cookies ed altri dispositivi simili;
- la riaffermazione dell'obbligo di cancellare o rendere anonimi i dati relativi al traffico non più necessari ai fini della trasmissione di una comunicazione e l'autorizzazione della loro memorizzazione solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione.
- l'introduzione della nozione di *dati relativi all'ubicazione diversi dai dati relativi al traffico* e la definizione delle condizioni che ne possono legittimare il trattamento. Si tratta di dati che le reti mobili digitali possono avere la capacità di trattare e che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni. Questi dati vengono utilizzati per fornire servizi a valore aggiunto, come ad esempio i servizi di informazioni individuali sul traffico e di radioguida.

In particolare, due scelte contenute originariamente nella proposta della Commissione sono state confermate dal Consiglio: si tratta della scelta del consenso preliminare ai fini dell'inserimento dei dati personali in elenchi telefonici (art.12) che comporta, per gli abbonati, il diritto di determinare se i loro dati personali possano essere pubblicati in un elenco e, in caso affermativo, quali debbano figurarvi. La ragione della scelta si basa sulla considerazione che per i nuovi servizi di comunicazione elettronica come il *Gsm* e la posta elettronica non risulta più opportuno dare per scontato che gli utenti di tali servizi devono figurare negli elenchi pubblici in modo automatico, cioè in assenza di ulteriore loro determinazione.

La seconda scelta condivisa concerne la protezione contro le comunicazioni indesiderate effettuate, anche a mezzo della posta elettronica (inclusi *Sms* e *Mms*) a fini di *"direct marketing"*.

Questo comporta il divieto di inviare messaggi elettronici non richiesti tranne nei confronti degli abbonati che abbiano dichiarato di voler ricevere tali messaggi elettronici (art.13).

La direttiva 2002/58/CE in questo caso armonizza a livello dei quindici Stati membri il criterio del consenso preventivo (*opt in*) già introdotto in alcuni Stati, tra cui l'Italia, come criterio che legittima il trattamento. Come chiarito nella direttiva, infatti, tali forme di comunicazioni commerciali indesiderate possono da un lato essere relativamente facili ed economiche da inviare e dall'altro imporre un onere e/o un costo al destinatario. Inoltre, in taluni casi il loro volume può causare difficoltà per le reti di comunicazione elettronica e le apparecchiature terminali. Per tali forme è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi.

Altre novità nel diritto comunitario e nel settore giustizia-affari interni

80 Profili generali

Nel confermare quanto già segnalato nella precedente Relazione riguardo al venir meno, in ambito europeo, delle occasioni di dibattito e discussione istituzionali nel settore della protezione dei dati, nel 2002 si è notata, più in generale, una disattenzione a tale tema da ricollegarsi in gran parte agli effetti dei tragici eventi dell'11 settembre, che hanno posto all'attenzione di tutte le istituzioni comunitarie il tema del terrorismo e, quindi, della lotta alla criminalità ed alla *cybercriminalità*, richiedendo alle stesse la concentrazione di gran parte delle risorse nello studio ed elaborazione di strumenti efficaci a contrastare il fenomeno. Ciò in contrasto con l'introduzione di uno specifico articolo nella Carta dei diritti fondamentali (art. 8) ed il conseguente pieno riconoscimento del ruolo che la protezione dei dati personali assume nella realizzazione e sviluppo dell'integrazione europea attraverso l'inserimento del diritto alla protezione dei dati personali nel testo di trattato che la Convenzione europea sta elaborando.

Come si è già evidenziato, non vi sono più state convocazioni del gruppo di lavoro protezione dati del Consiglio dell'UE, mentre il gruppo c.d. di *"terzo pilastro"*, denominato "Sistemi di informazione e protezione dei dati", è stato soppresso a seguito di una generale revisione dei gruppi operanti nel citato pilastro, pur essendovi stato il tempestivo intervento del Garante volto a rappresentare al Rappresentante permanente d'Italia presso l'UE la necessità che l'attività di revisione tenesse doverosamente conto -anche nel contesto della creazione di uno spazio di libertà, sicurezza e giustizia- del riconoscimento dell'importanza e della specificità della protezione dai dati personali, in quanto strettamente attinente ai diritti fondamentali della persona umana.

In questo quadro, necessariamente sono aumentati il ruolo e le competenze del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 della direttiva 95/46/CE, ed il lavoro da esso svolto per interpretare, segnalare e indirizzare, attraverso l'adozione di pareri, raccomandazioni ad altre iniziative, l'attività della Commissione europea (e, di riflesso, degli Stati membri) in relazione all'applicazione dei principi della direttiva generale in materia di protezione dei dati personali e delle specifiche ulteriori disposizioni per il settore delle comunicazioni elettroniche.

