22 Le relazioni internazionali

Le conferenze tra autorità di protezione dei dati a livello europeo

Le autorità di protezione dati europee si sono incontrate in primavera, in un'occasione divenuta ormai istituzionale (*Spring Conference*), a Budapest il 24 e il 25 aprile 2006. Durante la conferenza è stata adottata un'importante dichiarazione dedicata alle garanzie in tema di protezione dei dati con riferimento al potenziamento dello scambio e della circolazione di informazioni nel settore giudiziario e di polizia. Le autorità hanno ribadito che l'applicazione del principio di disponibilità –secondo il quale tutti i dati in possesso delle autorità giudiziarie e di polizia dei singoli Stati dovranno essere resi accessibili, in linea di principio, alle omologhe autorità degli altri Paesi– deve essere associato ad un sistema di tutela della protezione dati particolarmente elevato ed armonizzato a livello comunitario. Per tale motivo le autorità hanno affermato la necessità di creare, nell'ambito del *cd.* "terzo pilastro", un quadro di riferimento che garantisca il giusto equilibrio nello scambio di informazioni tra le autorità giudiziarie e di polizia, bilanciando sicurezza dei cittadini europei da un lato, e le libertà civili dall'altro nel rispetto del principio di proporzionalità. I Garanti hanno fatto appello ai Parlamenti (europeo e nazionali) e ai Governi affinché sia prestata particolare attenzione alle libertà dei cittadini, soprattutto nel momento in cui la possibilità di scambio di informazioni si intensifica.

Nell'ambito della Conferenza, il Garante è intervenuto nelle sessioni dedicate all'impiego della tecnologia *Rfid* e ai dati genetici (*v.* anche *par.* 23.4).

Conferenze delle autorità su scala internazionale

La 28ma Conferenza internazionale delle autorità per la protezione dei dati, al momento presenti in 58 Paesi, si è svolta a Londra il 2 e il 3 novembre 2006, ed è stata dedicata al tema della *"Società della sorveglianza"*.

Il dibattito si è focalizzato sui rischi e sui benefici dello sviluppo tecnologico associati alle attività di sorveglianza. Si tratta di pericoli che, nel caso di una sorveglianza occulta, eccessiva o incontrollata travalicano l'ambito della protezione dei dati investendo l'intera trama della società civile. In tale nuovo contesto, le autorità per la *privacy* sono chiamate a sviluppare strategie innovative anche per comunicare con più efficacia la fondamentale importanza che assume oggi la tutela dei dati personali. Ciò comporta un contatto ravvicinato con i legislatori e la messa a punto di nuovi approcci e strumenti comunicativi per sensibilizzare maggiormente i cittadini di ogni paese sui diritti legati alla protezione della vita privata.

La conferenza si è conclusa con l'adozione di una dichiarazione concernente le prospettive della difesa della *privacy* nel mondo globalizzato. *"Comunicare la protezione dei dati e potenziarne l'efficacia"* è stato il significativo titolo dell'iniziativa, che dopo aver rinvenuto nel ritmo dei mutamenti tecnologici, nello sviluppo di nuove norme anti-terrorismo e nella non sempre positiva percezione del ruolo e delle funzioni delle autorità di protezione dei dati i maggiori rischi per le libertà personali, individua linee di azione per il futuro. Si è previsto perciò un forte impegno delle autorità nel definire e attuare modalità innovative, maggiormente efficaci e mirate, che migliorino la cooperazione tra le stesse e consentano, sui diversi temi affrontati, di sviluppare azioni congiunte e coordinate e un'approfondita riflessione volta ad individuare le forme ed i modi per un più incisivo riconoscimento istituzionale delle autorità e del loro ruolo a livello internazionale.

Durante la conferenza sono state inoltre adottate dai Garanti due risoluzioni, la prima concernente la tutela della *privacy* in rapporto ai motori di ricerca, la seconda relativa ad alcune modifiche organizzative per aumentare l'impatto e la visibilità della conferenza stessa.

Alla conferenza ha partecipato l'intero Collegio del Garante. Il segretario generale Giovanni Buttarelli è intervenuto in una sessione dedicata al ruolo delle autorità di controllo di fronte alle nuove tecnologie (*v. par.* 23.4).

Nel corso della conferenza di Londra le autorità europee per la *privacy* hanno anche adottato una dichiarazione sulla protezione dei dati nelle attività di cooperazione giudiziaria e di polizia, in linea con quella adottata nella *Spring Conference*, e hanno ribadito la necessità di assicurare un quadro di garanzie in materia di protezione dei dati nel "terzo pilastro".

