22 Relazioni internazionali

Lo stato di recepimento delle direttive comunitarie negli Stati membri dell'Unione europea

Non vi sono particolari novità da segnalare per quanto riguarda il recepimento della direttiva generale in materia di protezione dei dati personali (direttiva n. 95/46/Ce), poiché tutti gli Stati membri hanno già adottato disposizioni attuative nel diritto interno e non sussistono attualmente, né sono state avviate procedure di infrazione dalla Commissione europea.

Occorre invece menzionare brevemente alcuni sviluppi intercorsi nel 2005 in rapporto alla direttiva "*e-Privacy*" (direttiva n. 2002/58/Ce). Come riferito nella *Relazione* 2004 (p. 141), la Commissione europea aveva adito la Corte di giustizia nei confronti di alcuni Paesi (Belgio, Grecia, Lussemburgo) per omessa segnalazione delle misure nazionali di recepimento della direttiva n. 2002/58/Ce. Successivamente, Belgio e Lussemburgo hanno notificato l'adozione dei provvedimenti che recepiscono le disposizioni della direttiva e il procedimento avviato nei loro confronti si è quindi concluso. Viceversa, la Grecia non risulta aver notificato le norme nazionali di trasposizione e risulta altresì essere l'unico Stato membro dell'Ue nei cui confronti è aperto un procedimento dinanzi alla Corte per mancato recepimento della direttiva stessa.

Sono tuttavia in corso altre procedure di infrazione aperte nei confronti di Repubblica Ceca, Germania, Lettonia e Slovacchia per imperfetta trasposizione delle disposizioni contenute nella medesima direttiva. In particolare, Repubblica Ceca, Lettonia e Slovacchia non avrebbero attuato correttamente le norme comunitarie in materia di comunicazioni commerciali indesiderate (art. 13 dir. n. 2002/58/Ce), mentre la Slovacchia non avrebbe introdotto l'obbligo di informare gli utenti della presenza e dei meccanismi di funzionamento dei *cookie*. Rispetto alla Germania, i servizi della Commissione stanno inoltre valutando la trasposizione delle norme concernenti i dati relativi all'ubicazione (art. 9), che non sarebbero pienamente recepite nel diritto interno. Infine, è da segnalare che la Commissione europea ha inviato un "parere motivato" al Regno Unito (il secondo passo nella procedura di infrazione, che fa seguito all'invio di una lettera di "messa in mora") per non aver notificato alcuna misura di attuazione relativa al territorio di Gibilterra, cui si applicano le norme comunitarie ai sensi del Trattato di adesione del Regno Unito alle Comunità europee.

Conferenze delle autorità di protezione dei dati a livello europeo

Dal 1991, le autorità di protezione dati europee si incontrano tutti gli anni in primavera in un'occasione divenuta ormai istituzionale, la *cd. Spring Conference*. Nel 2005, la Conferenza di primavera si è svolta il 25 e 26 aprile a Cracovia ed è stata dedicata in particolare alla valutazione dell'impatto della direttiva n. 95/46/Ce, a dieci anni dalla sua approvazione. Fra gli altri temi all'ordine del giorno meritano di essere menzionati il trasferimento di dati verso Paesi "non adeguati", con particolare riferimento alle "regole vincolanti nell'impresa" (*Binding Corporate Rules*), alla figura dell'incaricato per la *privacy* (*privacy officer*) e alle modalità di regolazione nazionale del diritto di accesso da parte dell'interessato ai propri dati personali.

Il dibattito che ha caratterizzato maggiormente la Conferenza, dando luogo ad una Dichiarazione e ad una presa di posizione ufficiali delle autorità di protezione dati, ha riguardato il tema dei flussi di dati nelle attività giudiziarie e di polizia, anche in previsione dell'adozione da parte della Commissione europea di uno stru-

mento che fissi le garanzie da applicare al trattamento dei dati personali nel *cd.* "Terzo pilastro". Nel documento comune, le autorità, dando atto che le attività di lotta al terrorismo e al crimine organizzato comportano un rafforzamento dello scambio di dati personali, hanno chiesto che tale scambio avvenga apprestando previamente un sistema di garanzie adeguato per la protezione dei dati personali.

Le autorità hanno ribadito che gli *standard* fissati nella direttiva n. 95/46/Ce restano validi anche per il trattamento di dati per le predette finalità, ed hanno rilevato in particolare che la proporzionalità del trattamento deve essere utilizzata come criterio per valutare la necessità delle misure che prevedono uno scambio di informazioni nel Terzo pilastro. Ciò significa che dovrà essere garantito il controllo a livello nazionale e comunitario da parte delle autorità indipendenti, con il coinvolgimento degli Stati membri.

Successivamente alla presentazione da parte della Commissione europea, in data 11 ottobre 2005, di una proposta di decisione-quadro per introdurre principi armonizzati di protezione dati nei trattamenti di dati per finalità di giustizia e polizia (2005/0202/Cns), le autorità garanti hanno inoltre adottato un parere nel quale, oltre a richiamare le linee esposte nella dichiarazione, hanno sviluppato una serie di osservazioni puntuali sul testo.

Conferenze delle autorità su scala internazionale

La 27ma Conferenza internazionale dei Garanti si è tenuta in Svizzera, a Montreux, dal 14 al 16 settembre 2005, ed ha riunito le autorità di 45 Paesi. Durante la Conferenza sono state poste al centro dell'attenzione le tematiche relative alla tutela delle libertà fondamentali –in particolare della *privacy*– nell'attuale contesto geopolitico, delle applicazioni biometriche, dello sviluppo di tecnologie invasive, del *marketing* politico e della creazione e gestione delle biobanche.

A quest'ultimo tema è stata dedicata una intera sessione, presieduta dal presidente del Garante prof. Francesco Pizzetti, il quale ha affrontato i delicati problemi posti dalle strutture che conservano a scopi sanitari o di ricerca i campioni biologici, con particolare riguardo alla necessità di determinare quali soggetti possano trattare dati relativi a campioni biologici, alle modalità di controllo del loro utilizzo e al rischio di sovrapposizione dei compiti delle autorità di garanzia e dei comitati etici.

Nell'ambito dei lavori della Conferenza, il segretario generale dell'Autorità dott. Giovanni Buttarelli è intervenuto sul tema della comunicazione politica, soffermandosi sull'analisi dei principi guida dettati dal *provvedimento* del 7 settembre 2005 [doc. *web* n. 1165613] per una propaganda elettorale rispettosa dei cittadini, e auspicando l'adozione di un codice deontologico che disciplini in modo organico il *marketing* politico, nonché l'individuazione di principi generali in cui tutte le autorità nazionali possano riconoscersi.

Al termine della Conferenza sono stati adottati tre importanti documenti. Nella Dichiarazione su "La protezione dei dati personali e della *privacy* in un mondo globalizzato: un diritto universale che rispetta le diversità", i Garanti hanno ribadito l'impegno a collaborare con i governi e con gli organismi internazionali e sopranazionali, al fine di mettere a punto una "convenzione universale" per la protezione delle persone fisiche rispetto al trattamento di dati personali. A tal fine le autorità hanno rivolto un invito alle Nazioni unite affinché preparino uno strumento giuridico vincolante, un'esortazione a tutti i governi del mondo affinché promuovano l'adozione di strumenti in materia di protezione dei dati e della *privacy* conformi ai principi fondamentali (fra cui rientra il principio del controllo indipendente e dell'esistenza di sanzioni) e un appello al Consiglio d'Europa affinché inviti anche gli Stati non membri ad aderire alla Convenzione n. 108/1981 e al suo Protocollo addizionale.