E' aumentata quindi -come meglio si vedrà nel paragrafo successivo- la visibilità del Gruppo stesso il quale, sotto la presidenza del Presidente del Garante italiano, è stato più volte richiesto di partecipare ad audizioni ed a pubblici incontri promossi dal Parlamento europeo per discutere ed approfondire temi di particolare rilevanza (l'Accordo sul *Safe Harbor* con gli Stati Uniti e, più di recente, i trattamenti di dati effettuati nell'ambito delle cooperazioni di polizia e giudiziaria, nonché i riflessi che l'introduzione di norme di ordine pubblico a seguito degli eventi dell'11 settembre da parte degli USA determina sulla protezione dei dati in Europa – caso APIS-PNR).

Il Gruppo, già in un parere adottato alla fine del 2001, aveva ribadito l'esigenza di un approccio equilibrato nella lotta al terrorismo, in particolare dopo gli eventi dell'11 settembre 2001, per far sì che il diritto alla sicurezza e il diritto alla *privacy* coesistano in maniera equilibrata, suggerendo pertanto di abbandonare l'equazione *"più sicurezza meno privacy"*, di evitare forme generalizzate di sorveglianza, di valutare le conseguenze delle misure antiterrorismo sulle libertà delle persone. Nel parere si sottolineava come la lotta al terrorismo non dovesse ridurre il livello di tutela dei diritti fondamentali che caratterizza ogni società democratica, ma che occorresse sempre rispettare determinate condizioni che costituiscono anche il fondamento delle società democratiche in cui viviamo: da questo punto di vista le numerose iniziative legislative e di altra natura approvate o in discussione a livello comunitario e nazionale in molti casi sembrano destinate ad avere un ambito di applicazione molto più ampio della lotta contro il terrorismo. Come esempio, nel parere del Gruppo viene citata la proliferazione di strumenti per il riconoscimento dell'identità, anche attraverso dispositivi biometrici, o la previsione dei reati di *"criminalità informatica"*, la cui definizione -a giudizio del Gruppo- è molto ampia e lascia spazio a interpretazioni non rispettose del principio di legalità.

L'introduzione di misure legislative negli USA volte ad imporre sanzioni alla compagnie aeree che operano voli da e per gli Stati Uniti qualora non forniscano in anticipo alle autorità statunitensi una serie di dati relativi ai passeggeri ed ai membri dell'equipaggio, anche attraverso l'accesso diretto ai dati trattati nei sistemi di prenotazione e controllo delle partenze (che non si limitano ai dati relativi ai tragitti da o verso gli USA, ma includono anche preferenze personali dei passeggeri abituali iscritti a programmi *"frequent flyer"* tra cui informazioni di tipo sanitario), ha nuovamente e specificamente determinato l'intervento del Gruppo che, nell'ottobre 2002, ha adottato un parere (n. 6/2002) nel quale ha ritenuto che, pur nel rispetto della sovranità degli Stati, una previsione normativa di tal genere (ed i conseguenti obblighi per i destinatari) ingenera difficoltà nell'applicazione della direttiva 95/46/CE cui le compagnie aeree che operano sul territorio comunitario sono soggette.

Successivamente, dopo un intervento della Commissione europea che ha ritenuto di poter negoziare una sorta di sostanziale accordo "ponte" con autorità amministrative USA, si è avuto un ampio dibattito nel Parlamento europeo, che ha chiesto un fermo ripensamento ed un vero negoziato su basi giuridiche solide ed appropriate. Il 25 marzo la Commissione *"Libertà pubbliche"* del Parlamento europeo ha organizzato un seminario per dibattere ulteriormente il tema con i diversi soggetti: Commissione europea, autorità americane, compagnie aeree, organizzazioni rappresentative dei consumatori/utenti. Al seminario sono intervenuti, anche in considerazione del ruolo rivestito di Presidente del Gruppo, il Presidente del Garante e, in qualità di Presidente dell'Autorità di controllo *Schengen*, il segretario generale del Garante.

Alla luce di quanto evidenziato ed anche in considerazione delle proposte finora maturate nel corso del lavori della Convenzione europea, che portano alla previsione di un nuovo articolo specificamente rivolto alla protezione dei dati personali, superando quindi la divisione tra materie di primo e terzo pilastro, potrebbe allora porsi la questione di una diversa e migliore collocazione del Gruppo stesso all'interno del quadro delle competenze comunitarie.

Per quanto concerne gli ulteriori aspetti di novità legati al diritto comunitario, si segnala poi la presentazione, nel giugno del 2002, da parte della Commissione europea di una propo-

sta di direttiva relativa al riutilizzo dei documenti del settore pubblico e al loro sfruttamento a fini commerciali.

La proposta di direttiva è stata esaminata dal gruppo di lavoro del consiglio *"Telecomunicazioni"* ed alle discussioni ha preso parte attiva, nell'ambito della delegazione italiana, l'Ufficio del Garante. Nel corso del Consiglio dei Ministri delle telecomunicazioni del 27-28 marzo 2003 sul testo della proposta è stato raggiunto un accordo politico.