Conferenza internazionale sul trasferimento dei dati

Nel mese di ottobre si è tenuta a Bruxelles una conferenza internazionale sul trasferimento dei dati, organizzata dalla Commissione europea, dal Gruppo art. 29 e dalla *Federal Trade Commission* statunitense. Tale conferenza ha rappresentato la prosecuzione di un incontro svoltosi nel 2005 negli Usa con l'intento di chiarire gli aspetti controversi e incrementare l'utilizzo dell'accordo *Safe Harbor* per il trasferimento dei dati, ma ha allargato il tema di riflessione a tutti i principali strumenti previsti dalla direttiva n. 95/46/Ce, o comunque utilizzati al fine di garantire che il trasferimento dei dati fuori dall'Unione europea non comporti un affievolimento delle tutele previste nel quadro normativo europeo. Il Garante ha avuto un ruolo molto rilevante nel corso dei lavori, avendo ricevuto il compito di coordinare il *workshop* di apertura dedicato al *Safe Harbor* (in persona del segretario generale Giovanni Buttarelli) e quello di chiusura dedicato alle prospettive del trasferimento dei dati in un mondo globalizzato (in persona del presidente Francesco Pizzetti).

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

Procedure interne di denuncia

Il Gruppo art. 29 (che riunisce i rappresentanti delle autorità per la protezione dei dati europee, ed è stato istituito ai sensi dell'art. 29 della direttiva n. 95/46/Ce) si è pronunciato all'inizio del 2006 su un tema tuttora non uniformemente disciplinato nei paesi dell'Unione europea: la pratica di creare procedure di denuncia all'interno delle società (*cd.* "*whistleblowing*"; Wp 117). Il Gruppo si è in particolare soffermato, nella sua analisi, sulle procedure di denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli interni, la revisione dei conti, la lotta contro la corruzione e la criminalità bancaria e finanziaria, e ha fornito linee-guida per le imprese che intendano introdurle.

Procedure del genere, che possono aiutare un'impresa ad attuare correttamente i principi di governo societario e ad individuare fatti passibili di comprometterne la posizione, devono essere infatti attuate nel rispetto della direttiva n. 95/46/Ce, con particolare riferimento al diritto fondamentale alla protezione dei dati personali sia del denunciante, sia del denunciato.

Il Gruppo ha ribadito che i principi della direttiva devono essere applicati integralmente alle procedure di denuncia. In particolare, i sistemi di segnalazione devono essere finalizzati all'adempimento di un obbligo legale, imposto dal diritto comunitario o dal diritto degli Stati membri, diretto a istituire procedure di controllo interno in settori specifici, ovvero ritenuti necessari per il perseguimento dell'interesse legittimo del responsabile del trattamento. Tale interesse legittimo va però valutato e bilanciato con l'interesse o i diritti e le libertà fondamentali della persona.

22

Altri aspetti analizzati in dettaglio riguardano l'applicazione dei principi relativi alla qualità e alla proporzionalità dei dati trattati (limitazione del numero di soggetti autorizzati a denunciare presunte irregolarità, limitazione del numero dei soggetti denunciabili, promozione delle denunce nominative riservate rispetto a quelle anonime), l'obbligo di informativa, le misure di sicurezza da adottare nei trattamenti posti in essere, l'osservanza dei termini di conservazione dei dati, il diritto del denunciato di accedere ai dati che lo riguardano, di chiederne la rettifica o la cancellazione.

Vengono anche forniti suggerimenti riguardo alla gestione delle procedure di denuncia e, in particolare, è indicata l'opportunità per l'impresa di istituire un organo specifico preposto alla gestione delle denunce e all'attività di verifica, composto da personale in possesso di un'apposita formazione e vincolato da precisi obblighi di riservatezza.

Il Gruppo ha ritenuto che, se l'impresa è una multinazionale, in applicazione del principio di proporzionalità la valutazione delle denunce dovrebbe svolgersi a livello locale, ossia in un Paese dell'Unione europea, senza una condivisione automatica da parte di tutto il gruppo di imprese. Qualora, poi, le procedure comportino la possibilità di un trasferimento di dati verso Paesi terzi che non presentano un livello adeguato di protezione dei dati, le informazioni trattate potranno essere effettivamente trasferite solo in presenza del necessario presupposto giuridico, e cioè se il destinatario ha aderito al *Safe Harbor* (nel caso in cui abbia sede negli Usa), ha sottoscritto le clausole contrattuali *standard*, ovvero ha adottato Bcr (*v. par.* 11).