Nella stessa Dichiarazione sono stati inoltre sollecitati:

- gli organismi internazionali, ad istituire al proprio interno autorità di vigilanza indipendenti dotate di poteri di controllo;
- le organizzazioni non governative internazionali, a mettere a punto *standard* basati sui principi fondamentali della protezione dati;
- i produttori di *hardware* e *software*, a sviluppare prodotti e sistemi che incorporino tecnologie idonee a potenziare la *privacy*.

Nella "Risoluzione sull'utilizzo della biometria in passaporti, carte di identità e titoli di viaggio"[doc. *web* n. 1170552], le autorità, dopo aver rilevato l'impiego crescente dei dati biometrici sia nel settore pubblico, sia in quello privato, nonché i rischi connessi alla possibilità di raccogliere tali dati all'insaputa dell'interessato e di utilizzarli come identificatori univoci a livello globale, hanno richiesto:

- che l'impiego delle tecnologie biometriche preveda garanzie efficaci al fine di limitare i rischi connessi alla loro natura;
- che si tengano rigidamente distinti i dati biometrici raccolti e memorizzati per finalità di natura pubblica in base ad obblighi di legge (ad esempio, i controlli alle frontiere) e quelli raccolti e memorizzati per finalità contrattuali sulla base del consenso;
- che si limiti tecnicamente l'impiego della biometria nei passaporti e nelle carte d'identità alle finalità di verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal titolare all'atto della presentazione del documento stesso.

Infine, nella "Risoluzione sull'utilizzo di dati personali per la comunicazione politica" [doc. *web* n. 1170546], predisposta e presentata dal Garante, è stato ribadito che ogni attività di comunicazione politica che comporti il trattamento di dati personali deve rispettare i diritti e le libertà fondamentali degli interessati, fra cui rientra il diritto alla protezione dei dati personali.

Nel documento, i principi di *data protection* consolidati vengono declinati con riferimento alla comunicazione politica. In particolare, si stabilisce che i dati personali devono essere trattati solo se necessari per il raggiungimento delle finalità di comunicazione politica; devono essere raccolti attraverso fonti accessibili lecitamente, accurati, pertinenti, non eccedenti e aggiornati. I dati raccolti da fonti, istituzioni o associazioni pubbliche o private possono essere utilizzati per scopi di comunicazione politica solo se il trattamento ulteriore è compatibile con le finalità per le quali sono stati raccolti e gli interessati sono stati informati. L'informativa deve precedere la raccolta dei dati e specificare l'identità del titolare e le tipologie di flussi, mentre il trattamento deve essere fondato sul consenso dell'interessato o su un altro presupposto legittimo previsto dalla legge. I titolari del trattamento, siano essi forze politiche o singoli candidati, devono adottare tutte le misure di sicurezza necessarie a tutelare l'integrità delle informazioni e a prevenire la perdita e/o l'utilizzo abusivo dei dati. Devono inoltre essere riconosciuti agli interessati il diritto di accesso, rettifica, blocco e/o cancellazione, nonché il diritto di opporsi alle comunicazioni indesiderate e il diritto di chiedere, gratuitamente e con modalità semplici, di non ricevere ulteriori messaggi. L'esistenza di tali diritti deve essere menzionata nell'informativa e in caso di violazione devono essere previsti adeguati rimedi giuridici e sanzioni.

22.1. *La cooperazione tra autorità garanti nell'Ue: il Gruppo art. 29*

Nel 2005 è stato avviato un più intenso rapporto di collaborazione del con la Commissione e, in particolare, con il nuovo commissario italiano on. Frattini, vice

presidente e responsabile del settore Libertà, sicurezza e giustizia, per garantire il pieno rispetto del diritto alla protezione dei dati personali e favorire un dialogo più intenso tra le autorità indipendenti e le istituzioni comunitarie.

Per sottolineare questo impegno, in gennaio il Commissario ha incontrato il Gruppo riaffermando le linee di azione e gli impegni già presi in materia dalla nuova Commissione e annunciati sia nel primo contatto con il Parlamento europeo, sia nella precedente riunione di dicembre con le autorità comuni di controllo.

Proprietà intellettuale

L'incremento della circolazione delle informazioni legato allo sviluppo di Internet pone il delicato problema del controllo delle informazioni protette dal diritto d'autore, in particolar modo con riferimento ai diritti e agli obblighi dei soggetti che hanno interessi rispetto alle informazioni protette dal *copyright* e dei soggetti che sono coinvolti nel *digital rights management*. Il Gruppo art. 29 si è occupato del rapporto tra diritti di proprietà intellettuale e protezione dati in un documento di lavoro adottato il 18 gennaio 2005 (WP 104). Il documento è rivolto ai soggetti coinvolti a vario titolo nella gestione del *copyright* (titolari, produttori, fornitori di servizi e utenti).

Con riferimento alla tutela preventiva del diritto d'autore, nel documento sono state analizzate le tecnologie usate più frequentemente per il trattamento di dati personali. In alcuni casi viene chiesto all'utente di identificarsi per poter accedere a determinati contenuti, e viene associato al contenuto scaricato da Internet un identificatore univoco, che lega inscindibilmente l'utente a quel contenuto. In altri casi vengono impiegate tecniche di tracciamento finalizzate ad individuare gli utenti che scaricano documenti o altro materiale protetto senza averne il diritto: in questi casi i legittimi titolari del diritto d'autore ricorrono solitamente all'indirizzo *Ip* dell'utente, oppure impongono ai fornitori di servizi Internet di comunicare i dati in loro possesso, ovvero confrontano tali informazioni con i dati contenuti nei registri *Whois*. Il Gruppo, rispetto ai casi appena descritti, ha ricordato la necessità di rispettare alcuni principi fondamentali in materia di protezione dati, e in particolare la possibilità di mantenere l'anonimato nelle operazioni che avvengono in Internet, l'impiego di identificatori univoci solo se disciplinato da specifiche norme nazionali secondo quanto previsto dalla direttiva n. 95/46/Ce, lo sviluppo di ausili tecnologici che consentano di ridurre l'ambito dei dati personali utilizzati in rapporto alle singole operazioni (*Privacy Enhancing Technologies-Pet*), l'obbligo di fornire agli interessati un'informativa adeguata e preventiva, il rispetto del principio di finalità e la necessità di delimitare il tempo di conservazione dei dati.

Con riferimento alla tutela *ex post*, finalizzata a individuare i soggetti sospettati di avere violato la normativa sul diritto d'autore, sono stati parimenti ribaditi alcuni principi. I dati contenuti nel registro *Whois* non devono essere utilizzati per finalità incompatibili con quelle per cui sono stati raccolti, e gli *Internet Service Provider* (Isp) non sono tenuti a fornire a soggetti privati, titolari di diritti d'autore, le informazioni in loro possesso, raccolte per la fornitura dei servizi di tlc (diverso è il caso in cui la richiesta provenga da autorità giudiziarie o di polizia, sulla base di specifiche disposizioni di legge). Con riferimento al tempo di conservazione dei dati, gli Isp non sono tenuti a conservare a tempo indeterminato tutti i dati di traffico relativi a informazioni tutelate dal diritto d'autore. La conservazione di dati giudiziari può avvenire solo nel rispetto di rigide disposizioni adottate dai singoli Stati membri, i quali devono prevedere anche adeguate garanzie per gli interessati.

