In relazione ai campioni di materiali genetici, viene ribadita la necessità di garantire pienamente i diritti degli interessati durante il trattamento, così come l'opportunità di distruggere o rendere anonimi i campioni non appena ottenute le informazioni necessarie, anche in considerazione del loro eventuale impiego per fini di clonazione. Tutti i dati genetici devono inoltre essere trattati solo da professionisti qualificati, sulla base di specifiche autorizzazioni e regole.

Il documento si chiude invitando le autorità nazionali a svolgere un ruolo attivo nei rispettivi Paesi, con la previsione di forme di *prior checking* (in particolare per le cd. bio-banche) e ponendo l'accento sulla necessità di applicare i principi di proporzionalità e finalità.

La Conferenza di Sydney

44 La Conferenza e le Risoluzioni

Il Garante ha partecipato a numerose conferenze internazionali (su cui *infra,* parag. 52.3.): in questa sede va ricordata in particolare la partecipazione alla 25ª Conferenza internazionale delle autorità per la protezione dei dati personali, svoltasi a Sydney dal 10 al 12 settembre 2003.

La conferenza australiana ha rappresentato, infatti, un momento significativo nella discussione su una serie di temi emersi recentemente con piena evidenza: i prossimi passi nella regolamentazione della protezione dei dati personali, gli effetti che le normative sulla *privacy* producono a livello globale su imprese e consumatori, gli organismi, le tecnologie e gli incentivi per sostenere e sviluppare la difesa del diritto alla riservatezza, le implicazioni della protezione dei dati personali in campo giuridico, i rapporti tra tutela dell'ordine pubblico e rispetto delle persone, il ruolo svolto dalla *privacy* nella società contemporanea.

Alla Conferenza, che ha visto riuniti rappresentanti delle autorità per la protezione dei dati personali, esperti, imprese e rappresentanti governativi di oltre quaranta Paesi, l'autorità italiana ha partecipato con una delegazione guidata dal presidente prof. Stefano Rodotà, dal componente del collegio, on. Mauro Paissan e dal segretario generale, Giovanni Buttarelli. Il prof. Rodotà ha presieduto la sessione inaugurale dedicata alle nuove prospettive di regolamentazione della *privacy*. La Conferenza è stata preceduta da seminari di formazione e conferenze su diversi argomenti: tra queste va segnalata quella svoltasi l'8 settembre 2003 a Melbourne, dedicata a corpo fisico, corpo elettronico e dati personali, aperta dallo stesso prof. Rodotà.

La Conferenza si è conclusa con l'approvazione di cinque risoluzioni che richiamano l'attenzione su aspetti attuali e significativi della vita privata dei cittadini.

44.1. Trasferimento dei dati dei passeggeri

Una risoluzione riguarda il trasferimento di dati personali riguardanti i passeggeri da parte delle compagnie aeree alle autorità statunitensi. In essa viene affermato che nella lotta contro il terrorismo e la criminalità organizzata gli Stati devono osservare i principi fondamentali in materia di protezione dei dati, e che le informazioni sui viaggiatori diretti negli Usa possono essere acquisite e trasferite solo all'interno di un contesto che tenga conto delle esigenze di protezione dei dati ed in base ad un accordo internazionale. Questo accordo dovrebbe contenere norme adeguate in relazione ad alcuni profili: limitazione delle finalità, non eccedenza dei dati raccolti, tempi di conservazione, informativa, diritto di accesso, previsione di un'autorità di controllo indipendente.

44.2. Informativa

Al tema dell'informativa e, in particolare, all'esigenza di migliorarne insieme la chiarezza e l'efficacia dei contenuti è stata dedicata un'altra risoluzione, in cui è stato affermato che l'informativa deve essere il più possibile chiara e concisa. Le autorità garanti si sono impegnate ad elaborare un modello *standard* che soggetti pubblici e privati potranno utilizzare per fornire informazioni essenziali sul trattamento con un linguaggio semplice, inequivocabile e diretto. Nel modello deve essere specificato il soggetto che tratta i dati e le finalità per le quali li tratta. Inoltre, deve essere spiegato come contattare tale soggetto e quali sono i diritti riconosciuti agli interessati e deve indicarsi l'autorità di controllo alla quale rivolgersi. Nell'informativa sintetica saranno poi forniti gli elementi per reperire ulteriori informazioni, secondo le esigenze del singolo interessato. Questa informativa deve essere fornita prima di richiedere qualsiasi dato personale e, per quanto riguarda il settore telematico, possibilmente in maniera automatizzata (su questo punto la Conferenza si è richiamata espressamente al lavoro svolto in materia dal Gruppo di cui all'art. 29 della direttiva europea n. 95/46/CE).

Le autorità hanno anche ribadito la propria disponibilità a collaborare con tutti i soggetti impegnati a migliorare la comunicazione fra imprese, pubblica amministrazione e cittadini, in un'ottica di trasparenza e di rispetto per la vita privata.