L'intento alla base della direttiva è quello di agevolare il riutilizzo delle informazioni del settore pubblico al fine di favorire la crescita di un mercato di servizi informativi a valore aggiunto estesi in maniera omogenea a tutti gli stati membri dell'Unione, anche nella prospettiva della diffusione di nuove piattaforme di comunicazione. Secondo la Commissione, la realizzazione di servizi informativi a livello europeo è di fatto ostacolata dall'esistenza di norme e prassi diverse negli Stati membri in materia di tariffe, tempi di risposta, accordi di esclusiva e disponibilità generale dei dati ai fini del riutilizzo. Per favorire lo sviluppo di prodotti informativi a valore aggiunto e limitare le distorsioni della concorrenza sul mercato europeo, la Commissione si propone di definire attraverso la direttiva un quadro di garanzie, relative alla definizione di condizioni di mercato eque e trasparenti, tariffazione, tempi e modalità di risposta, compatibile con le normative nazionali, senza interferire sulle previsioni nazionali riguardanti il diritto di accesso e nel pieno rispetto delle disposizioni in materia di protezione dei dati personali.

Un'altra iniziativa legislativa promossa dalla Commissione, sulla quale è iniziata la discussione in seno al Consiglio e riguardo la quale il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ha espresso, il 2 luglio 2002, un parere preliminare, riguarda l'armonizzazione delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di credito al consumo.

Si tratta di una proposta di notevole ampiezza ed impatto, che prevede la creazione e gestione di banche dati ed introduce talune disposizioni per il trattamento dei dati, pur nella generale salvaguardia e richiamo delle disposizioni della direttiva 95/46/CE. L'Ufficio ne segue attentamente l'*iter*, anche al fine di formulare proposte emendative e soppressive di talune parti del testo proposto che potrebbero avere riflessi su emanandi provvedimenti interni (codici di deontologia).

Nel settore giustizia ed affari interni si segnala inoltre l'effettiva costituzione ed entrata in funzione di *Eurojust* e si registrano diverse richieste, dibattute nel gruppi di lavoro di terzo pilastro ed in ambito del Consiglio GAI, volte a consentire l'accesso al sistema informativo *Schengen* da parte di *Europol* e di consentire allo stesso di accedere ai dati della banca dati *Eurodac*. Sono anche allo studio i sistemi per rendere *Eurojust* parte di questi sistemi.

La cooperazione tra Autorità garanti in Europa

81 Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

Come anticipato nel precedente paragrafo, molto ampia ed attenta è stata l'attività svolta dal Gruppo, di cui il Presidente del Garante è stato riconfermato all'unanimità Presidente.

La conferma rappresenta un riconoscimento al lavoro svolto nei due anni del primo mandato, che ha visto, tra l'altro, la chiusura del negoziato tra USA ed UE riguardo alla tutela della *privacy* da assicurare ai cittadini europei i cui dati personali devono essere trasferiti oltreoceano, l'elaborazione delle linee guida sulla *privacy* in *Internet*, la presa di posizione sulla necessità di un approccio equilibrato nella lotta al terrorismo, l'emanazione di vari pareri sul genoma umano, sulle comunicazioni elettroniche, sul *cybercrime*, sul trattamento dei dati nel rapporto di lavoro.

L'attività del Gruppo nel corso del 2002 ha affrontato, in particolare, il rapporto tra sicurezza e *privacy*, l'uso dei dati genetici, l'espandersi delle nuove tecnologie a fini di controllo e sorveglianza, l'impatto della società elettronica e la tutela dei diritti fondamentali dei cittadini europei, il trasferimento di dati verso Paesi terzi, l'uso delle clausole contrattuali standard e l'approfondimento delle esigenze rappresentate dall'industria e dalle società multinazionali per avere un quadro di riferimento il più possibile uniforme rispetto ai principi ed ai criteri per effettuare il trasferimento stesso. Nella definizione del calendario dei lavori e nella definizione dei temi da approfondire si è tenuto in particolare conto del lavoro di "controllo" sullo stato d'applicazione della direttiva da parte della Commissione, cui si è fatto cenno nel par. 76.

Una parte rilevante dell'attività è stata concentrata sull'attenta valutazione delle sfide poste dalle nuove tecnologie, dallo sviluppo della società dell'informazione e in particolare di *Internet*. Si segnalano i pareri sulla "standardizzazione" della *privacy* in Europa (parere 1/2002 WP 57 del 30 maggio 2002), sull'uso di un identificativo unico negli apparecchi terminali di telecomunicazioni (parere 2/2002 WP 58 del 30 maggio 2002) ed i documenti di lavoro riguardanti: la determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento di dati personali su *Internet* da parte di siti non stabiliti nell'UE (WP 56 del 30 maggio 2002); primi orientamenti del Gruppo in merito ai servizi d'autenticazione *on line* (tema sul quale i lavori del Gruppo sono continuati ed hanno portato all'adozione di un più corposo documento di lavoro il 20 gennaio 2003 WP 68); la vigilanza sulle comunicazioni elettroniche sul posto di lavoro (WP 55 del 29 maggio 2002); il trattamento di dati personali tramite videosorveglianza, promosso dai componenti italiani del Gruppo, documento che, una volta adottato, è stato aperto alla pubblica consultazione sul sito della Commissione dedicati ai lavori del Gruppo (WP 67 del 25 novembre 2002).