Servizi di filtraggio delle *e-mail*

La diffusione ormai capillare dei servizi di posta elettronica si accompagna alla disponibilità di sistemi che mirano a ridurre le "interferenze" estranee alla comunicazione (i *cd.* "filtri" per l'eliminazione, *ad es.*, di *spam* o *virus*) ma possono configurare, per le loro caratteristiche tecniche, un'interferenza nella libertà di comunicazione. Le autorità di protezione dati hanno inteso fornire alcune specifiche indicazioni agli operatori del settore (in particolare, Isp e gestori di servizi di posta elettronica) anche alla luce dei principi della direttiva n. 2002/58/Ce (Wp 118).

Oltre a ricordare le salvaguardie che devono associarsi alle attività di scansione delle *e-mail,* il documento sottolinea la necessità di incorporare i principi di tutela della *privacy* nel *software* utilizzato per la gestione della posta elettronica, riducendo al minimo il trattamento di dati personali e ricorrendovi soltanto per lo stretto indispensabile al raggiungimento delle finalità della comunicazione.

Il parere chiarisce che un *provider* può scansionare lecitamente la posta elettronica alla ricerca di *virus* o *spam* senza il consenso dell'utente/abbonato, purché si rispettino determinate garanzie (fra cui quella di un'adeguata informativa); viceversa, non può scansionare la posta elettronica in cerca di contenuti potenzialmente illegali (*ad es.*, *file* pornografici o di contenuto razzista) perché questo tipo di operazioni rappresenterebbe una forma di intercettazione delle comunicazioni.

Rispetto allo *screening* della posta elettronica effettuato per l'individuazione di *virus*, il documento sottolinea che si tratta di un obbligo in materia di sicurezza imposto, fra l'altro, dall'art. 4 della direttiva n. 2002/58/Ce. In quanto tale, esso non necessita del consenso dell'utente; tuttavia, il *provider* deve astenersi dal rivelare il contenuto della comunicazione e limitare l'analisi dei contenuti alla sola ricerca di possibili *virus*.

Peraltro, anche lo *screening* anti-*spam* è ritenuto assimilabile ad una misura di sicurezza, poiché lo *spam* può compromettere la funzionalità dei servizi di posta elettronica in quanto tali; tuttavia, i *provider* vengono invitati a consentire agli utenti la disattivazione dei sistemi di filtraggio, nonché l'indicazione caso per caso dei messaggi individuati come *spam* che di fatto non lo siano, e dei tipi di *spam* da filtrare,

Direttiva sulla conservazione dei dati di traffico

in modo da non limitare la libertà di comunicazione. Resta fermo il principio sopra accennato, in base al quale la ricerca di specifici contenuti, potenzialmente illeciti, può configurare una vera e propria intercettazione delle comunicazioni, e pertanto non può rientrare negli obblighi *standard* dei *provider* dovendo essere fornita, eventualmente, come servizio opzionale sulla base del consenso dell'utente.

Nella *Relazione* 2005 (pp. 147 ss.) si è svolta un'ampia disamina della proposta di direttiva in materia di conservazione dei dati di traffico per finalità di ordine pubblico e di contrasto all'attività criminosa, nonché dell'attività svolta al riguardo dalle autorità di protezione dei dati personali a livello europeo.

A seguito dell'adozione, il 15 marzo 2006, della direttiva n. 2006/24/Ce del Parlamento europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (che modifica in parte la direttiva n. 2002/58/Ce), le autorità di protezione dei dati europee sono nuovamente intervenute per rappresentare le notevoli preoccupazioni rispetto alle disposizioni introdotte (Wp 119).

Dopo aver richiamato il parere fortemente critico espresso sull'allora proposta di direttiva –*cfr*. il Wp 113 del 21 ottobre 2005– le autorità di protezione dei dati hanno ribadito che le disposizioni della direttiva, fondate sulla decisione, senza precedenti, di conservare per anni tutti i dati di comunicazione, avranno conseguenze di ampia portata per tutti i cittadini europei e per la loro *privacy*. La motivazione di tale conservazione, ovvero la necessità di contrastare gravi forme di reati, non rende la misura meno invasiva: la massiccia raccolta e conservazione invade infatti la vita quotidiana di ogni cittadino e può porre a repentaglio i valori e le libertà fondamentali di cui godono i cittadini europei.

Preso atto dell'adozione della direttiva, le autorità di protezione dei dati hanno chiesto almeno che, nell'attuare la direttiva, ogni Stato membro adotti provvedimenti atti a ridurne l'incidenza sulla *privacy* delle persone. Il Gruppo ha anche sottolineato come nel testo manchino adeguate e specifiche garanzie rispetto al trattamento dei dati comunicati lasciando spazio alla possibilità di interpretazioni e attuazioni divergenti tra gli Stati membri. Le autorità hanno dunque ritenuto d'importanza cruciale che le disposizioni della direttiva siano interpretate e attuate secondo modalità armonizzate, tali da assicurare ai cittadini il medesimo grado di tutela in tutta l'Unione europea.