44.3. Organizzazioni internazionali

Una terza risoluzione si è occupata degli organismi internazionali e sovranazionali. Le autorità hanno invitato questi ultimi ad impegnarsi nell'osservare le regole compatibili con i principi fissati a livello internazionale nella materia della tutela della *privacy* (direttive Ue, raccomandazioni del Consiglio d'Europa, linee-guida Ocse), tra le quali la creazione di autorità di controllo interne, effettivamente indipendenti sul piano operativo. È poi necessaria, a giudizio delle autorità garanti, una valutazione preliminare dell'impatto in materia di riservatezza di qualsiasi norma o regolamento elaborato da un organismo internazionale e che abbia riflessi sulla legislazione dei singoli stati.

44.4. Aggiornamenti automatici di **software**

Gli aggiornamenti automatici di *software* hanno formato oggetto di un'altra risoluzione adottata a Sydney. In particolare è stato rilevato che le case produttrici di *software* ricorrono sempre più a meccanismi non trasparenti per trasferire aggiornamenti di *software* nei computer dei singoli utenti. Per evitare i rischi derivanti dalla possibilità di leggere e raccogliere dati personali memorizzati nel *computer* dei singoli utenti senza che questi ne abbiano consapevolezza, e per non esporre gli utenti stessi al rischio di commettere involontariamente un illecito, la Conferenza ha invitato le società:

- ad aggiornare il *software on line* solo su richiesta dell'utente, secondo procedure trasparenti;

- a non richiedere dati personali se non assolutamente necessari per effettuare l'aggiornamento, anche in tal caso solo con il consenso informato dell'utente.

La risoluzione ha inoltre sottolineato l'opportunità di offrire forme alternative di distribuzione del *software* (ad esempio, attraverso specifici *Cd-Rom*).

44.5. **Radio frequency identification**

L'ultima risoluzione, adottata non contestualmente allo svolgimento della Conferenza, si è occupata del tema dell'identificazione attraverso radiofrequenze *(Rfid)*.

I dispositivi basati su tale sistema, che vengono utilizzati sempre più spesso, comportano significative implicazioni anche in materia di tutela della *privacy*. La tecnologia impiegata, infatti, potrebbe ricostruire le attività di singoli individui e istituire collegamenti fra le informazioni raccolte e banche dati preesistenti.

Per tali motivi le autorità garanti hanno invitato i titolari di trattamenti ad utilizzare, laddove possibile, approcci alternativi rispetto alla raccolta di dati personali o alla profilazione della clientela. Quando tale tecnologia risulta indispensabile, per scopi legittimi, la raccolta deve essere comunque chiara e trasparente, i dati devono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati raccolti e conservati solo fino al raggiungimento di tale scopo, e gli interessati dovrebbero avere la possibilità di cancellare i dati e di disattivare o distruggere le etichette *Rfid*. Viene inoltre sottolineata l'importanza di tener conto dei principi enunciati in materia di dati personali anche nella fase di progettazione e nell'utilizzazione di prodotti cui siano applicabili tecnologie basate su *Rfid*.

IL GARANTE

VI - L'attività del Garante

45 La collaborazione fornita dal Garante alle attività del Parlamento e del Governo

45.1. L'Autorità e le attività di sindacato ispettivo e di indirizzo del Parlamento

Anche nel corso del 2003 l'Autorità ha seguito con attenzione l'attività di sindacato ispettivo e di indirizzo esercitata dal Parlamento, in relazione agli aspetti di specifico interesse in materia di protezione dei dati personali, fornendo al Governo, laddove richiesto, i chiarimenti e le indicazioni necessarie.

Sono stati pure inviati al Governo gli elementi richiesti in relazione ad alcuni atti di sindacato fra i quali, in particolare, un'interrogazione a risposta immediata presentata dall'on. Folena (3-02832), relativa all'acquisizione da parte degli Usa dei dati dei passeggeri conservati nella banca dati dell'Alitalia (*Nota* 4 novembre 2003). In tale occasione il Garante ha ricordato, fra l'altro, che la richiesta formulata dalle autorità americane alle compagnie aeree di accedere a tutti i dati contenuti nel *Pnr* (*Passenger name record*, su cui cfr. *supra*, parag. 36.) relativi ad individui diretti, provenienti o in transito verso gli Stati Uniti, va valutata alla stregua delle disposizioni comunitarie in materia (in particolare, l'art. 25 della direttiva n. 95/46/CE).

Va infine ricordato che due mozioni analoghe della maggioranza (1-00304 Leone ed altri) e dell'opposizione (1-00215 Folena ed altri), poi approvate all'unanimità dal Parlamento il 14 gennaio 2004, con riferimento alle problematiche inerenti alla conversione del d.l. n. 354/2003 hanno impegnato il Governo a rimuovere tutte le norme potenzialmente lesive dei diritti di riservatezza e a regolamentare in modo più efficace il trattamento dei dati di traffico della telefonia mobile, al fine di tutelare il diritto degli individui (sul punto, cfr. più diffusamente parag. 1.11.).