Altri pareri hanno riguardato la proposta di direttiva in materia di credito al consumo (parere 3/2002 WP 60 del 2 luglio 2002, già richiamato), l'adeguatezza della protezione dei dati in Argentina (parere 4/2002 WP63 del 3 ottobre 2002), la determinazione adottata dai

Garanti europei della protezione dei dati nel corso della conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni (parere 5/2002 WP 64 dell'11 ottobre 2002). Il parere si riferisce alle richieste formulate dalle forze di polizia tendenti ad una preliminare, generalizzata, conservazione di tali dati e richiama al rispetto dei principi sanciti in materia, da ultimo, dall'articolo 15 della direttiva 2002 /58/Ce.

Nei primi mesi del 2003 il Gruppo ha adottato un parere sulla conservazione dei dati di traffico a fini di tariffazione (parere 1/2003 WP 69 del 29 gennaio 2003), proprio per chiarire gli ambiti che la citata direttiva offre alla possibilità di derogare al principio generale fissato all'articolo 6 in base al quale i dati relativi al traffico devono essere cancellati o resi anonimi al termine della comunicazione (chiamata o connessione).

Il Gruppo ha continuato ad occuparsi ed a seguire con grande attenzione l'applicazione ed il funzionamento dell'accordo con gli Stati Uniti (cd. *Safe Harbor*). Una prima, provvisoria valutazione, effettuata dalla Commissione nei primissimi mesi del 2002, aveva dato risultati non soddisfacenti e, in una successiva visita negli USA i rappresentanti del Gruppo avevano confermato la necessità che l'accordo fosse applicato con serietà.

Il rapporto della Commissione offriva diversi spunti di riflessione, evidenziando come, pur essendo presenti tutti. i requisiti necessari per darvi applicazione vi fosse in realtà, da parte delle non numerose imprese che avevano aderito su base volontaria al *Safe Harbor*, un deficit di trasparenza sia riguardo alle informazioni messe a disposizione dei cittadini sia riguardo alla completezza delle informazioni stesse (ad esempio, per quanto riguarda il diritto di accedere ai dati e di farli cancellare in determinati casi). Inoltre, i sei organismi per la risoluzione delle controversie (tra gli altri, *BBBOnline*, *TRUSTe*, *DMA*), ai quali le imprese USA possono demandare la gestione degli eventuali ricorsi presentati da cittadini UE, non risultavano fornire informazioni complete su come istruire i ricorsi ed autocertificare l'adesione ai meccanismi previsti dal *Safe Harbor*. Questo nonostante l'impegno profuso dalla Federal Trade Commission e dal Dipartimento per il commercio degli USA per diffondere la conoscenza dell'accordo e promuoverne la corretta applicazione.

I Garanti europei, hanno deciso lo scorso 2 luglio a *Bruxelles* di condurre un'analisi approfondita sull'attuazione dell'accordo.

Il Gruppo ha ritenuto, infatti, necessario disporre di informazioni più approfondite e aggiornate per meglio assolvere il proprio ruolo rispetto alle questioni attinenti alla protezione dei dati personali. L'obiettivo di quest'attività informativa è soprattutto quello di valutare, in uno spirito costruttivo, come superare eventuali divergenze rispetto all'attuazione di alcune disposizioni del *Safe Harbor* e colmare le lacune esistenti in termini di prassi applicative. Ciò risulta tanto più necessario se si vuole estendere l'ambito di applicazione dell'accordo ad altre tipologie di trattamento, o magari ad altri Paesi.

Il Gruppo ha richiamato, in tale situazione, la risoluzione adottata dal Parlamento europeo il 5 luglio 2000 a proposito dell'accordo di *Safe Harbor*, ed ha invitato tutte le autorità, gli enti e le associazioni interessate a collaborare per fornire informazioni aggiornate e specifiche su:

- misure per aumentare la trasparenza del funzionamento dell'Accordo;
- possibilità di definire strumenti di verifica ulteriori per quanto riguarda l'adesione all'Accordo e l'eventuale perdita dei benefici da esso derivanti (in caso di comportamenti non conseguenti);
- iniziative per migliorare fra le imprese la conoscenza dei requisiti da soddisfare per rimanere nel *Safe Harbor*;
- misure necessarie per perfezionare i meccanismi di risoluzione delle controversie, favorirne la conoscenza su entrambe le sponde dell'Atlantico e armonizzare le modalità di informazione rispetto agli esiti di tali controversie;
- iniziative da intraprendere per potenziare la cooperazione fra il *"panel"* costituito dalle autorità europee con il compito di esaminare eventuali controversie (al quale possono decidere di rivolgersi anche le imprese USA), gli organismi USA di risoluzione delle controversie previsti dall'Accordo e la *Federal Trade Commission*.