Rfid

L'utilizzo delle tecnologie *Rfid* (*Radio Frequency Identification*) pone diverse problematiche da analizzare per il pieno rispetto dei diritti degli interessati. La tecnologia *Rfid* è utilizzata in un numero crescente di settori, fra i quali si possono ricordare

il settore dei trasporti, della distribuzione, dell'aviazione, della sanità, del controllo degli accessi, della vendita al dettaglio; pur caratterizzata da evidenti vantaggi da un punto di vista economico –anche in considerazione dei costi relativamente contenuti– se non correttamente utilizzata la *Rfid* può infatti consentire indebite intrusioni nella sfera privata. Attraverso questi dispositivi è infatti possibile raccogliere surrettiziamente differenti categorie di dati: ad esempio, profilare i clienti, monitorando i loro comportamenti, i capi di abbigliamento, gli accessori o le medicine utilizzate.

Il Gruppo art. 29 ha approvato un documento di lavoro (WP 105, 19 gennaio 2005), rivolto agli utilizzatori di queste tecnologie e ai produttori ed organismi che si occupano di standardizzazione, chiamati a cooperare per orientare queste tecnologie in termini più rispettosi della *privacy*.

Dopo aver richiamato l'attenzione sulla necessità di applicare tutti i principi contenuti nelle direttive europee in materia di protezione dei dati laddove si trattino informazioni relative ad un individuo identificato o identificabile, il Gruppo ha sottolineato la possibilità di utilizzare dispositivi tecnologici e accorgimenti di varia natura al fine di dare effettiva attuazione a tali principi. Esistono, infatti, strumenti che, a vari livelli, permettono di sviluppare i principi di protezione dati già all'interno di dispositivi come quelli basati sulle tecnologie *Rfid*.

Fra le indicazioni specifiche fornite dal Gruppo di lavoro si evidenziano in particolare:

a) il riconoscimento del diritto degli interessati ad essere informati, sia sulla presenza di dispositivi *Rfid*, sia sulla loro attivazione (*ad es.*, attraverso pittogrammi, o segnalazioni luminose);

b) la possibilità di esercitare il diritto di accesso, rettifica, cancellazione ecc. (viene consigliato l'utilizzo di linguaggi *standard* come l'*Xml* o di dispositivi per la disattivazione permanente o temporanea);

c) la necessità che il trattamento di dati personali attraverso la tecnologia *Rfid* sia comunque basato sul consenso dell'interessato e, laddove sia possibile ritirare il consenso, che siano utilizzati dispositivi in grado di disattivare facilmente il *tag Rfid* (*tag disabler*);

d) la necessità di proteggere i dati personali contenuti nei *tag Rfid* attraverso misure di sicurezza proporzionali alla natura del trattamento effettuato (cifratura e autenticazione del lettore *Rfid*, impiego di protocolli *standard* di autenticazione secondo norme Iso, impiego di metodi di autenticazione crittografica ecc.).

Il documento è stato sottoposto ad una consultazione pubblica, conclusasi il 31 marzo 2005, a cui hanno partecipato soggetti pubblici e privati. Sulla base dell'analisi delle risposte è stato preparato un documento di sintesi che non esprime considerazioni di merito e si limita a evidenziare alcune questioni maggiormente controverse:

- non necessità di integrare la direttiva n. 95/46/Ce con norme specifiche per la *Rfid*. Tale opportunità non risulta condivisa dalle imprese, secondo le quali una regolamentazione troppo dettagliata potrebbe avere ripercussioni negative in termini di concorrenza rispetto ad altre aree del mondo;
- richiesta al Gruppo art. 29 di fornire ulteriori indicazioni riferite specificamente a determinate applicazioni (*ad es.*, uso di dispositivi *Rfid* nelle attività commerciali, nei passaporti, nei trasporti pubblici);
- necessità di approfondire la natura dei trattamenti effettuati attraverso dispositivi *Rfid*, con particolare riguardo all'esistenza di un trattamento effettivo di dati personali e al concetto di dato personale, che a giudizio di alcuni commentatori è interpretato in modo eccessivamente estensivo dal Gruppo art. 29;

A seguito di queste riflessioni il Gruppo art. 29 ha ritenuto di dover costituire un sottogruppo che approfondisca il concetto di "dato personale" con particolare riguardo alle applicazioni *Rfid*.

Dati relativi all'ubicazione

La possibilità di ricavare informazioni sulla localizzazione via satellite e la maggiore diffusione della telefonia mobile hanno determinato un aumento enorme dell'uso di dati relativi all'ubicazione nell'offerta di beni e servizi.

Il Gruppo art. 29, in un parere sul tema dell'uso di dati relativi all'ubicazione al fine della fornitura di servizi a valore aggiunto (WP 115, 25 novembre 2005), ha ricordato che a tale settore vanno applicate le disposizioni delle direttive comunitarie in materia di protezione dati. Con riferimento al diritto nazionale applicabile è stato evidenziato il principio secondo cui il trattamento di dati relativi all'ubicazione è soggetto al diritto dello Stato membro in cui è stabilito il responsabile del trattamento, anziché a quello dello Stato membro di cui è cittadino la persona interessata. Quando il responsabile non è stabilito in uno Stato membro, il trasferimento di dati può avvenire solo alle condizioni previste dal capo IV della direttiva n. 95/46/Ce.

Per quanto riguarda l'informativa, il documento ribadisce l'obbligo di renderla a carico del fornitore del servizio a valore aggiunto ovvero, se quest'ultimo non ha contatti diretti con la persona interessata, dell'operatore delle comunicazioni elettroniche. L'informativa può essere fornita o direttamente ogni volta che il servizio viene utilizzato, oppure nelle condizioni generali del servizio, purché in quest'ultime caso le informazioni siano consultabili in qualsiasi momento e in maniera semplice.

Il Gruppo si è soffermato anche sul tema del consenso, escludendo che questo possa essere prestato nel quadro dell'accettazione delle condizioni generali del servizio offerto. I fornitori di servizi sono chiamati a predisporre misure adeguate per garantire che la persona che ha manifestato il consenso sia effettivamente quella cui i dati si riferiscono, e rappresenti l'effettivo utilizzatore dell'apparecchiatura terminale. Pertanto, è stata richiamata l'attenzione degli operatori sulla necessità di introdurre misure efficaci per la verifica e l'autenticazione delle richieste di accesso ai dati di ubicazione. Il consenso deve poter essere revocato in qualsiasi momento, anche in via temporanea, mediante una funzione semplice e gratuita. I dati relativi all'ubicazione possono essere trattati solo per la durata necessaria alla fornitura di un servizio a valore aggiunto, e con tutte le precauzioni relative alle misure di sicurezza finalizzate a garantire la riservatezza e l'integrità dei dati.

La seconda parte del documento è dedicata a due casi che sollevano problemi più delicati con riferimento al trattamento dei dati personali: il trattamento di dati di localizzazione riferiti a minori e a lavoratori dipendenti.

Per quanto riguarda i minori, il Gruppo art. 29 ha ricordato che la Convenzione internazionale sui diritti del fanciullo prevede già che qualsiasi decisione concernente i minori debba essere presa tenendo in considerazione, in primo luogo, il migliore interesse del fanciullo, e che nessun fanciullo possa essere oggetto di interferenze arbitrarie o illegali nella vita privata. I fornitori di servizi devono pertanto introdurre procedure adeguate per identificare le persone che si registrano come "genitori" e limitare solo ad esse l'accesso.