Risulta fondamentale al riguardo che vi sia uniformità di previsioni e di garanzie rispetto a quanto segue:

- *indicazione precisa dello scopo*. I dati vanno conservati soltanto per scopi specifici. Di conseguenza, si deve definire e determinare con chiarezza il concetto di "reati gravi". Ogni altro trattamento dei dati va escluso, oppure limitato rigorosamente in base a specifiche garanzie;
- *limitazione dell'accesso*. I dati devono essere disponibili soltanto ad autorità garanti della legge, specificamente individuate in un elenco reso pubblico, quando tale accesso sia necessario ai fini delle indagini rivolte all'accertamento ed al perseguimento dei reati menzionati nella direttiva. Di ogni accesso deve essere mantenuta una registrazione (*log*); occorre inoltre un controllo sulle registrazioni da parte dell'autorità di vigilanza;
- *minimizzazione dei dati da conservare*. I dati da conservare vanno limitati al minimo e ogni aggiunta va testata per accertarne l'assoluta necessità;
- *selezione dei dati da recuperare*. Le indagini, gli accertamenti e il perseguimento di reati gravi non devono comportare il recupero generalizzato, da parte delle autorità giudiziarie e di polizia, dei dati, tra quelli conservati,

riguardanti le abitudini in fatto di spostamenti e di comunicazioni di persone non sospette;
- *esame giudiziale/indipendente dell'accesso autorizzato*. L'accesso ai dati va autorizzato caso per caso dalle autorità giudiziarie, ad eccezione di quegli Stati in cui una specifica possibilità di accesso è prevista dalla legge ed è soggetta a supervisione indipendente. Se possibile, nelle autorizzazioni si devono precisare quali particolari dati sono necessari per il caso specifico in questione;
- *scopi dei prestatori di servizi*. I prestatori di servizi pubblici di comunicazione o gestori di reti telematiche non sono autorizzati ad elaborare per altri fini, in particolare per finalità loro proprie, i dati conservati unicamente a scopi di ordine pubblico;
- *separazione dei sistemi*. I sistemi di memorizzazione dei dati per le finalità della direttiva (ordine pubblico) devono essere separati logicamente dai sistemi utilizzati per fini commerciali;
- *misure di sicurezza*. Devono essere definite norme riguardanti le misure di sicurezza di natura tecnica ed organizzativa che i suddetti prestatori di servizi devono adottare.

Obbligazioni alimentari

Il Gruppo art. 29 ha approvato un parere sulla proposta di regolamento del Consiglio relativa alla competenza, alla legge applicabile, al riconoscimento e all'esecuzione delle decisioni e alla cooperazione in materia di obbligazioni alimentari (Wp 123). In tale parere il Gruppo, oltre a formulare osservazioni specifiche sui singoli articoli del Capo VIII della proposta di regolamento –che disciplinano la raccolta di informazioni relative alla situazione del creditore e del debitore e allo scambio di dati tramite una rete di autorità centrali nazionali– ha ribadito la necessità di ottemperare alle regole della direttiva n. 95/46/Ce, e in particolare ai principi di finalità e di *data quality* stabiliti nell'art. 6, ai criteri che rendono legittimo un trattamento previsti dall'art. 7, alle particolari garanzie previste per i dati sensibili dall'art. 8, e agli altri obblighi in materia di informativa, diritto di accesso e misure minime di sicurezza.

Progetto *eCall*

Fra le molte iniziative in ambito europeo per promuovere la sicurezza stradale (progetto *"eSafety"*), quella denominata *"eCall"* è volta all'introduzione di un sistema telematico europeo per le chiamate di emergenza in caso di incidenti stradali.

Il sistema *eCall* non è ancora implementato a livello Ue; l'obiettivo del gruppo di lavoro che ne sta sviluppando le caratteristiche è di renderlo disponibile su tutte le vetture prodotte dal 1° settembre 2010 in poi. Il Gruppo art. 29 ha ritenuto opportuno fornire alcune indicazioni operative in considerazione delle molteplici implicazioni relative alla protezione dei dati personali degli utenti e dei proprietari coinvolti, sottolineando che l'alta utilità sociale del progetto non può comportare una riduzione delle garanzie fissate nella direttiva sulla protezione dei dati e nelle leggi nazionali in materia (Wp 125). Le linee-guida elaborate dal Gruppo dei garanti europei potranno dunque incidere sin d'ora sulla configurazione definitiva del sistema.