Sulla base delle informazioni raccolte il Gruppo si è riservato di adottare in tempi rapidi un parere con il quale indicare alla Commissione profili utili ai fini della valutazione complessiva del funzionamento del *Safe Harbor*. Nel prendere atto che ancora non sono stati compiutamente forniti gli elementi richiesti, il Gruppo ha dovuto riconoscere che al momento non dispone di informazioni tali da far ritenere ottimale il funzionamento dell'accordo, poi successivamente sollecitate.

Un altro tema di grande interesse sul quale i Garanti si sono pronunciati nell'autunno del 2002 ha riguardato la trasmissione da parte delle compagnie aeree di informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti (parere 6/2002 WP 66 del 24 ottobre 2002).

L'obbligo per le compagnie operanti voli da, verso ed in transito gli Stati Uniti è stato introdotto nella legislazione americana a seguito degli attentati dell'11 settembre 2001. L'imposizione di un tale vincolo, accompagnato inoltre da sanzioni che possono giungere al divieto di sorvolo ed alla perdita dei diritti di atterraggio, oltre a quelle di natura pecuniaria, ha determinato seri riflessi riguardo all'applicazione della direttiva europea in materia di protezione dei dati personali.

Il parere del Gruppo ha evidenziato i rischi della normativa statunitense ed ha richiamato al rispetto delle normative europee.

Per evitare l'entrata in vigore del sistema sanzionatorio, alcuni mesi più tardi, rappresentanti della Commissione europea e delle Dogane USA hanno iniziato un negoziato per definire le condizioni da rispettare a tal fine. Le immediate, forti reazioni del Parlamento europeo e del Gruppo hanno imposto che l'eventuale fornitura dei dati fosse il frutto di un accordo formale. Il Gruppo sta attualmente lavorando alla definizione dei tempi e modi per discutere in ordine alle soluzioni ipotizzabili.

In materia di videosorveglianza, come si è ricordato, i Garanti europei, lo scorso 2 ottobre, hanno approvato in via preliminare un importante documento in cui sono state affermate alcune regole fondamentali che tutti i titolari di trattamenti pubblici e privati effettuati attraverso sistemi di videosorveglianza dovrebbero adottare. Il documento è stato pubblicato sul

sito del Garante e su quello dell'UE ed è stato messo a disposizione per raccogliere suggerimenti ed osservazioni nell'ambito di una ampia consultazione pubblica.

Scopi leciti e chiaramente definiti, raccolta dei dati personali ridotta al minimo, adeguata informazione dei cittadini europei. Questi alcuni dei pilastri del "decalogo" messo a punto dal Gruppo per un uso delle telecamere nel pieno rispetto della riservatezza degli individui.

Il "decalogo" europeo nasce dall'esigenza di definire un quadro di riferimento uniforme ed armonico a livello comunitario riguardo all'installazione di tali sistemi, e contiene indicazioni generali (da specificare ulteriormente nei singoli settori di applicazione) che rappresentano un denominatore comune minimo al quale fare riferimento.

Le indicazioni riguardano in parte anche i trattamenti di dati che non ricadono sotto le disposizioni della direttiva sulla protezione dei dati, come ad esempio, i 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.

Come nel decalogo italiano (*Provv.* 29 novembre 2000) e in quello in adozione presso il Consiglio d'Europa, le regole messe a punto riguardano aspetti fondamentali quali l'effettiva necessità del ricorso ai sistemi di videosorveglianza, la definizione di precisi scopi in base ai quali raccogliere le immagini, la necessità di informare i cittadini circa l'installazione delle telecamere, l'adozione di misure di sicurezza.

82 La partecipazione ad altri comitati e gruppi di lavoro

Sempre nell'ambito della definizione di forme di collaborazione e scambio tra le autorità di protezione dei dati, va ricordato l'*International Working group on data protection in telecommunications* (cd. Gruppo di Berlino), che si propone come luogo di discussione ed approfondimento, non solo a livello europeo, tra esperti in materia di tecnologie ed informazione su temi quali *Internet*, crittografia, comunicazioni elettroniche.

Il gruppo nel periodo considerato ha tenuto due riunioni: la prima a *Berlino* e la seconda a *Zurigo*.

In tali incontri, oltre ai consueti aggiornamenti sullo stato di attuazione e sul completamento della disciplina inerente alla tutela dei dati personali, sono stati affrontati alcuni temi, tra cui quello delle frodi poste in essere *on line*, su cui si è soffermato il rappresentante della *Federal Trade Commission* (FTC) statunitense, che ha sollecitato lo sviluppo di forme di cooperazione transfrontaliere, caratterizzate da celerità ed efficacia e basate su una ampia conservazione dei dati di traffico e la loro *disclosure* (a prescindere dal consenso dell'interessato) in caso di richiesta da parte dei soggetti incaricati di svolgere le indagini. Da parte europea sono stati rappresentati gli ostacoli alla realizzazione di questa attività dal punto di vista della tutela della *privacy* individuale, con particolare riguardo alla *data retention* (pur nell'ambito di un bilanciamento con le esigenze di *enforcement*).