In riferimento alla localizzazione di lavoratori dipendenti il Gruppo ha sottolineato che la liceità del trattamento dei dati relativi all'ubicazione non deve basarsi esclusivamente sul consenso del lavoratore (il quale, peraltro, rappresenta il "soggetto debole" del rapporto), ma deve essere affrontata in una prospettiva più ampia anche attraverso accordi collettivi. Il trattamento deve inoltre corrispondere ad un'esigenza specifica dell'impresa. Il Gruppo ha poi richiamato l'attenzione sulla necessità di rispettare tutti gli altri principi di protezione dei dati e in particolare i limiti

al periodo di conservazione (che non dovrebbe superare due mesi) nonché le misure di sicurezza, al fine di evitare che soggetti non autorizzati accedano ai dati relativi all'ubicazione dei lavoratori dipendenti.

Rapporto sulla notificazione

All'esito delle attività di cui si era già riferito nella *Relazione* 2004 (p. 142), il Gruppo ha reso pubblico un rapporto (WP 106, 18 gennaio 2005), con il quale ha fornito ai Paesi membri indicazioni rispetto alla notificazione dei trattamenti di dati personali. Il rapporto si accompagna ad un *Vademecum* (messo a punto sotto il coordinamento del Garante italiano nel 2004 e perfezionato durante il 2005) sulla disciplina della notificazione vigente nei 25 Paesi Ue, in modo da consentire, a chiunque lo desideri (titolari di trattamento e/o interessati), di poter conoscere come si articoli e si diversifichi il sistema della notificazione in ambito Ue, e quali siano i passi da compiere per notificare un trattamento nei diversi Stati membri.

Nel rapporto, è stato osservato che la notificazione resta un adempimento necessario, in particolare nei Paesi di recente adesione all'Ue, laddove riveste anche la funzione generalpreventiva di richiamare l'attenzione sull'esistenza di particolari obblighi connessi alla legislazione sulla protezione dei dati; tuttavia, essa non deve mai costituire un puro appesantimento di stampo burocratico. Per questo motivo, nell'ottica di semplificazione degli obblighi amministrativi già indicata come obiettivo dalla Commissione europea (*v. Relazione* 2004, p. 142), il Gruppo ha segnalato la possibilità di razionalizzare e semplificare i meccanismi di notificazione:

- promuovendo forme di notificazione *on-line* o comunque basate in massima parte su strumenti elettronici (moduli scaricabili o compilabili via Internet, utilizzo della firma digitale);
- invitando il legislatore nazionale a riflettere sull'opportunità di introdurre la figura dei *cd.* "*privacy officer*" (soggetti che all'interno di un'azienda o di un ente siano incaricati di vigilare sul rispetto della normativa in materia di *privacy* e di censire tutti i trattamenti di dati personali effettuati, con conseguente esenzione dall'obbligo di notificazione all'autorità nazionale di protezione dei dati);
- avvalendosi di tutte le soluzioni di esenzione dall'obbligo di notifica praticabili alla luce della direttiva n. 95/46/Ce;
- avviando una riflessione a livello nazionale sull'effettiva necessità della richiesta di alcuni elementi attualmente previsti nei modelli di notificazione, che vadano al di là di un "nucleo comune" di informazioni (periodo di conservazione dei dati, origine dei dati, meccanismi per l'esercizio dei diritti riconosciuti agli interessati), rispetto agli elementi "minimi" obbligatori ai sensi dell'art. 19, comma 3, della direttiva. La scelta del *common core* sembra costituire un'opzione ragionevole e sul quale la maggioranza dei Paesi Ue risulta concordare;
- valutando la necessità di conferire maggiori poteri alle autorità di protezione dati nella scelta dell'approccio più indicato ed efficace in termini di notificazione.

Il rapporto propone, infine, un meccanismo di notificazione semplificata per i soggetti stabiliti in più Stati membri, che prevederebbe la presentazione di una notificazione "completa" in un solo Paese (tendenzialmente quello in cui ha sede, ad esempio, l'impresa capogruppo), contestualmente ad una sorta di notificazione "ridotta" da presentare negli altri Paesi in cui il soggetto in questione risulti stabilito. Su quest'ultimo punto, la discussione nel Gruppo è ancora aperta.

Pnr - Canada

Il Gruppo art. 29 si è pronunciato favorevolmente, con il parere n. 1/2005 (WP 103, 19 gennaio 2005), sul livello di adeguatezza in materia di protezione dati offerto dal Canada con riferimento alla trasmissione da parte delle compagnie aeree

dei dati di identificazione dei passeggeri (Pnr) e di informazioni anticipate sui viaggiatori (Apis). Il Gruppo si era già pronunciato su tale argomento nel 2004 (parere n. 3/2004), sollevando una serie di critiche al sistema messo in piedi con riferimento ai principi di protezione dati, e invitando la Commissione a proseguire i negoziati con il Canada.

I negoziati successivi hanno portato il Canada a rivedere il sistema d'informazione sui passeggeri, e in particolare a modificare i seguenti aspetti:

- il sistema è stato configurato per ricevere i dati Apis/Pnr dalle compagnie aeree attraverso il sistema "*push*";
- è stato identificato un elenco chiaro e limitato dei reati gravi direttamente connessi con il terrorismo;
- le tipologie di dati da trasferire sono state ridotte da 38 a 25, con l'esclusione dei dati sensibili e dei campi "testo aperto" o "osservazioni generali";
- il tempo di conservazione dei dati è stato ridotto da 6 anni a 3 anni;
- la comunicazione dei dati sui passeggeri ad altre autorità è stata circoscritta, e il trasferimento è stato limitato ai Paesi di cui sia stata accertata l'adeguatezza;
- è stato indicato l'obbligo di fornire un'adeguata informativa da parte del *Canada Border Service Agency*, così come l'impegno a garantire i diritti di accesso, rettifica e opposizione non solo alle persone interessate presenti in Canada;
- è stata infine prevista una verifica congiunta dell'attuazione degli impegni assunti.

Cd. Binding Corporate Rules

Il Gruppo art. 29 ha approvato nel corso del 2005 due documenti (WP 107, 14 aprile 2005 e WP 108, 14 aprile 2005) riguardanti le "regole vincolanti nell'impresa" (*Binding Corporate Rules*-Bcr). Le imprese, soprattutto multinazionali, hanno chiesto con riferimento all'autorizzazione al trasferimento dei dati, di poter dialogare con un solo interlocutore, anziché di volta in volta con le singole 25 autorità nazionali. Le Bcr sono uno degli strumenti attraverso i quali le imprese multinazionali potranno trasferire dati personali da Paesi Ue verso Paesi terzi non adeguati; esse potranno consentire alle autorità di protezione dati di svolgere una valutazione comparata nella prospettiva di garanzie auspicabilmente più uniformi e nel rispetto delle prerogative di ciascuna.