Il sistema *eCall*, se installato a bordo di un'autovettura, consentirà di generare una chiamata d'emergenza sia manualmente da parte degli occupanti, sia automaticamente attraverso l'attivazione di alcuni sensori (analoghi a quelli degli *airbag*). In tal modo sarà stabilita una connessione vocale direttamente con la centrale del 112 (numero di emergenza europeo) competente; contemporaneamente saranno inviate al medesimo operatore di centrale operativa ricevente alcune informazioni più direttamente relative all'incidente. È possibile anche l'invio di informazioni ulteriori (*cd. "Full Data Set"*) a terzi (compagnie assicurative, officine, enti previdenziali) sulla base di specifici accordi fra l'utente/proprietario del veicolo e tali soggetti. Il

funzionamento del sistema si fonda su un *Memorandum* d'Intesa sottoscritto fra la Commissione europea, le case produttrici di autovetture e gli Stati membri dell'Ue, in cui sono fissati i principi fondamentali.

Il Gruppo ha riconosciuto in prima battuta che il sistema *eCall*, come attualmente configurato, è compatibile con la direttiva sulla protezione dei dati. Gli elementi valutati positivamente dal Gruppo dei garanti comprendono la chiara indicazione della titolarità del trattamento dei dati trasmessi (il servizio pubblico cui faranno capo le chiamate provenienti dai veicoli); la circostanza che non si verifica un tracciamento permanente dei veicoli da parte del sistema satellitare *Gps*, in quanto le ultime tre posizioni del veicolo rilevate (necessarie per garantirne una localizzazione ottimale) sono inviate al 112 soltanto in caso di attivazione (ossia di incidente), e le restanti non sono memorizzate in alcun *data-base*; il fatto che la configurazione del sistema attualmente sia prevista su base volontaria e che le case produttrici non saranno quindi obbligate a prevedere l'installazione di sistemi *eCall* sulle vetture di nuova produzione.

Restano, tuttavia, alcuni aspetti sui quali il Gruppo ha ritenuto necessario richiamare l'attenzione:

- non è possibile prescindere dal requisito del consenso ai fini dell'utilizzazione del sistema: l'utente/proprietario del veicolo deve avere la possibilità di attivare/disattivare il sistema attraverso modalità semplici e chiare, indipendentemente dalla configurazione volontaria o meno dell'installazione *eCall*;
- devono essere previste maggiori garanzie qualora si voglia fare uso del *Full Data Set*, ossia delle informazioni aggiuntive che possono essere trasmesse in caso di incidente a terzi, sulla base di accordi contrattuali e nel rispetto dei principi di proporzionalità e di pertinenza del trattamento. In particolare, devono essere comunicate solamente le informazioni strettamente necessarie per le sole finalità che specifici soggetti terzi perseguono;
- qualora per difficoltà connesse all'implementazione del sistema fosse prevista l'installazione obbligatoria del dispositivo *eCall* sui veicoli europei (*ad es.*, attraverso uno strumento *ad hoc*, quale un regolamento), dovranno essere fissate le necessarie garanzie attraverso la legislazione nazionale anche per evitare forme indebite di sorveglianza degli utenti e trattamenti ulteriori dei dati generati dal sistema.

Revisione del quadro normativo sulle comunicazioni elettroniche

La revisione del "pacchetto normativo comunitario" in materia di comunicazioni elettroniche è stata avviata negli ultimi mesi del 2005 ed è proseguita per tutto il 2006, riguardando anche la direttiva n. 2002/58/Ce (direttiva *e-Privacy*). In particolare, dopo aver concluso il 31 gennaio 2006 una consultazione pubblica lanciata nel 2005 al fine di ricevere indicazioni e suggerimenti, la Commissione europea ha pubblicato nel mese di giugno 2006 una "comunicazione" sulla revisione del quadro normativo, che affronta anche la direttiva *e-Privacy*. Alla comunicazione si accompagna uno *"Staff Document"* che illustra in maggiore dettaglio le proposte elaborate dalla Commissione, nonché un documento di *"Impact Assessment"* che presenta pro e contro delle singole proposte formulate. Su questi documenti e proposte la Commissione europea ha lanciato, nel mese di luglio, una nuova consultazione pubblica, chiusa il 27 ottobre 2006. A tale consultazione il Gruppo ha contribuito con un documento approvato il 26 settembre 2006 (Wp 126).