45.2. L'attività consultiva del Garante sugli atti del Governo

L'articolo 154, comma 4, del d.lg. n. 196/2003 (che riproduce l'art. 31, comma 2, della legge n. 675/1996) stabilisce che il Presidente del Consiglio dei ministri e ciascun ministro debbano consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere in materia di protezione di dati personali.

In relazione a tale competenza, nel corso dell'anno il Garante ha espresso vari pareri anche in importanti materie, fra cui, in particolare, quelli riguardanti:

- due schemi di regolamento in attuazione della legge n. 189/2002 concernenti, l'uno, il riordino del regolamento di attuazione del testo unico in materia di immigrazione e condizione dello straniero (d.P.R. n. 394/1999) e, l'altro, lo sviluppo e la razionalizzazione dei sistemi informativi delle pubbliche amministrazioni coinvolte nell'applicazione della legge, in particolare ai fini del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (*Parere* 4 marzo 2004);

Il permesso di soggiorno elettronico

- lo schema di decreto interministeriale (Ministri per l'innovazione e le tecnologie e dell'interno) che disciplina il permesso di soggiorno elettronico. Dopo un primo parere del 15 ottobre 2003, a seguito di incontri tecnici tra rappresentanti dell'Autorità e del Ministero dell'interno, in cui sono stati forniti chiarimenti sul piano applicativo, il Garante ha formulato un secondo parere il 4 marzo 2004 con il quale ha, fra l'altro, indicato gli interventi necessari per garantire gli interessati in occasione della raccolta delle impronte digitali e, in particolare, nel caso di inserimento di dati biometrici nel documento elettronico. Al riguardo, l'Autorità ha anche confermato la propria disponibilità a proseguire la cooperazione con il Ministero al fine di approfondire i problemi ed i rischi derivanti dalle differenti tecniche di identificazione e di autenticazione, descritte dai Garanti europei a proposito dei dati biometrici nel parere del 1° agosto 2003 (su cui, *supra*, parag. 38.). Ciò anche allo scopo di individuare le cautele necessarie nella fase di attivazione del documento elettronico e di consegna dei documenti o di accesso selezionato ai dati, nonché le migliori garanzie di sicurezza disponibili. L'esito di tali approfondimenti potrebbe essere trasfuso nelle misure e negli accorgimenti che, in materia di dati biometrici, devono essere individuati dal Garante ai sensi dell'art. 55 del Codice;

- lo schema di decreto del Presidente della Repubblica recante il regolamento di disciplina dell'accesso al servizio di informatica giuridica del Centro elettronico di documentazione (C.e.d.) della Corte di cassazione (*Parere* 27 febbraio 2004).

- lo schema di regolamento (Ministri per la funzione pubblica e dell'interno) di gestione dell'Indice nazionale delle anagrafi (I.n.a.), in attuazione dell'art. 2-*quater* del decreto legge 27 dicembre 2000, n. 392, convertito dalla legge n. 26/2001 (*Parere* 13 febbraio 2004);

- uno schema di decreto dirigenziale del Ministero della giustizia, di attuazione in via parziale e transitoria dell'art. 39 del d.P.R. 14 novembre 2002, n. 313 (testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti), concernente la consultazione del casellario giudiziale da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi (*Parere* 28 gennaio 2004).

In occasione degli incontri di lavoro che hanno preceduto la redazione dello schema di decreto, l'Autorità aveva constatato il carattere transitorio della soluzione elaborata, in attesa di una regolamentazione definitiva della procedura di accesso diretto ai sensi dell'art. 39 del d.P.R. n. 313/2002. Nel parere del 28 gennaio 2004 è stata sottolineata la necessità che l'accesso ai dati giudiziari registrati nel casellario giudiziale, nonché il successivo utilizzo da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi, siano consentiti nel rispetto dei limiti previsti dallo stesso d.P.R. n. 313/2002 e in misura proporzionata alle finalità da perseguire.

Consultazione ed utilizzo dei dati del casellario giudiziale da parte delle p.a.