Il Gruppo ha definito gli aspetti procedurali nel documento WP 107, che prevede la designazione di un'autorità di protezione dati quale *leader* della valutazione, alla quale tutte le altre autorità interessate dovrebbero far capo per commenti e osservazioni. La designazione spetta alla società multinazionale, che dovrà rifarsi ai criteri indicati nel documento, fra i quali viene data priorità alla considerazione del Paese ove è situata la capogruppo o la sede centrale europea della multinazionale. Le autorità sono libere di accettare o meno tale designazione sulla base della documentazione prodotta dalla società, formulando eventualmente una controproposta. La procedura prevede, stabilita l'autorità-*leader*, l'elaborazione di una bozza finale di "regole vincolanti nell'impresa" da sottoporre alla valutazione congiunta di tutte le autorità interessate, coordinate dall'autorità-*leader*; l'accettazione della bozza è da intendersi come riconoscimento dell'adeguatezza delle norme in essa contenute e, quindi, come autorizzazione al loro impiego.

Il WP 108 integra e completa il documento precedente, fornendo indicazioni specifiche sui contenuti delle regole vincolanti nell'impresa. Il Gruppo ha elaborato una sorta di "*checklist*" che le imprese devono utilizzare per verificare che le rispettive Bcr rispondano ai principi fissati nella direttiva n. 95/46/Ce. In particolare, deve essere dimostrata l'effettiva vincolatività delle norme, sia rispetto all'interno del

gruppo (controllate, collegate, dipendenti, terzi fornitori), sia rispetto all'esterno, soprattutto ai fini dell'esercizio dei diritti riconosciuti agli interessati.

Interpretazione dell'art. 26 (1) della direttiva n. 95/46/Ce

Il Gruppo art. 29 ha adottato un documento di lavoro (WP 114, 25 novembre 2005) sul tema del trasferimento dei dati personali verso Paesi che non garantiscono un livello di protezione adeguato, al fine di fornire un'interpretazione che consenta un'applicazione uniforme negli Stati Ue dell'art. 26 (1) della direttiva n. 95/46/Ce, che prevede deroghe rispetto al principio di adeguatezza della destinazione enunciato nell'art. 25.

Il Gruppo ha sottolineato, in particolare, che le disposizioni dell'art. 26 (1) devono essere interpretate in modo restrittivo, e che le deroghe possono essere utilizzate solo nei casi in cui i rischi per l'interessato siano ridotti, o in cui si può ritenere che altri interessi prevalgano sul diritto dell'interessato alla riservatezza. Nel documento vengono inoltre formulate diverse raccomandazioni volte ad incoraggiare i responsabili del trattamento a garantire, nella maggior parte dei casi, l'uso "fisiologico" dell'art. 25; viene svolta poi un'analisi dei concetti di "consenso" e di "esecuzione di un contratto", deroghe sulle quali i responsabili del trattamento tendono a basarsi più di frequente.

Sistema Vis

Il Gruppo art. 29 ha adottato un parere (WP 110, 23 giugno 2005) sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione sui visti e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (sistema Vis). Secondo la proposta, l'archivio Vis verrebbe costituito da una banca dati centrale e da interfacce nazionali; sarebbe accessibile da sistemi nazionali collegati con i consolati e i posti di frontiera di ciascun paese partecipante; l'archivio conterrebbe i dati identificativi di tutte le persone che richiederanno visti di ingresso trimestrali per uno dei Paesi aderenti all'Accordo di Schengen. Oltre ai dati alfanumerici, sarebbero registrati anche i dati biometrici, in particolare la foto digitalizzata del richiedente e le sue impronte digitali.

Il Gruppo ha ritenuto che la raccolta massiccia di dati personali e biometrici in una banca dati centralizzata, in concomitanza con uno scambio di dati effettuato su larga scala e riguardante un enorme numero di persone, risulti gravemente rischiosa con riferimento alla garanzia dei principi fondamentali della protezione dati.

Per tale ragione, il Gruppo ha chiesto:

- che vengano specificate chiaramente ed esaustivamente le finalità del trattamento dei dati contenuti nel Vis, in rapporto alla politica comune sui visti che ne costituisce il fondamento giuridico;
- che siano stabiliti tempi di conservazione dei dati limitati e proporzionati;
- che siano definite con precisione le autorità abilitate ad introdurre dati nel Vis, così come a modificarli e a cancellarli, anche su richiesta dell'interessato.

Nel parere viene infine ribadita la necessità di individuare gli organismi che possono accedere al sistema (con particolare riguardo per le previste interconnessioni con il Sistema informativo Schengen), nonché di specificare meglio le funzioni di controllo e supervisione rimesse alla competenza delle autorità nazionali per la protezione dei dati personali.

Biometria nei passaporti

Dopo l'adozione della Decisione della Commissione sulle specifiche tecniche relative alle caratteristiche di sicurezza e agli elementi biometrici nei passaporti, il Gruppo art. 29 si è pronunciato (WP 112, 30 giugno 2005) sull'attuazione del regolamento comunitario relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri.

Il Gruppo, dopo aver ribadito i principi enunciati nel parere precedente e confermato le segnalazioni inviate al riguardo al Parlamento europeo, ha richiamato i

rischi legati all'acquisizione presso i cittadini europei di dati biometrici in forma digitalizzata, che potranno essere memorizzati in banche di dati centralizzate e resi disponibili per tutta una serie di scopi non tutti previsti. Per tale ragione, il Gruppo ha espresso ampie riserve riguardo alla costituzione di una banca dati centralizzata, sia europea, sia nazionale, di informazioni biometriche, la quale violerebbe il principio basilare della proporzionalità nel trattamento di dati personali.

Secondo il Gruppo, l'impiego della biometria va limitato ai soli scopi di verifica, allo scopo della comparazione dei dati inclusi nel documento, con i dati riscontrabili direttamente presso il detentore all'atto della presentazione del documento. Il Gruppo ha inoltre chiesto che possano avere accesso ai dati memorizzati nel *chip* solo le *"autorità competenti"* e che venga istituito un registro esaustivo delle medesime autorità e degli organismi autorizzati al trattamento.

Riguardo agli aspetti tecnici, il Gruppo art. 29 ha espresso forti perplessità sulla possibilità di garantire la sicurezza attraverso l'introduzione di *chip* "senza contatto" (*ad es.*, *tag Rfid*), nonché sull'opportunità dell'inserimento di caratteristiche biometriche direttamente nel *chip*. A questo proposito, il Gruppo si è invece espresso in favore dell'istituzione di un'infrastruttura globale a chiave pubblica (*Pki*).

Sis II

Il Gruppo art. 29 ha adottato un parere (WP 116, 25 novembre 2005), predisposto sotto il coordinamento della delegazione italiana, relativo alle proposte presentate dalla Commissione europea che definiscono l'istituzione di un nuovo sistema informativo (Sis II) destinato a sostituire l'attuale Sistema informativo Schengen (Sis). Il Sis è previsto e disciplinato dalla Convenzione Schengen e rappresenta uno strumento fondamentale per lo scambio di dati ai fini della non ammissione di stranieri segnalati nei Paesi aderenti alla Convenzione, nonché per favorire la cooperazione nelle attività di polizia.

Le nuove norme proposte prevedono per il futuro Sis II un ampliamento di natura funzionale e strutturale, oltre che in termini di contenuti. Le principali novità riguardano infatti: l'articolazione della banca dati centralizzata, unitamente alle nuove funzioni di tipo dinamico che si vogliono introdurre (in particolare, la possibilità di interconnessioni fra segnalazioni inserite per finalità diverse nel Sis II); le modalità di consultazione dei dati da parte delle autorità nazionali e degli organismi sopranazionali (Europol, Eurojust); la possibilità di inserire nuove categorie di dati compresi quelli di natura biometrica (immagine digitale del volto e impronte digitali); l'esercizio dei diritti riconosciuti agli interessati; i tempi di conservazione dei dati.

