmente vi sono parecchi casi su cui deve ancora esprimersi.

I casi affrontati hanno portato a decisioni relative a importanti questioni di principio. In particolare, è stato affermato che l'Europol deve considerare nel merito ogni richiesta di accesso, anziché applicare un approccio generale e che deve rispondere ad ogni richiesta nella lingua in cui la stessa è formulata, purché sia una delle lingue ufficiali dell'Unione europea.

22.10. *Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune*

Come si è ricordato nelle precedenti Relazioni, a seguito della ratifica ed entrata in vigore della Convenzione sull'uso dell'informatica nel settore doganale, è stato creato un sistema informativo automatizzato comune ai paesi membri dell'Ue (Sistema informativo doganale-Sid) per facilitare la prevenzione, ricerca e repressione delle infrazioni sia delle norme comunitarie, sia delle leggi nazionali, attraverso lo scambio di dati ed informazioni fornite dai servizi doganali di ciascuno Stato membro.

Il sistema consiste in una base di dati centrale cui si può accedere tramite terminali in ogni Stato membro. La Commissione europea provvede alla gestione tecnica dell'infrastruttura del Sid.

La vigilanza sul corretto funziamento del Sid è affidata ad una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

Nel corso del 2004 l'Autorità si è riunita due volte ed in particolare nella seconda riunione, svoltasi nel mese di dicembre, sono stati affrontati aspetti cruciali per la sua configurazione ed attività.

In primo luogo è emerso un delicato problema di funzionalità dell'Acc: infatti, pur essendo state approvate le linee guida per svolgere la prima ispezione al Sid e costituito il *team* di esperti per effettuarla, la stessa non ha potuto svolgersi per mancanza di disponibilità finanziaria. Le attuali disposizioni di *budget* del Consiglio consentono il rimborso –tra l'altro non all'Autorità nazionale che sostiene le spese, ma al Governo– delle sole spese di viaggio di un componente in occasione delle riunioni dell'Acc e non ci sono stanziamenti per consentire le altre attività, pur previste dalla Convenzione. L'attività di ispezione dovrebbe quindi svolgersi ad intero carico delle autorità che compongono il *team* di esperti.

Ne è scaturita una riflessione tra i componenti i quali hanno lamentato che la situazione creatasi incide gravemente sulla funzionalità dell'Autorità e lede il presupposto stesso della sua esistenza, quello, cioè, di sorvegliare sul funzionamento del Sid anche attraverso l'accesso allo stesso (v. art. 18 della Convenzione). È stato chiesto al Presidente di rappresentare nei modi più appropriati tale doglianza.

Altro punto importante riguarda l'ancora scarsa utilizzazione del sistema da parte delle autorità doganali. Per approfondire gli aspetti che rendono problematico l'utilizzo del sistema, nella riunione di dicembre sono stati invitati rappresentanti dell'Olaf e del Gruppo di cooperazione doganale del Consiglio.

Ne è emerso un quadro complesso, legato anche alla presenza contestuale di numerose basi di dati nel settore: i rappresentanti delle istituzioni comunitarie hanno però confermato la volontà di far sì che il Sid sia posto al centro della cooperazione doganale e di prevederne addirittura il potenziamento, al fine di metterlo in grado di svolgere attività di analisi dei rischi. L'Autorità, su questo punto, ha ricordato la necessità del pieno rispetto della Convenzione ed ha auspicato un analogo potenziamento del suo ruolo, dichiarandosi disponibile a fornire ogni contributo ai futuri lavori.

22.11. *La partecipazione ad altri comitati e gruppi di lavoro*

IWGDPT

Il Garante ha partecipato ai due incontri dell'*International Working Group on Data Protection in Telecommunications* (IWGDPT) che si sono svolti in Argentina (Buenos Aires, 14-15 aprile 2004) e in Germania (Berlino, 18-19 novembre 2004).

Il primo incontro ha preso in esame in particolare i problemi connessi alla libertà di espressione nel mondo *on-line*, ai nuovi servizi di comunicazione (*wireless, Mms*) e agli effetti che essi producono sulla *privacy*, nonché alle problematiche concernenti le tecnologie *Rfid*. Su questi temi i delegati hanno adottato tre documenti che richiamano l'esigenza di garantire il rispetto dei principi di protezione dati, anche attraverso un'adeguata informativa del pubblico, la disponibilità di strumenti che consentano agli interessati l'esercizio dei diritti loro riconosciuti e l'adozione di idonee misure di sicurezza.

Durante il secondo incontro sono stati adottati due documenti rispettivamente dedicati agli strumenti e alle procedure per combattere le frodi informatiche nel rispetto della *privacy* e alle modalità concrete attraverso le quali i soggetti deputati alla sicurezza delle reti possano acquisire le necessarie conoscenze dal punto di vista della protezione dei dati. Sono stati inoltre affrontati i problemi legati alle tecnologie di localizzazione e di videosorveglianza (con particolare riferimento alla registrazione delle immagini, all'utilizzo di sistemi di riconoscimento dello *stress* attraverso l'analisi della voce e i pericoli connessi al *Voice over IP* nel caso in cui il terminale usato per la ricezione delle comunicazioni sia un *computer*).

La delegazione italiana ha chiesto, in conclusione, di inserire il tema dell'*e-health*, ed in particolare della cartella clinica *on-line*, nell'ordine del giorno dei prossimi incontri.