Le osservazioni del Garante hanno tenuto conto anche del ricorso presentato da un privato interessato all'aggiudicazione di un appalto, che lamentava l'utilizzo da parte della pubblica amministrazione, ai fini dell'esclusione dalla gara, di dati contenuti in un certificato generale del casellario, contestando che quest'ultimo potesse essere rila-

sciato ad un soggetto pubblico, considerata l'equiparazione dei certificati rilasciabili ai privati interessati e alle pubbliche amministrazioni. L'Autorità ha ritenuto infondate le tesi del ricorrente, alla luce della normativa vigente, che consente alla pubblica amministrazione di acquisire dal casellario i dati necessari per accertamenti d'ufficio o per il controllo delle autodichiarazioni presentate dai privati (il ricorrente ha impugnato la decisione davanti all'autorità giudiziaria: v. pure *supra*, parag. 27.). Tuttavia, sia nella decisione del ricorso, sia nel parere del 28 gennaio scorso, il Garante ha richiamato l'attenzione del Ministero della giustizia sulla necessità di completare al più presto ed in via definitiva la messa a punto del sistema di consultazione in via telematica del casellario da parte delle pubbliche amministrazioni e dei gestori di pubblico servizio, superando l'attuale fase transitoria così da consentire un utilizzo selettivo delle informazioni necessarie nell'ambito dello specifico procedimento avviato;

- lo schema di d.P.C.M. recante regole tecniche per la generazione, apposizione e verifica delle firme digitali, adottato ai sensi del testo unico in materia di documentazione amministrativa (d.P.R. n. 445/2000), in sostituzione del d.P.C.M. 8 febbraio 1999 (Parere 19 novembre 2003);

- lo schema di regolamento recante disposizioni per il diritto di accesso agli atti delle imprese di assicurazione, in attuazione dell'art. 3 della l. 5 marzo 2001, n. 57 (*Parere* 13 agosto 2003). A tal proposito, si sottolinea che le indicazioni fornite dal Garante in merito alla necessità di mantenere chiara la distinzione tra il diritto di accesso agli atti delle imprese di assicurazione ed il diritto di accesso ai dati di cui al d. lg. n. 196/2003, sono state recepite nel d.m. 20 febbraio 2004, n. 74 (v. in particolare l'art. 1, comma 2);

- lo schema del regolamento di attuazione ed organizzazione della banca dati relativa ai minori dichiarati adottabili istituita dall'articolo 40 della legge 28 marzo 2001, n. 149 (*Parere* 11 luglio 2003); il regolamento è stato poi adottato con d.m. 24 febbraio 2004, n. 91 in *Gazzetta Ufficiale* 9 aprile 2004, n. 84;

Carta nazionale dei servizi

- lo schema di d.P.R. recante il regolamento sulle caratteristiche e le modalità per il rilascio della Carta nazionale dei servizi (*Parere* 9 luglio 2003). In tale parere il Garante ha richiesto un'attenta valutazione, da parte dell'amministrazione procedente, circa la pertinenza dei dati da inserire nella carta, che in ogni caso non potrebbero essere dati sensibili; si è inoltre espresso in favore della loro utilizzazione da parte delle amministrazioni esclusivamente a fini di identificazione dell'interessato e di legittimazione al servizio offerto. L'Autorità ha poi richiesto che le disposizioni dello schema relative all'utilizzo dell'Indice nazionale delle anagrafi (Ina) fossero rese coerenti con la funzione propria di tale indice, che è quella di mero strumento per l'individuazione agevole del comune di residenza degli interessati e non di sostanziale anagrafe nazionale;

- lo schema di regolamento per la tenuta dei fascicoli personali della carriera diplomatica ai sensi dell'art. 113 del d.P.R. n. 18/1967 (*Parere* 19 giugno 2003). Il regolamento è stato poi adottato con il decreto del Ministro degli affari esteri 13 ottobre 2003, n. 311;

- lo schema di regolamento concernente le modalità di istituzione e tenuta presso la Presidenza del Consiglio dei ministri della banca dati informatica dei componenti degli organi di amministrazione attiva, consultiva e di controllo dello Stato e degli enti pubblici a carattere nazionale e delle relative modalità di nomina (*Parere* 9 aprile 2003);

- lo schema di regolamento in materia di estensione delle disposizioni antiriciclaggio ad attività non finanziarie particolarmente suscettibili di utilizzazione a fini di riciclaggio, in attuazione dell'art. 4, comma 8, del d.lg. 25 settembre 1999, n. 374 (*Parere* 12 marzo 2003).

46 La cooperazione a livello europeo

46.1. L'attività del Gruppo istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE

Nel 2003 è proseguita la tendenza ad un ampliamento del ruolo e delle competenze del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

Intenso è stato il lavoro svolto da tale Gruppo per interpretare, segnalare ed indirizzare l'attività della Commissione europea in relazione all'applicazione dei principi della direttiva generale in materia. Il rischio che potrebbe presentarsi al riguardo è che il Gruppo sia però considerato, anche presso uffici comunitari, alla stregua di un gruppo di lavoro specializzato, anziché un organismo consultivo indipendente.

A causa dell'attuale esiguità della struttura di segretariato, che svolge una funzione di supporto al Gruppo, la predisposizione degli elementi per la discussione e la successiva valutazione delle proposte della Commissione è stata a volte compiuta direttamente dagli uffici della stessa Commissione che avevano chiesto l'avviso del Gruppo. I pareri sono stati, inoltre, talora sollecitati non già in fase di predisposizione di misure comunitarie, bensì a volte dopo la presentazione delle relative proposte al Consiglio.