Il Gruppo ha evidenziato alcuni aspetti critici che si accompagnano alle proposte della Commissione, da armonizzare meglio ai principi di protezione dati sanciti dalla direttiva n. 95/46/Ce, ed ha segnalato, rispetto a ciascuno di tali punti, emendamenti da apportare.

Per quanto attiene alle finalità del Sis II e all'individuazione dei soggetti autorizzati ad accedervi, i Garanti ritengono che, allo stato, non sia possibile consentire l'accesso ad organismi quali Europol ed Eurojust, perché ciò contrasterebbe con le finalità del sistema come attualmente configurate. Con riferimento alla possibilità di interconnessioni fra i dati relativi alle segnalazioni inserite per finalità diverse, il Gruppo ha rilevato che occorrono norme più dettagliate sull'utilizzo di tale meccanismo e sui soggetti autorizzati ad accedere alle informazioni.

Il Gruppo ha altresì segnalato che l'utilizzo di dati biometrici per finalità identificative non può avvenire su base sistematica, dovendo essere previsto soltanto "caso per caso" e se realmente indispensabile. Per quanto attiene alla salvaguardia dell'effettivo esercizio dei diritti riconosciuti agli interessati, si è ritenuto peraltro necessario garantire un'informazione adeguata sulle possibilità di opporsi alla decisione

dello Stato sull'inserimento di segnalazione nel Sis. Infine, con riferimento alla durata della conservazione dei dati inseriti nel sistema, il Gruppo ha chiesto di mantenere il termine di tre anni attualmente previsto nella Convenzione Schengen.

Conservazione dei dati di traffico *"Data Retention"*

La conservazione preventiva e generalizzata dei dati di traffico interferisce con il diritto fondamentale alla riservatezza delle comunicazioni; per questo motivo, in linea generale, il Gruppo art. 29 ha sempre ritenuto che il ricorso a tale misura debba essere riservato solo a casi eccezionali e per motivate e pressanti esigenze sociali, nonché sulla base di adeguate e specifiche garanzie previste per legge.

Nel 2005 il Gruppo ha adottato un parere (WP 113, 21 novembre 2005) coordinato dal Garante in merito alla proposta di direttiva sulla conservazione dei dati presentata dalla Commissione europea nel mese di settembre (Com(2005)438; ora direttiva n. 2006/24/Ce), come parte di un "pacchetto" di misure messe a punto nel quadro della lotta contro il terrorismo e la criminalità organizzata. Il Gruppo, come già in varie occasioni dopo gli eventi del settembre 2001, ha voluto sottolineare la propria consapevolezza e condivisione rispetto alle sfide poste dal terrorismo e alla necessità di farvi fronte in modo efficace; tuttavia, ha precisato che ciò deve avvenire senza minare i principi e diritti fondamentali (ivi compreso il diritto alla *privacy*) che formano la base delle società democratiche.

La proposta di direttiva ha previsto un obbligo generalizzato per tutti i fornitori di servizi di comunicazione di conservare i dati di traffico per finalità non connesse alla fatturazione, bensì per scopi investigativi. Pur prendendo atto con favore dell'intento di armonizzare il quadro normativo europeo in questo campo, in cui sussistono numerose diversità, il Gruppo non ha ritenuto che le motivazioni addotte dalle competenti autorità dei Paesi membri a sostegno della conservazione obbligatoria dei dati fossero sufficientemente solide, in particolare rispetto al periodo massimo di conservazione previsto nella proposta.

In questo contesto, i Garanti hanno chiesto alla Commissione ed al Parlamento (chiamato a decidere congiuntamente sull'adozione della direttiva) di prevedere alcune garanzie essenziali, anche alla luce di altri strumenti internazionali come la Convenzione europea dei diritti umani:

- specificare chiaramente le finalità della conservazione dei dati, che devono essere connesse alla lotta contro il terrorismo e la criminalità organizzata, anziché contro generiche forme di "grave criminalità";
- indicare chiaramente a quali condizioni le autorità competenti potrebbero accedere ai dati in oggetto ed utilizzarli per combattere la minaccia del terrorismo;
- limitare al massimo il periodo di eventuale conservazione, chiarendo che esso rappresenta il tetto massimo applicabile dagli Stati membri (che però dovrebbero poter prevedere periodi più brevi);
- dare massima pubblicità alle misure introdotte;
- prevedere un riesame periodico delle motivazioni alla base delle misure di conservazione obbligatoria dei dati (almeno ogni 2-3 anni);
- prevedere che, in ogni caso, si tratti di misure ad applicazione limitata nel tempo (3 anni) proprio per la natura circostanziale delle motivazioni che stanno alla base della proposta della Commissione.

I Garanti hanno richiamato queste ed altre specifiche garanzie in forma sintetica in un elenco finale recante venti prescrizioni. Tra esse vanno citati almeno: il divieto di trattamenti ulteriori dei dati conservati (se non in presenza di rigide e specifiche garanzie); l'opportunità di autorizzare l'accesso caso per caso attraverso decisioni dell'autorità giudiziaria o, comunque, delle autorità competenti; la predisposizione di misure concernenti la sicurezza e la separazione logica dei dati che i fornitori di

servizi devono adottare; la definizione precisa delle categorie di dati da conservare e la previsione di meccanismi di revisione di tali categorie; la necessità di escludere in ogni caso i dati relativi ai contenuti delle comunicazioni.

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

Il 2005 ha visto un'accelerazione delle iniziative legislative proposte dalla Commissione per rafforzare la cooperazione tra le autorità nazionali di polizia e giudiziarie.

Tra le più importanti, si segnalano le proposte per una nuova base legale del Sistema informativo Schengen e per la creazione del Sis II, presentate dalla Commissione il 31 maggio 2005, la bozza e la direttiva in materia di conservazione dei dati di traffico telefonico e telematico a fini di repressione dei reati. Altra proposta ufficialmente presentata dalla Commissione e da tempo auspicata ed attesa dai Garanti europei è quella relativa ai principi in materia di protezione dei dati nel Terzo pilastro.

L'attività del Garante nell'Autorità di controllo comune Schengen

Il Garante continua ad esercitare le funzioni di autorità nazionale per il controllo indipendente dell'archivio della sezione italiana del Sis e per 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, fa parte dell'Autorità di controllo comune (Acc).

Fra le attività di maggior rilievo dell'Acc, alle cui riunioni il Garante ha partecipato 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 (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.

Gran parte dell'attività dell'Acc ha continuato ad essere concentrata sui problemi legati allo sviluppo del Sistema informativo Schengen, il *cd.* Sis II. Il passaggio dall'attuale al nuovo sistema determinerà l'introduzione di nuove funzioni e di ulteriori dati tra cui, in particolare, dati biometrici (foto digitalizzate ed impronte digitali). È inoltre prevista l'interoperabilità tra Sis, Vis ed Eurodac per creare una sinergia tra grandi *data-base* europei e l'estensione delle possibilità di accesso al sistema per Europol ed Eurojust.

Le nuove categorie di informazioni e i nuovi tipi di dati, l'accesso al Sis e l'uso dei dati nel sistema, inclusa la possibilità di una loro trasmissione a Paesi terzi, sembrano volte a trasformare il Sis in un sistema di indagine e non più solo di informazione, mutandone quindi sensibilmente le finalità rispetto a quelle definite dalla Convenzione del 1990.