Altri temi hanno riguardato la diffusione di dati personali via *Internet*, l'invio di *Mms* (tema sul quale il Garante si è recentemente pronunciato e che ha fornito lo spunto per un intervento del rappresentante dell'Autorità presente all'incontro, l'invio di comunicazioni commerciali non sollecitate, sul quale le Autorità di protezione dei dati belga e francese hanno richiesto al pubblico di inviare segnalazioni e denunce (è in corso di completamento l'analisi di quelle ricevute).

Nel 2002 sono proseguiti gli incontri organizzati con cadenza semestrale ai fini dello scambio di informazioni e della definizione di un *modus operandi* comune per la trattazione dei ricorsi e delle segnalazioni 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, travalichino l'ambito nazionale. I due seminari si sono tenuti rispettivamente a *Dublino* il 14-15 marzo 2002 ed a *Berlino* il 25-26 novembre 2002 ("*Complaints Handling Workshops*").

Nel seminario di *Dublino* è stata dedicata particolare attenzione al tema dei flussi transfrontalieri di dati, con un approfondimento in merito ai poteri ispettivi e di controllo delle autorità nazionali. In particolare, sono stati presentati i risultati di un questionario sull'argomento fatto circolare fra tutte le autorità dell'UE. Ne è emerso un quadro piuttosto variegato, soprattutto per quanto concerne i criteri di effettuazione delle indagini ispettive in loco ed i poteri sanzionatori delle Autorità. Una tabella comparativa dei risultati è stata resa disponibile attraverso CIRCA ed è stata anche presentata alla *Spring Conference* di *Bonn* delle Autorità europee di protezione dei dati.

Il tema ha avuto ulteriori approfondimenti nel successivo incontro tenutosi a *Berlino* nel mese di novembre 2002, con un'analisi dei risultati del questionario. E' stata anche presentata la procedura seguita in Germania, in coordinamento tra le autorità dei singoli *Laender*, ai fini della valutazione di codici di condotta per il trasferimento di dati da parte di multinazionali.

Al seminario, che ha visto la partecipazione di un numero elevato di delegazioni (circa 24) in rappresentanza di tutte le Autorità garanti dell'UE e dei Paesi candidati all'adesione, sono stati anche oggetto di confronto altri temi, quali:

- la videosorveglianza, con una rassegna dei principali casi nei vari Paesi (il Garante ha illustrato i princìpi indicati del c.d. "decalogo");
- la procedura di trattazione dei ricorsi da parte dell'Autorità inglese, incentrata sull'obbligatoria compilazione di un modello per la presentazione di tali atti e sulla risoluzione preventiva dei problemi segnalati, in modo da evitare il contenzioso o l'applicazione di sanzioni, ed il trasferimento di dati all'estero.

Particolare interesse ha suscitato la trattazione del tema relativo alle cosiddette "centrali dei rischi creditizi": la Francia ha illustrato la situazione normativa esistente in Usa, Germania e UK, mentre il Garante ha presentato il provvedimento adottato in materia nel mese di novembre 2001.

Nel marzo del 2003, si è tenuto a *Varsavia* il VII seminario, cui hanno partecipato anche rappresentanti dei futuri Paesi membri dell'UE. Ad essi sono state fornite alcune indicazioni di metodo basate sull'esperienza sinora raccolta ed è stata condotta un'analisi delle modalità di trattazione di ricorsi e segnalazioni a livello nazionale, evidenziando le tipologie dei principali problemi incontrati e le soluzioni messe in atto.

Fra i temi esaminati in modo più specifico, occorre menzionare le cosiddette *"black lists"*, rispetto alle quali sono state evidenziate alcune importanti discrepanze anche nella normativa dei singoli Paesi UE. In parte connesso a tale tematica è il funzionamento delle cosiddette "centrali rischi": le delegazioni hanno sottolineato l'opportunità di elaborare una serie di indicazioni a livello comunitario, eventualmente attraverso il coinvolgimento del Gruppo per la tutela delle persone con riguardo ai dati personali.

Un terzo punto affrontato riguarda i trasferimenti di dati personali all'estero, anche alla luce degli sviluppi più recenti a livello comunitario. La delegazione italiana ha sintetizzato quattro casi emblematici relativi ad importanti società multinazionali alle quali erano stati chiesti chiarimenti in merito alle metodologie adottate; ne è emerso che i molteplici strumenti già oggi disponibili sembrano consentire di rispondere in modo adeguato alle esigenze di circolazione dei dati prospettate da aziende anche di grandi dimensioni. Si è concordato sull'esigenza di individuare un approccio uniforme, soprattutto onde evitare il rischio di un *authority shopping* da parte delle aziende; a tale scopo, si è proposto di potenziare l'uso degli strumenti offerti dallo spazio *web* di discussione CIRCA. Questo ed altri temi (trattamento di dati biometrici, bilanciamento di interessi, iniziative di sensibilizzazione) saranno approfonditi nel corso del prossimo *workshop*, che si terrà a Roma.