In proposito, un'iniziativa della Commissione tuttora in corso di elaborazione, sulla quale il Gruppo dei garanti europei ha fornito un parere preliminare, ha riguardato la proposta di una direttiva in materia di protezione dei dati dei lavoratori. Nel settore della protezione dei dati sono inoltre da segnalare le proposte della Commissione relative all'introduzione di modelli per il rilascio di visti e permessi di soggiorno, nonché di passaporti che prevedono l'inserimento obbligatorio di dati biometrici.

In ogni caso, come detto, il ruolo dei garanti europei in ambito comunitario ha acquisito un rilievo più forte.

Il Gruppo, che fino al 16 marzo scorso è stato presieduto dal prof. Rodotà, è stato più volte coinvolto ufficialmente nell'ambito di vari incontri, seminari, audizioni e lavori parlamentari, coordinati dal Parlamento europeo per discutere ed approfondire temi di particolare rilevanza: è quanto avvenuto, ad esempio, in relazione a

numerose proposte volte ad intensificare la creazione di basi di dati a livello europeo e a rendere accessibili, al di là delle previsioni delle singole convenzioni istitutive, i trattamenti di dati effettuati nell'ambito della cooperazione di polizia e giudiziaria.

Alla luce di ciò, potrebbe diventare necessario ridefinire la collocazione istituzionale del Gruppo nel quadro della complessa compagine comunitaria, come pure del suo segretariato. Questo anche in considerazione delle numerose proposte in corso di elaborazione su materie di confine tra il primo ed il terzo pilastro, la cui predisposizione compete ad uffici della Commissione diversi da quelli ai quali è affidata l'attuazione della direttiva n. 95/46/CE (D.g. mercato interno).

Nel corso del 2003, l'attività del Gruppo ha riguardato un'ampia gamma di tematiche, attinenti sia ai diversi ambiti di applicazione delle direttive n. 95/46/CE e n. 2002/58/CE, sia al trasferimento dei dati personali verso Paesi terzi.

Il Gruppo ha dedicato particolare attenzione alle richieste di alcuni Stati (Australia, Canada, Stati Uniti) di ottenere da parte delle compagnie aeree i dati personali dei passeggeri in viaggio da e verso il loro territorio. Tali richieste sono state motivate con la necessità di prevenire il terrorismo e di facilitare i compiti delle autorità doganali. Il Gruppo, nel ribadire l'esigenza di un approccio equilibrato alla lotta contro il terrorismo (v. Pareri n. 10/2001 e n. 6/2002), ha sottolineato la necessità di rispettare e di applicare correttamente anche in tale settore i principi sulla protezione dei dati personali (per maggiori dettagli sul punto, v. *supra*, parag. 36.).

Si ricorda, infine, un primo documento di lavoro (WP 86 del 23 gennaio 2004) sui dispositivi proposti dal consorzio *Trusted Computing Group* per incentivare la sicurezza delle transazioni elettroniche mediante strumenti non solo *software*, ma anche *hardware*.

46.2. La partecipazione ad altri comitati e gruppi di lavoro

Il Gruppo di Berlino

Sempre nell'ambito della definizione delle forme di collaborazione e scambio tra le autorità di protezione dei dati, va ricordata l'attività dell'*International Working Group on data protection in telecommunications* (cd. Gruppo di Berlino), in quanto sede di discussione ed approfondimento, non solo a livello europeo, su temi quali Internet, cifratura e comunicazioni elettroniche, tra esperti in materia di tecnologie ed informazione.

Nella riunione di Berlino del 2-3 settembre 2003 sono stati discussi numerosi temi, fra cui meritano di essere menzionati in particolare il *media privilege*, la *Radio frequency identification* (identificazione attraverso radio frequenze), il tempo di conservazione dei dati di traffico e lo *spamming*.

Con riferimento ai *media*, sono stati analizzati gli esiti dei questionari compilati a livello nazionale e sono state presentate le innovazioni introdotte in materia nella normativa nazionale dal d.lg. n. 196/2003.

È stato inoltre illustrato il contenuto del provvedimento del Garante relativo ai *Multimedia message systems (Mms)*, il quale potrà contribuire all'elaborazione di una dichiarazione che il Gruppo adotterà durante la prossima riunione.

Con riguardo alla *Radio frequency identification*, il Gruppo ha elaborato un documento che è successivamente servito come base per la risoluzione adottata dalle autorità di garanzia riunite a Sydney nel settembre del 2003 (v. *supra*, parag. 44.5.).

I *Complaints Handling Workshop*

Sono proseguiti gli incontri (cd. seminari in materia di *Complaints Handling*) organizzati ai fini dello scambio di informazioni e della definizione di linee operative comuni per la trattazione delle segnalazioni e dei ricorsi presentati alle autorità nazionali per la protezione dei dati, con particolare riguardo ai casi che, per la loro rilevanza o per la natura delle parti interessate, travalicano l'ambito nazionale.