L'Autorità ha adottato un lungo ed articolato parere sulle proposte presentate dalla Commissione nel mese di settembre, ribadendo le preoccupazione espresse nei precedenti pareri e offrendo anche formulazioni diverse per la discussione sul testo.

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

L'Autorità comune di controllo Europol ha proseguito la sua attività esprimendo, in particolare, un parere sul trasferimento di dati verso l'Australia.

Come già indicato nella precedente *Relazione*, si è svolta la consueta ispezione

annuale degli archivi che, come deliberato dall'Acc, si è concentrata sull'esame dei dati di natura personale trasmessi nell'ambito dell'accordo e sulla qualità dei dati trattati.

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. Il comitato ricorsi ha deciso in merito a due ricorsi.

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). 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. L'Autorità si è riunita una volta nel 2005.

Permangono i temi problematici già presentati nella scorsa *Relazione*, legati alla mancanza di risorse proprie per costituire il *team* di esperti che dovrebbe svolgere la prima ispezione al Sid, nonché allo scarso utilizzo del sistema da parte delle autorità doganali, che preferiscono in genere utilizzare canali bilaterali per gli scambi di informazioni.

Eurodac

Per quanto concerne Eurodac, la grande base di dati europei che contiene le impronte digitali dei richiedenti asilo e delle persone fermate dalla autorità di frontiera in posizione irregolare è attualmente affidata al Garante europeo per la protezione dei dati personali (Gepd). Nel 2005 il Gepd ha organizzato una riunione di coordinamento con le autorità nazionali di protezione dei dati per iniziare una collaborazione e verificare sulla base della comune esperienza la liceità dei trattamenti effettuati.

22.3. *Partecipazione ad altri comitati e gruppi di lavoro*

Circa Complaint

Gli incontri previsti nell'ambito della rete istituita fra le autorità europee per la protezione dei dati ai fini dello scambio di informazioni sulle casistiche nazionali e sul contenzioso si sono tenuti nel corso dell'anno a Budapest (10-11 marzo 2005) e a Parigi (17-18 novembre 2005).

Facendo seguito alle indicazioni emerse dal precedente *workshop* di Praga (novembre 2004), a partire dall'incontro di Budapest si è sperimentata una nuova formula di organizzazione, in base alla quale si prevede di dedicare una mezza giornata di riunione alla trattazione approfondita di un tema di interesse, attraverso sessioni parallele.

Tale approccio si è dimostrato efficace ed è stato quindi formalizzato in occasione della *Spring Conference* di Cracovia, che ha stabilito anche la nuova denominazione dei seminari, ora ribattezzati "*Case Handling Workshops*" (seminari sulla trattazione della casistica nazionale), per sottolineare anche l'ampliamento dell'ambito di discussione, non più limitato ai soli "ricorsi", ma riguardante l'intera gamma delle attività condotte dalle autorità nazionali sulle quali si ritenga necessario confrontarsi.

In tale sede è stata ribadita, inoltre, l'opportunità di concretizzare i risultati dei *workshop* sotto forma di documenti o proposte da sottoporre ai soggetti competenti

(in primo luogo, la *Spring Conference*, ma anche il Gruppo art. 29) nell'ottica di favorire la diffusione e l'elaborazione di *best practice*.

I temi affrontati nel corso del 2005 hanno riguardato, in particolare:

- le attività di ispezione e controllo svolte dalle autorità nazionali e le relative modalità esecutive. In proposito, l'autorità italiana ha formulato la proposta di istituire una lista di punti di contatto in materia di ispezioni e controlli, per facilitare lo scambio di informazioni e la rapida definizione di questioni controverse che investano più Paesi, così da redigere una possibile lista di "buone pratiche", basate sull'esperienza sinora formatasi in materia di controlli ed ispezioni, da utilizzare quale strumento per potenziare l'efficacia delle attività nei Paesi che già le hanno avviate, nonché come possibile impulso per i Paesi che ne stanno impostando le linee direttrici;
- i problemi connessi alla creazione di *black list* per la telefonia mobile, anche alla luce dell'assenza di norme specifiche nella maggioranza dei Paesi Ue;
- il trattamento di dati sanitari, con particolare riguardo alle istanze di accesso degli interessati ai dati relativi alla salute detenuti da strutture sanitarie, società di assicurazione e datori di lavoro, nonché al funzionamento dei sistemi nazionali basati sull'istituzione di "cartelle cliniche elettroniche" con tutti i problemi connessi;
- il trattamento dei dati nel settore bancario, soprattutto a seguito dell'adozione degli accordi "Basilea II" (in materia di lotta al riciclaggio e alla frode);
- il rapporto con i *media* e le opportunità di sensibilizzazione pubblica da ciò derivanti, con riguardo alla necessità di curare i rapporti con la stampa ed i *media* attraverso personale specializzato, e di elaborare strategie di *marketing* (in senso lato) che consentano di massimizzare la presenza delle autorità di protezione dei dati in tutti i settori della società;
- altri temi di attualità. Tra di essi, si segnalano le problematiche connesse alla legge Sarbanes-Oxley (che impone la comunicazione ad autorità Usa di dati relativi all'affidabilità di consulenti e revisori in materia contabile) e al correlato fenomeno del "*whistleblowing*" (segnalazioni anonime effettuate da dipendenti di un'azienda attraverso linee dedicate, cosiddette "*integrity lines*"); la raccolta di dati connessi all'origine razziale ed etnica per finalità antidiscriminatorie o per la tutela delle pari opportunità; la tutela della proprietà intellettuale in Internet; il rapporto fra comunicazione politica e diritto alla *privacy*.

Su tali punti, le autorità hanno convenuto di proseguire la discussione nei prossimi mesi.

Consiglio d'Europa

I temi più importanti, affrontati dal Comitato consultivo della Convenzione n. 108/1981 (T-Pd) nel corso del 2005, hanno riguardato l'applicazione dei principi di protezione dati alle reti telematiche e l'applicazione dei principi della Convenzione del Consiglio d'Europa alla raccolta e al trattamento dei dati biometrici.

Sul primo punto, uno studio commissionato dal Consiglio d'Europa ad esperti esterni ha evidenziato alcune problematiche legate a recenti sviluppi che sembrerebbero indicare l'opportunità della ridefinizione del concetto di identità, profondamente mutato nella direzione di una frammentazione crescente dell'identità personale e di una crescente difficoltà, per l'utente Internet, di veder garantiti i propri diritti.

Lo studio in esame ha affrontato in modo specifico il concetto di autodeterminazione informativa nel contesto di Internet, evidenziando i rischi connessi ai trattamenti di dati "invisibili" e la necessità di promuovere un approccio tecnologico alla tutela dei dati personali, intervenendo nella fase di configurazione dei sistemi

informativi. Fra i rischi legati all'impiego delle nuove tecnologie, l'attenzione del Consiglio d'Europa si è focalizzata, in particolare, sui temi della profilazione e dell'effettività del consenso.

In materia di trattamento di dati biometrici, è stato pubblicato un rapporto sullo stato di avanzamento dell'analisi dell'applicazione dei principi della Convenzione al trattamento di tali dati. Tale rapporto intende rappresentare "lo stato dell'arte", in particolare al fine di contribuire al dibattito internazionale, che in più sedi (*ad es.*, Ocse, Ue) ha posto al centro dell'attenzione le molte tematiche connesse alle tecnologie biometriche.