L'Autorità di controllo comune Schengen

83 L'attività dell'Autorità

L'Autorità comune di controllo (Acc), attualmente presieduta dal segretario generale del Garante, ha proseguito la sua attività di verifica e controllo del funzionamento della parte centrale del Sistema di informazione Schengen, nel perseguimento delle finalità che la Convenzione le attribuisce.

Una parte importante delle riunioni dell'Autorità è stata rivolta ad approfondire e discutere i progetti di sviluppo del sistema consistenti nell'introduzione di nuove funzioni, in particolare al fine di combattere il terrorismo, le quali dovrebbero prevedere l'accesso e l'uso dei dati contenuti nel SIS da parte di altri organismi, quali Europol ed Eurojust.

L'Autorità in due pareri, del 1 ottobre e del 3 dicembre, ha ribadito le sue perplessità riguardo a tali progetti ed ha segnalato per alcuni aspetti la carenza di idonee motivazioni e basi legali per poter esaminare nel merito la richiesta, attese le precise disposizioni della Convenzione relative all'accesso ed all'uso dei dati.

E' stato adottato inoltre un parere, nel giugno 2002, concernente le segnalazioni nel SIS delle persone la cui identità è stata usurpata ed il modo per evitare che le stesse subiscano conseguenze negative dall'abuso perpetrato da altri. Questo parere è stato richiamato in occasione del parere sul cd. *"SIS II"* proprio per sottolineare come la previsione di un ampliamento delle categorie di dati cui accedere e dei soggetti ai quali tale accesso ed uso è consentito non deve provocare una limitazione dei diritti delle persone che hanno subito il furto dei documenti di identità.

La disamina relativa ai problemi nascenti dal previsto passaggio al nuovo Sistema d'informazione Schengen, è stata compiuta dall'Autorità anche con riferimento ad altri aspetti quali il fatto che lo stesso sarà basato su nuove piattaforme informatiche, che conterrà ulteriori categorie di informazioni e sarà costruito in vista del futuro ampliamento ed allargamento dell'Unione europea: sarà quindi compito dell'autorità sorvegliare il processo e ricordare che, in parallelo, deve esservi una corrispondente estensione delle garanzie previste dall'originaria Convenzione.

Un altro importante parere adottato dall'Autorità riafferma che la valutazione in merito alla durata della conservazione delle segnalazioni concernenti dati personali inserite nel Sistema debba essere effettuata con esclusivo riferimento all'articolo 112 della Convenzione.

L'Autorità ha inoltre deciso di rendere biennale la redazione e la conseguente pubblicazione del rapporto di attività.

Il mantenimento del dialogo aperto con il Parlamento europeo (in particolare con la

Commissione "diritti e libertà pubbliche" che ha invitato il Presidente dell'Acc ad un'audizione pubblica l'8 ottobre 2002 ed ha recepito in dicembre le proposte dell'Acc sul SIS II), ed anche con il Comitato parlamentare cui è affidato in Italia il controllo sull'attuazione delle Convenzioni Schengen ed Europol, ha consentito al Presidente dell'Autorità Schengen di essere ascoltato riguardo alle questioni emergenti.

È stato inoltre approvato l'avvio dell'istituzione di una *newsletter* dell'Acc ed il rinnovo del sito *web* su impulso della presidenza italiana.

Nel periodo considerato è proseguita l'opera di controllo svolta dal Garante sul funzionamento dell'archivio della sezione nazionale del Sistema d'informazione, anche attraverso le numerose segnalazioni pervenute da privati.

Europol

84 L'attività dell'Autorità comune di controllo e i primi casi di contenzioso

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

L'Autorità ha seguito con attenzione i progetti di negoziato sottoposti dal Direttore dell'Europol per ottenere il consenso ad iniziare le trattative ai fini di effettuare lo scambio di dati con alcuni Paesi terzi. Particolare impegno è stato posto nel seguire il negoziato per pervenire ad un accordo formale che disciplinasse, nel rispetto dei principi in materia di protezione dei dati personali sanciti nella Convenzione stessa, la fornitura di dati da Europol agli Stati Uniti.

L'Autorità, interessata da Europol in attuazione della decisione di fornire dati agli USA a seguito degli attentati dell'11 settembre, aveva infatti rappresentato la necessità di stipulare con le competenti autorità americane un accordo formale, contenente le garanzie necessarie per poter operare in piena legittimità ed aveva espresso la volontà di essere interessata al relativo negoziato. L'attività dell'Autorità è testimoniata, in particolare, dalla nota verbale aggiuntiva all'accordo per lo scambio di dati.

Sono stati inoltre espressi pareri in relazione all'apertura di *file* di analisi, alla modifica dell'Atto che definisce la trasmissione di dati da Europol a Stati ed organismi terzi, nonché in relazione alle proposte di modifica della Convenzione presentate dal regno di Danimarca.

È stata compiuta una ulteriore ispezione alla sede dell'Europol che, in particolare, si è incentrata sugli archivi di analisi e sugli sviluppi tecnologici del sistema.

È stata approvata la prima relazione di attività e sono in corso contatti per la stampa e la presentazione della stessa.

Si sta lavorando per l'apertura di una pagina dedicata all'interno del sito di Europol.