Ai due incontri, tenutisi rispettivamente a Roma (VIII *Complaints Handling Workshop*, 23-24 ottobre 2003) ed a Stoccolma (IX *Complaints Handling Workshop*, 11-12 marzo 2004), hanno partecipato oltre quarantacinque delegati dei Paesi Ue e di quasi tutti i Paesi in via di adesione all'Unione.

Nel seminario di Roma è stata dedicata specifica attenzione al tema della biometria, con la discussione dei risultati di un questionario presentato dalla delegazione portoghese. Il tema della ricerca farmacologica e delle modalità di prestazione del consenso da parte dei pazienti e/o candidati è stato esaminato in relazione a un questionario predisposto dalla delegazione belga. La delegazione italiana ha impostato la discussione di due casi concreti di bilanciamento di interessi, evidenziando numerose difformità negli approcci seguiti dai singoli Paesi in rapporto, soprattutto, all'esistenza o meno di norme settoriali che indichino già criteri operativi. Sono stati pure presentati gli aggiornamenti relativi all'indagine conoscitiva condotta dal Garante nel 2002 sui meccanismi utilizzati dalle maggiori imprese italiane per trasferire dati personali (di clienti e/o dipendenti) verso Paesi terzi. La discussione ha poi preso in considerazione possibili linee-guida per assicurare che i seminari in materia di *"Complaints Handling"* continuino ad essere focalizzati su casi concreti e su positive modalità operative già in sperimentazione.

Alcuni dei temi affrontati durante l'incontro di Roma sono stati approfonditi in occasione del seminario di Stoccolma, con particolare riguardo alla biometria. Ciascuna delegazione ha, infatti, presentato un caso nazionale emblematico, prospettando le soluzioni volta per volta individuate. La delegazione portoghese ha segnalato l'esistenza di un "decalogo" emanato dall'autorità nazionale di protezione dati per regolamentare l'impiego di dispositivi biometrici ai fini del controllo dell'accesso a locali pubblici e/o privati. Sono state analizzate, inoltre, le strategie seguite dalle varie autorità nazionali per sollecitare l'attenzione dell'opinione pubblica. In particolare, l'autorità svedese e quella del Land di Brandeburgo hanno illustrato l'attività di sensibilizzazione ed educazione svolta rispetto ai cd. incaricati della protezione dei dati, cioè i soggetti che i titolari possono designare ai sensi dell'art. 18(2) della direttiva n. 95/46/CE con il compito, fra l'altro, di tenere un registro dei trattamenti, evitando così l'invio della notificazione all'autorità di controllo. I partecipanti hanno anche esaminato le priorità eventualmente individuate dalle rispettive autorità in relazione alle attività ispettive. Infine, è proseguita la discussione sulla configurazione futura dei seminari e, in particolare, sullo spostamento del nucleo centrale di attività dalla trattazione di casi che coinvolgono più Paesi al confronto su casi concreti affrontati dalle singole autorità. Un documento in merito è stato presentato per la discussione all'*European Spring Conference of Data Protection Commissioners* (Rotterdam, 21-23 aprile 2004).

46.3. EUROPOL: l'attività dell'Autorità comune di controllo e i primi casi di contenzioso

L'Autorità comune di controllo prevista dall'art. 24 della Convenzione Europol ha continuato la sua attività di verifica e controllo sulla gestione degli archivi Europol, che dal luglio 1999 comprendono gli archivi di analisi.

Tale Autorità ha seguito con attenzione i progetti di negoziato sottoposti dal Direttore dell'Europol per ottenere il consenso ad iniziare le trattative volte allo scambio di dati con alcuni Paesi terzi. Sono stati inoltre espressi pareri in merito all'apertura di *file* di analisi e alla nozione di dato personale nel contesto Europol, compresa la possibilità di includervi anche le persone decedute.

L'Autorità comune si è inoltre occupata degli sviluppi applicativi dell'accordo Europol-Stati Uniti per la trasmissione di dati personali a seguito della ristrutturazione del *Department of Homeland Security* ed ha espresso le sue preoccupazioni riguardo ai lavori per la revisione dei sistemi di informazione esistenti nel cd. terzo pilastro, che si svolgono presso il Consiglio dell'Unione europea ed ai quali partecipa il segretariato comune delle autorità comuni di controllo in tale ambito.

Nell'ottobre del 2003 sono stati rinnovati diversi componenti dell'Autorità comune di controllo e del Comitato ricorsi, per scadenza del rispettivo mandato, ed è iniziata un'attività di definizione delle regole per l'accesso agli atti e ai documenti detenuti dall'Autorità comune. Ciò anche in relazione all'apertura di uno specifico sito *web (http://europoljsb.ue.eu.int/home/default.asp?lang=it)* ed alla scelta dei documenti da mettere a disposizione del pubblico (oltre al rapporto di attività e al testo dei pareri adottati, anche informazioni sulla composizione dell'Autorità, sui compiti attribuiti, nonché sul funzionamento del comitato ricorsi).