Per quanto riguarda la direttiva *e-Privacy*, le proposte di modifica avanzate della Commissione si limitavano sostanzialmente agli aspetti di "sicurezza" delle reti di comunicazione e alla necessità di aumentare i poteri delle autorità nazionali di regolamentazione; pertanto, l'impianto complessivo della direttiva n. 2002/58 rimarrebbe inalterato. Nel suo parere, il Gruppo ha accolto con favore questa posi-

22

zione della Commissione, pur sottolineando alcune incongruenze:

- in via generale, il potenziamento delle misure di sicurezza non può tradursi in provvedimenti tali da comprimere la riservatezza o facilitare la sorveglianza delle comunicazioni elettroniche;
- rispetto alla proposta di obbligare i fornitori di servizi a segnalare non soltanto i possibili rischi per la sicurezza delle reti di comunicazione, ma anche le violazioni concretamente verificatesi, il Gruppo ha proposto di estendere tale comunicazione alla totalità degli utenti e non solo alle potenziali "vittime";
- è necessaria maggiore chiarezza rispetto alla questione della responsabilità, ossia se gli obblighi previsti dalla direttiva siano applicabili ai fornitori di infrastrutture per l'accesso, ai fornitori di servizi, o ad entrambi. Su questo punto il Gruppo ha richiamato le osservazioni formulate nel proprio parere (Wp 36) reso nel 2000 in occasione dei lavori preparatori della direttiva n. 2002/58/Ce;
- l'incremento dei poteri delle autorità di regolamentazione non dovrebbe tradursi in un onere eccessivo o improprio; in particolare, secondo il Gruppo, non spetta alle autorità di protezione dei dati fissare i criteri tecnici per l'attuazione delle misure di sicurezza eventualmente indicate, che dovrebbero essere sviluppati dai soggetti preposti alla regolamentazione specifica del settore delle comunicazioni elettroniche.

Direttiva n. 2004/82/Ce

La direttiva n. 2004/82/Ce ha introdotto l'obbligo, per i vettori aerei che effettuano voli diretti all'interno del territorio Schengen, di comunicare anticipatamente i dati relativi alle persone trasportate, su richiesta delle autorità responsabili dei controlli alle frontiere esterne dell'Unione europea. Si tratta di una direttiva complementare alle disposizioni della Convenzione Schengen, finalizzata ad utilizzare alcuni degli spazi lasciati alla discrezionalità dei legislatori nazionali dalla direttiva n. 95/46/Ce (art. 13), approntando una disciplina armonizzata. La direttiva avrebbe dovuto essere recepita nel diritto interno degli Stati membri entro il 5 settembre 2006; in realtà molti Paesi, fra i quali l'Italia, alla fine del 2006 non avevano ancora completato le procedure finalizzate all'adozione dei necessari strumenti di recepimento.

In tale ottica, il Gruppo ha adottato un parere per offrire un ausilio agli Stati membri nella loro attività di trasposizione normativa, al fine di garantire la massima uniformità possibile ed evitare che i cittadini dell'Unione siano soggetti a trattamenti differenziati (Wp 127). Il Gruppo ha sottolineato che l'interpretazione e l'applicazione delle disposizioni contenute nella direttiva in questione devono avvenire nel rispetto dei principi previsti nella direttiva n. 95/46/Ce, e che tali disposizioni devono essere lette in modo restrittivo, trattandosi di una disciplina limitativa dei diritti delle persone.

Pertanto, il parere ricorda l'obbligo per gli Stati membri di rispettare alcuni principi fondamentali in materia di protezione dei dati:

- *principio di finalità*. L'obiettivo della raccolta dei dati è indicato chiaramente dalla direttiva, e consiste nel miglioramento dei controlli alle frontiere esterne dell'Ue e nella lotta all'immigrazione illegale. Le norme nazionali non possono allontanarsi da tale obiettivo, *ad es.* estendendo l'obbligo della raccolta di dati ai voli interni all'Unione europea. Inoltre, nell'interpretare la deroga prevista dall'art. 6 della direttiva, che consente di utilizzare i dati per finalità di "applicazione normativa" (attività giudiziarie e di polizia), il Gruppo sottolinea l'esigenza di individuare tali finalità a livello nazionale secondo un approccio egualmente restrittivo: ad esempio, per l'investigazione di reati gravi, in casi specifici e con precise salvaguardie di protezione dei dati;

- *principio di necessità, pertinenza e proporzionalità dei dati*. L'elencazione delle categorie di dati trattabili delimita la raccolta nel "massimo", e non nel "minimo". La raccolta di dati biometrici sarebbe eccedente rispetto agli obiettivi della direttiva, che non specifica in alcun modo le rispettive modalità di trattamento;
- *principio di conservazione limitata dei dati*. La direttiva, mentre specifica che i dati raccolti possono essere conservati, in deroga al termine generale di ventiquattro ore, per un periodo superiore qualora siano necessari alle autorità competenti "nell'esercizio delle attività previste dalla legge", non fissa alcun termine specifico di conservazione per tale ultima ipotesi. Il Gruppo ritiene che le norme nazionali dovrebbero consentire tale conservazione prolungata solo in casi specifici (impossibilità di accertare l'identità dei viaggiatori, non disponibilità di documenti di viaggio appropriati); in ogni caso, gli Stati membri dovrebbero provvedere affinché in queste specifiche evenienze i dati non siano conservati oltre il tempo assolutamente necessario.