Avendo descritto le specificità della biometria e dei sistemi che utilizzano indicatori biometrici, con particolare riguardo all'architettura centralizzata o decentralizzata di tali sistemi e alle rispettive implicazioni in termini di protezione dei dati, il rapporto esamina in particolare l'applicazione delle singole disposizioni della Convenzione a questa costellazione di trattamenti. Pur senza giungere a conclusioni definitive, il T-Pd segnala che i principi della Convenzione sono idonei a mantenere la propria validità anche rispetto ai trattamenti legati all'impiego di sistemi biometrici, risultando opportuna, prima del ricorso a tali sistemi, la verifica da parte del titolare del trattamento relativa all'esistenza e alla praticabilità di opzioni meno invasive. Infatti, attraverso il ricorso a identificatori biometrici viene incrementata la possibilità di ledere la dignità delle persone, anche in base alla circostanza per cui i dati risultano direttamente "prelevati" dal corpo umano e possono restare inalterti nel corso della vita.

Fra le altre iniziative sviluppate dal T-Pd merita almeno un cenno la proposta di istituire una "giornata europea della protezione dei dati", alla quale potrebbero associarsi iniziative a livello nazionale per sensibilizzare i cittadini rispetto ai loro diritti e alle attività delle autorità nazionali.

Ocse

Il Garante ha partecipato anche nel 2005 ai lavori del gruppo che in seno all'Ocse si occupa dei temi legati alla *privacy*. Il *Working Party on Information Security and Privacy* (Wpisp) ha proseguito il suo impegno sul tema della sicurezza, già considerato come tema prioritario a partire dal 2001, e si è concentrato in particolare sull'attuazione delle linee-guida. Grazie al lavoro di sintesi condotto dal segretariato sulla base delle risposte ad un questionario inoltrato alle delegazioni nazionali, è emersa l'indicazione di quattro settori prioritari ai quali dedicare l'attenzione del gruppo nel prossimo futuro: incentivazione dell'attività di sensibilizzazione rispetto al tema della sicurezza, soprattutto nei confronti delle amministrazioni locali e degli utenti finali; censimento condotto a livello nazionale con riferimento ai *Computer Emergency Response Team* (Cert), e sviluppo delle relative potenzialità attraverso la raccolta degli eventi più significativi che si verificano in rete; incremento della protezione delle infrastrutture critiche e analisi di dettaglio sui temi della sicurezza legati all'*e-Government*; sviluppo di indicatori attendibili in grado di misurare le spese pubbliche e private dedicate alla sicurezza.

Fra gli altri temi discussi nell'ambito del Wpisp in riferimento alla sicurezza nell'uso delle nuove tecnologie, meritano di essere menzionati almeno quelli legati ai sistemi di autenticazione elettronica e all'*Rfid*. Con riferimento al primo tema, la discussione si è soffermata sulla necessità di rendere più coerenti i differenti approcci nazionali, di sviluppare adeguati strumenti che agevolino l'interoperabilità, di censire le *best practice* in tema di autenticazione, di promuovere la conoscenza dei benefici che derivano dall'autenticazione, di stabilire un dialogo fra le differenti giurisdizioni nazionali nell'utilizzo dell'autenticazione e di approfondire lo studio delle possibili vie per gestire i problemi connessi all'identità digitale.

Per quanto riguarda l'*Rfid*, l'Ocse ha organizzato nel mese di ottobre 2005 un

forum dedicato al tema, nell'ambito del quale si sono confrontati soggetti pubblici, esponenti del mondo dell'industria, dell'università e della società civile. Numerosi interventi hanno evidenziato l'ampia gamma di applicazioni di questa tecnologia, confrontandoli con i rischi emersi in riferimento alla sicurezza e alla *privacy*.

Più in generale, vale la pena ricordare i lavori avviati sui modelli di informativa e sulla cooperazione nelle attività di implementazione della normativa in materia di *privacy*.

Rispetto all'elaborazione di modelli di informativa, occorre ricordare che il Gruppo art. 29 aveva già indicato la strada di un approccio "stratificato" nella redazione delle informative *on-line*, attraverso un documento pubblicato al termine del 2004 del quale si è riferito nella *Relazione* 2004 (p. 142). Nell'approccio del Gruppo, la "soluzione in prima battuta" dovrebbe essere rappresentata dalla versione sintetica dell'informativa, con la possibilità di spostarsi agevolmente ai livelli successivi (caratterizzati da più ampi dettagli e indicazioni), qualora l'interessato ritenga necessario approfondire il quadro relativo al trattamento.

In questa stessa prospettiva, si situa la riflessione condotta in ambito Ocse sulla *cd. Multilayered Information Notice*, al fine di ottenere informative "facili da leggere", complete nei contenuti ed omogenee. Secondo l'Ocse, gli strumenti comunicativi utilizzabili a tale scopo sono riconducibili, sostanzialmente, a tre modelli: un'informativa molto breve, quando lo spazio è molto limitato; un'informativa "concentrata", che consenta comunque di far presente gli elementi essenziali (titolare del trattamento, tipo di dati, modalità e finalità del trattamento, natura obbligatoria o facoltativa, recapito per contattare l'organizzazione); un'informativa completa ed approfondita, disponibile su richiesta dell'interessato. E' stato perciò proposto di elaborare un documento-guida per l'elaborazione di modelli idonei di informativa da parte delle imprese e dei governi.

Il Wpisp ha inoltre ritenuto di occuparsi nuovamente del flusso transfrontaliero dei dati, partendo dalla considerazione che la globalizzazione pone nuove sfide che non potevano essere state previste dalle linee-guida Ocse del 1980.

In particolare, si è fatto esplicito riferimento alla diffusione crescente di documenti di identità che contengono dati biometrici, all'impiego sempre più diffuso di forme di *outsourcing* nella gestione dei dati, alle tracce lasciate dall'impiego di tutte le nuove tecnologie e alla raccolta senza precedenti di dati personali da parte delle autorità pubbliche, connessa a motivi di sicurezza e lotta al terrorismo. Questi fenomeni comportano una crescita esponenziale della circolazione transfrontaliera di dati che diventa più rischiosa quando i dati personali vengono trattati in Paesi nei quali la tutela non è sufficiente, soprattutto con riferimento alla possibilità di esercizio dei diritti di accesso e di rettifica. Per tali ragioni è necessario stabilire procedure condivise che facilitino l'assistenza reciproca in ambito applicativo quando si affrontano questioni che coinvolgono una pluralità di Stati. É stato così proposto di condividere le rispettive conoscenze ed esperienze soprattutto nel settore dell'applicazione transfrontaliera delle norme di legge. A tale riguardo l'esperienza del Gruppo art. 29 nel settore dell'*enforcement* è stata segnalata come esempio virtuoso cui ispirarsi nel trovare soluzioni a problemi comuni.

Il punto di partenza di questa riflessione potrebbe essere rinvenuto nei principi già presenti nelle linee-guida Ocse del 1980. Per questi motivi è stata avviata una riflessione che resta suscettibile di portare all'adozione di nuove linee-guida, ovvero di un protocollo addizionale alle linee-guida, che affrontino il tema di cooperazione transfrontaliera in materia di *enforcement*.

In particolare si ritiene necessario:

- garantire che i cittadini e i residenti di altri Paesi possano esercitare i loro