Il Comitato di appello ha ricevuto i primi ricorsi, di cui uno attualmente in trattazione.

Il controllo sul Sistema informativo doganale

85 La creazione dell'Autorità di controllo

Con la legge 30 luglio 1998, n. 291, l'Italia ha autorizzato la ratifica e l'esecuzione della Convenzione sull'uso dell'informatica nel settore doganale, elaborata in base all'articolo K3 del Trattato sull'Unione europea del 26 luglio 1995.

La convenzione mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'UE, particolarmente attraverso lo scambio di dati personali.

A tal fine è stata prevista la creazione di un sistema informativo automatizzato comune (Sistema informativo doganale-SID) che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La convenzione istituisce una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

L'Autorità ha iniziato i suoi lavori nel corso della primavera del 2002 ed ha provveduto alla nomina del Presidente e del vice presidente (quest'ultimo nella persona di un dirigente dell'Ufficio del Garante). Ha poi adottato il regolamento interno ed un parere sull'istituzione di un archivio di identificazione dei fascicoli a fini doganali.

Eurodac

86 Collaborazione tra Stati membri e garanzie per gli interessati

L'autorità comune di controllo Eurodac per il confronto delle impronte digitali dei richiedenti asilo è stata istituita ed ha tenuto la sua prima riunione nel dicembre 2002, pervenendo alla nomina del Presidente ed all'adozione del regolamento interno.

La funzionalità dell'organismo è però ben lungi dall'essere effettiva in quanto, all'atto dell'ormai imminente istituzione dell'organo di controllo indipendente di cui all'art. 286, par. 2 del Trattato di Amsterdam i compiti di supervisione e controllo provvisoriamente svolti da tale organo, saranno attribuiti al Garante europeo.

All'autorità di controllo indipendente, in attuazione appunto dell'art. 286 del Trattato di Amsterdam, il regolamento n. 45/2001 conferisce il compito di controllare la correttezza dei trattamenti di dati effettuati dalle istituzioni e dagli organismi dell'UE.

Consiglio d'Europa

87 La convenzione sul *cybercrime*

La Convenzione del Consiglio d'Europa sul *cybercrime*, sottoscritta da 30 Paesi il 23 novembre 2001, è stata finora ratificata da soli due Stati (Albania e Croazia); pertanto non è ancora entrata in vigore non essendo stato raggiunto il numero minimo richiesto di 5 ratifiche, di cui almeno 3 di Stati membri del Consiglio d'Europa.

Si ricorda che tra i firmatari figurano Paesi non membri del Consiglio d'Europa (Stati Uniti, Canada, Giappone e Sud Africa).

Successivamente è stato negoziato, ad aperto alla firma il 21 gennaio 2003, un Protocollo aggiuntivo che prevede l'estensione del campo d'applicazione della Convenzione, incluse tutte le disposizioni sostanziali e procedurali, nonché quelle che disciplinano la cooperazione internazionale, agli atti di natura razzista o xenofoba commessi per mezzo di strumenti informatici.

A cagione, e successivamente agli attentati dell'11 settembre 2001, anche il Consiglio d'Europa ha iniziato una intensa attività rivolta a rendere più efficace la reazione internazionale contro il terrorismo ed, in questo quadro, a sviluppare strumenti legali per combattere lo stesso.

Il Consiglio d'Europa aveva già, fin dal 1977, adottato una specifica Convenzione sull'eliminazione del terrorismo.

Dopo gli attentati dell'11 settembre, il Comitato dei ministri aveva richiesto uno sforzo più incisivo. Tutti i 44 Stati membri hanno firmato la citata Convenzione ed è stato conferito un formale incarico di rivedere gli strumenti adottati dal Consiglio d'Europa in materia di lotta al terrorismo ad un Gruppo -il GMT o Gruppo multidisciplinare per un'azione internazionale contro il terrorismo- di cui fanno parte, oltre ai rappresentanti degli Stati membri del Consiglio d'Europa, anche Stati Uniti, Canada, Giappone, Messico e Santa Sede.

Il Gruppo ha presentato il rapporto finale delle attività formulando una proposta di protocollo emendativo della Convenzione del 1977. Nel gennaio 2003 l'Assemblea parlamentare ha adottato un parere sul testo ed il Comitato dei ministri ha formalmente approvato la proposta il 13 febbraio 2003. L'apertura alla firma è prefissata per il 15 maggio 2003.

Le proposte emendative riguardano sostanzialmente la de-politicizzazione di alcuni atti criminosi, che divengono quindi oggetto di estradizioni, oltre ad una semplificazione delle procedure per ampliare la lista dei crimini estradabili.

Il Consiglio d'Europa, ha nel contempo incaricato il Comitato diritti umani di studiare e proporre delle linee guida sulla lotta al terrorismo ed i diritti umani. Le linee-guida, che sono state adottate dal Comitato dei Ministri nel luglio 2002, costituiscono certamente il primo testo internazionale in questo campo, anche se non direttamente vincolante per gli Stati.