Iniziative di *enforcement*

Lo svolgimento di azioni coordinate a livello Ue da parte delle autorità di protezione dati degli Stati membri nell'ambito delle attività svolte in seno al Gruppo art. 29 è stato pianificato e attuato per la prima volta nel corso del 2006. Il settore scelto per la prima investigazione comune è stato quello delle società di assicurazione che offrono polizze per i trattamenti sanitari, ambito in cui eventuali inosservanze dei principi sulla protezione dei dati possono avere serie implicazioni su un numero significativo di cittadini europei.

Le compagnie sono state chiamate a fornire le informazioni richieste secondo uno schema (questionario) identico per tutti gli Stati membri.

La scelta di esaminare congiuntamente tale settore segue la dichiarazione del Gruppo art. 29 adottata il 25 novembre 2004, nella quale le autorità europee di protezione dei dati avevano indicato che la promozione dell'ottemperanza armonizzata della normativa sulla protezione dei dati costituisce uno dei suoi obiettivi strategici e permanenti. La dichiarazione sottolineava l'importanza delle *cd.* "attività di esecuzione" come strumento per potenziare l'ottemperanza, e l'opportunità di un approccio maggiormente propositivo nei riguardi di questa attività, considerando che uno dei fondamentali obiettivi conferiti dalla direttiva al Gruppo consiste proprio nel contribuire all'applicazione armonizzata ed uniforme delle disposizioni nazionali in materia di protezione dei dati.

A tale scopo, ciascuna autorità nazionale di protezione dati ha selezionato un campione rappresentativo delle compagnie assicurative che, a livello nazionale, offrono polizze assicurative per i trattamenti sanitari privati, in modo da coprire almeno il 50% del mercato di settore, e ha somministrato il questionario per le risposte, in alcuni casi utilizzando i poteri conferiti dall'ordinamento (per l'attività svolta dal Garante, *v. par.* 10.2).

Sulla base delle risposte ricevute, sono stati redatti i rapporti nazionali contenenti in forma aggregata le risultanze in relazione alle singole questioni trattate. I rapporti nazionali sono stati analizzati per valutare l'opportunità di impartire specifiche prescrizioni al settore da parte delle autorità europee ovvero di lasciare alle autorità nazionali eventuali iniziative al riguardo. I documenti finali sono in corso di elaborazione.

Libro verde sulle tecnologie di rilevazione

Il Gruppo art. 29 ha contribuito anche alla consultazione pubblica (conclusasi il 10 gennaio 2007) aperta dalla Commissione europea rispetto al "Libro verde sulle tecnologie di rilevazione" nel lavoro delle autorità di contrasto (doganali, di polizia, *ecc.*). Il libro verde intendeva raccogliere spunti e suggerimenti concreti per realizzare un approccio congiunto rispetto alle tecnologie di rilevazione (ovvero di sorveglianza) nell'ottica di una migliore integrazione fra soggetti pubblici (utilizzatori

22

di tali tecnologie) e soggetti privati (produttori delle tecnologie). Standardizzazione, ricerca, certificazione e interoperabilità sono le parole-chiave ricorrenti nel documento elaborato dalla Commissione, che propone una serie di quesiti su ciascuno degli argomenti suddetti. Il Gruppo art. 29 ha formulato alcune osservazioni sui singoli quesiti e sull'impostazione complessiva del documento (Wp 129), manifestando l'intenzione di essere coinvolto nei futuri sviluppi del programma comunitario concernente tali tecnologie (soprattutto rispetto all'esigenza di costruire un approccio che preveda l'incorporazione di salvaguardie a tutela della *privacy* fin dalla fase di progettazione delle singole tecnologie e dei singoli prodotti).

Pur apprezzando l'attenzione posta dalla Commissione alle tematiche di protezione dati, il Gruppo ha segnalato l'esigenza di tenere in piena considerazione i principi già fissati in materia, oltre che dalla direttiva n. 95/46/Ce, anche da altri strumenti quali la Convenzione europea dei diritti dell'uomo e le pertinenti raccomandazioni del Consiglio d'Europa (in particolare la raccomandazione n. R(87)15 sul trattamento di dati personali da parte delle forze di polizia). È stata inoltre ribadita l'opportunità di distinguere fra le esigenze connesse alla lotta al terrorismo e quelle relative al contrasto di altre gravi forme di criminalità, che postulano diversi approcci e garanzie.