Una discussione approfondita è stata dedicata alla bozza di accordo predisposta per lo scambio di dati ed informazioni tra Europol ed Eurojust.

Alle riunioni erano presenti, in veste di osservatori, i rappresentanti degli organismi incaricati della protezione dei dati dei Paesi in via di adesione all'Unione europea.

È stata anche svolta l'annuale ispezione alla sede dell'Europol incentrata sugli archivi di analisi e sugli sviluppi tecnologici del sistema, ed è stata effettuata una visita di controllo per verificare il grado di adempimento di Europol alle raccomandazioni impartite a seguito dell'ispezione.

La prima relazione di attività dell'Autorità comune

La prima relazione di attività, riguardante il periodo ottobre 1998-ottobre 2002, è stata ufficialmente presentata dal Presidente agli organi competenti ed è stata resa disponibile nelle diverse versioni linguistiche, sia in formato cartaceo (cfr. l'allegato alla presente Relazione), sia in formato elettronico sul sito *web* dell'Autorità comune.

Va, infine, ricordata la modifica della Convenzione Europol adottata dal Consiglio dei ministri giustizia e affari interni, che amplia il ruolo di Europol rispetto agli specifici scopi conferitigli inizialmente dalla Convenzione.

46.4. Il sistema informativo doganale

Il Sistema informativo automatizzato comune (Sistema informativo doganale-S.i.d.) è stato istituito dalla Convenzione sull'uso dell'informatica nel settore doganale del 26 luglio 1995, elaborata in base all'articolo K3 del Trattato Ue e ratificata dall'Italia con la legge 30 luglio 1998, n. 291.

La Convenzione mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'Ue, specie attraverso lo scambio di dati personali. A tal fine è appunto prevista la creazione del Sistema informativo doganale, che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La Convenzione istituisce, inoltre, un'autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati, che ha iniziato i suoi lavori nel corso della primavera del 2002. Nel periodo in esame l'Autorità ha definito il proprio regolamento interno e i metodi di lavoro. Ha espresso, inoltre, il parere sull'istituzione di un archivio di identificazione dei fascicoli a fini doganali (cd. Fide). Nelle ultime riunioni, l'Autorità comune di controllo si è occupata in particolare di definire gli aspetti relativi all'effettuazione di ispezioni *in loco*.

46.5. Eurodac

A seguito della nomina e costituzione dell'Autorità di controllo indipendente, avvenuta con la decisione del Parlamento e del Consiglio del 22 dicembre 2003, l'Autorità comune di controllo Eurodac per il confronto delle impronte digitali di coloro che richiedono l'asilo ha esaurito le sue funzioni.

La nuova Autorità di controllo su Eurodac

Il controllo su tale sistema informativo, costituito e gestito dalla Commissione, spetterà infatti in via definitiva alla predetta autorità di controllo indipendente prevista dall'art. 286, par. 2, del Trattato di Amsterdam, che ha il compito di controllare la correttezza dei trattamenti di dati effettuati dalle istituzioni e dagli organismi dell'Ue.

La nuova cornice normativa in materia di protezione dati è stata illustrata dai servizi giuridici della Commissione nel corso dell'ultima riunione dell'Autorità comune di controllo, in cui sono state esposte, in particolare, le funzioni e i legami fra i differenti organi di controllo competenti in materia. In tale occasione sono stati pure presentati i regolamenti che stabiliscono i criteri e i meccanismi di determinazione dello Stato membro responsabile dell'esame di una domanda di asilo e le modalità attuative, in particolare il funzionamento della rete DubliNET.

È stato inoltre evidenziato che la banca dati dell'Unità centrale aumenta costantemente di dimensioni, e che vengono alla luce anche doppie e triple "identificazioni positive", ciò che prova la reale utilità del sistema. La Commissione ha sottolineato l'alta qualità dei dati contenuti nella banca dati centrale ed ha evidenziato la necessità di un'analoga qualità in ambito nazionale al momento della raccolta delle impronte digitali inviate ad Eurodac per l'accertamento.

47 L'attività dell'Autorità nell'ambito del Consiglio d'Europa

47.1. I gruppi di esperti

Il Protocollo addizionale alla Convenzione n. 108 del 1981, che prevede l'istituzione di autorità di controllo indipendenti con compiti di verifica e controllo dei trattamenti, e disciplina i flussi transfrontalieri di dati, aperto alla firma l'8 novembre 2001, avendo raggiunto il numero di ratifiche necessario, entrerà in vigore il 1° luglio 2004.

L'Italia è tra i Paesi firmatari, ma non ha ancora presentato in Parlamento il disegno di legge di ratifica.

Per quanto riguarda le modifiche alla ricordata Convenzione n. 108 per consentire alle Comunità europee di aderirvi, l'Italia non ha firmato il relativo Protocollo emendativo. Essendo necessaria l'accettazione degli emendamenti da parte di tutti i Paesi dell'Unione europea, tali modifiche non sono quindi ancora entrate in vigore.

Nel quadro dell'attività del Consiglio d'Europa meritano di essere menzionati i lavori dei cd. gruppi di esperti: il Comitato CJ-PD, nato nell'ambito del Comitato per la cooperazione giudiziaria e soppresso a seguito del processo di razionalizzazione delle risorse utilizzabili, è riuscito comunque, nel corso della sua ultima riunione, svoltasi nel dicembre 2003, a portare a compimento i lavori sulle linee guida per l'uso delle carte intelligenti *(smart card)*.

Il Comitato T-PD

Il Comitato T-PD cd. convenzionale, in quanto costituito direttamente dalla Convenzione n. 108 e quindi non sopprimibile per decisione amministrativa, nell'unica riunione plenaria svoltasi anch'essa nel mese di dicembre 2003, si è trovato a valutare le problematiche derivanti dalla soppressione del CJ-PD e, in particolare, le modalità di prosecuzione dei lavori sul trattamento di dati biometrici, che il CJ-PD non ha potuto completare.

Proprio a causa dell'inserimento nei suoi lavori delle problematiche legate alla biometria, il TP-D ha poi dovuto rivedere le priorità stabilite per il 2003 e per il 2004, programmando un approfondimento sui seguenti temi:

- l'applicazione dei principi della Convenzione in relazione agli sviluppi tecnologici. Il Comitato si propone così di esaminare meglio, alla luce della Convenzione, come un indirizzo di posta elettronica o il numero di un telefono cellulare sia da considerare "dato personale". Intende inoltre valutare i rischi che derivano dalla diffusione di nuove tecnologie (molteplicità dei fini, conservazione dei dati da parte dei "nuovi media") come pure le opportunità che ne possono discendere in merito alla protezione dei dati personali (PETs, tecnologie non invasive, ecc);

- l'applicazione dei principi di protezione dei dati ad Internet, in relazione ai quali il TP-D ha preparato un progetto di mandato per uno studio preliminare da far effettuare ad un consulente.

48 Altre iniziative in ambito internazionale: Ocse

Nel periodo di riferimento il Garante ha continuato a seguire i lavori del *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse, sottogruppo del *Committee for Information Computer and Communication Policy (Iccp)*.

Fra i problemi di maggior rilievo affrontati negli incontri svoltisi nel 2003 in relazione al trattamento dei dati personali, si debbono ricordare l'attuazione delle linee-guida sulla sicurezza, lo *spamming*, la biometria, e la creazione di un apposito gruppo che si occuperà di sicurezza nei viaggi internazionali *(travel security)*, gruppo a cui parteciperà questa Autorità. Le conclusioni raggiunte in sede Ocse su tali temi sono già state esposte in appositi paragrafi della *Relazione*, ai quali pertanto si rinvia per un'analisi dettagliata (v. parag. 41.1. e 41.2.).

49 Il sistema di informazione Schengen (Sis)

Nel corso dell'anno sono state sottoposte al Garante, quale autorità di controllo sulla sezione nazionale del Sistema informativo Schengen (Sis), numerose richieste di verifica in merito all'eventuale o corretta registrazione, negli archivi del Sis, di dati personali dei soggetti interessati ed alla liceità dei relativi trattamenti. Si tratta, in gran parte, di domande che attengono al diniego di visto, per lo più adottato a causa di segnalazioni, ai fini della non ammissione nella cd. area Schengen, di persone nei cui confronti sono stati emessi provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno (espulsione, respingimento alla frontiera).

Si è registrato anche quest'anno un notevole incremento delle richieste pervenute, da attribuire pure alla procedura di regolarizzazione di cittadini extracomunitari introdotta dalla legge n. 189/2002; le richieste provengono soprattutto da Paesi dell'Est europeo e, in particolare, dalla Romania.

Nell'arco temporale che va dal 1° gennaio 2003 al 31 marzo 2004 le richieste sono state 480, di cui 464 già definite.

Per svolgere al meglio i propri compiti e fronteggiare più rapidamente anche le domande di chiarimenti sulla normativa di riferimento, nel febbraio 2003 il Garante ha nuovamente riassunto l'esatto ambito delle proprie competenze: ha così precisato che gli interessati possono rivolgere a questa Autorità richieste di verifica dei dati che li riguardano inseriti nel Sis, ovvero di aggiornamento, di rettifica o di cancellazione dei medesimi dati. Al Garante, invece, non sono conferiti compiti di adozione, revoca o controllo dei provvedimenti amministrativi che sono alla base delle segnalazioni contenute nel Sis.

Per rimediare poi a problemi insorti nei casi in cui erano state segnalate usurpazioni d'identità o omonimie, è stata ulteriormente sperimentata nel 2003, in colla-