Infine, si è rappresentato che il principio di minimizzazione resta requisito generale per la legittimità dell'utilizzazione di dati personali, soprattutto con riguardo alla proposta creazione di sistemi paneuropei per l'analisi dei dati raccolti attraverso le tecnologie della rilevazione. Il Gruppo ha sottolineato l'importanza di esaminare in concreto le implicazioni associate alla realizzazione di nuovi prodotti o strumenti basati su tecnologie di rilevazione e sorveglianza, e di ricomprendere anche il rispetto dei principi fondamentali sanciti dalla direttiva sulla protezione dei dati fra le "buone prassi da sviluppare" attraverso l'approccio coordinato fra settore pubblico e settore privato cui fa riferimento il libro verde.

Cartelle cliniche elettroniche

La creazione di sistemi nazionali di sanità elettronica è un obiettivo di rilevante interesse pubblico, perseguito in misura diversa da tutti gli Stati dell'Unione europea, compresa l'Italia. In questo contesto, il Gruppo ha ritenuto opportuno fissare un quadro giuridico di garanzie che, a vari livelli, i legislatori nazionali sono chiamati a rendere operative nella configurazione e nella gestione dei sistemi di sanità elettronica.

Con un documento di lavoro approvato nel mese di febbraio 2007 (Wp 131) all'esito di un'attività istruttoria condotta durante il 2006, le autorità hanno analizzato i requisiti di legge e i parametri applicativi da tenere presenti nella strutturazione e nella gestione di sistemi nazionali di "cartelle cliniche elettroniche". Sul documento è prevista l'apertura di una consultazione pubblica per sollecitare contributi e commenti, in particolare dal mondo della sanità e della ricerca.

Il documento si compone di una parte generale, ove sono indicate le premesse per l'istituzione di un sistema nazionale di cartelle cliniche elettroniche, e di una parte speciale dedicata all'individuazione delle garanzie idonee a garantire il rispetto dei principi di protezione dati in un sistema del genere.

Nell'ambito della prima parte, guardando ai requisiti fissati dalla direttiva rispetto al trattamento dei dati "sensibili" (quali i dati sanitari), i Garanti hanno concluso che il fondamento più appropriato per l'istituzione di un sistema di cartelle cliniche elettroniche (a prescindere dalla sua configurazione) è offerto dall'articolo 8, comma 4, della direttiva n. 95/46/Ce. Tale disposizione consente agli Stati membri di trattare i dati sensibili senza il consenso della persona interessata, purché ciò avvenga per motivi di "interesse pubblico rilevante" e siano fissate misure legislative o di altra natura che garantiscano la protezione dei dati.

La seconda parte del documento si occupa delle garanzie da individuare attraverso un organico quadro normativo. Primaria importanza viene riconosciuta al rispetto del principio di autodeterminazione, che comporta la necessità di prevedere spazi e momenti diversi per consentire agli interessati (pazienti) di esprimere tale autodeterminazione attraverso il consenso vero e proprio (*opt-in*) ovvero forme di dissenso (*opt-out*), da valutare e graduare opportunamente. Dovranno essere fissate anche idonee garanzie rispetto all'accesso ai dati da parte di operatori sanitari, del paziente e di terzi, con riguardo alle misure di carattere tecnico quali identificazione, autenticazione e autorizzazione. La necessità di separare le diverse categorie di dati eventualmente compresi nella cartella clinica elettronica consiglia di prevedere una struttura modulare, avendo riguardo alle finalità del trattamento e/o ai soggetti che possono accedere ai dati.

Restano fermi i requisiti in materia di sicurezza, che possono variare in rapporto alle più generali disposizioni nazionali in materia, nonché quelli riferiti ai trasferimenti di dati verso Paesi terzi; su questo punto, in particolare, il Gruppo ha proposto il trasferimento dei dati in forma anonimizzata o pseudonimizzata, senza rivelare l'identità del paziente se non quando assolutamente necessario (*ad es.*, in caso di consulto). Anche eventuali utilizzazioni secondarie dei dati contenuti nella cartella elettronica (per scopi di ricerca o di altra natura) dovranno essere regolamentate specificamente a livello nazionale, nel rispetto di tutti i principi stabiliti in merito dalla direttiva.

Alcune questioni necessiteranno di approfondimenti ulteriori e del contributo specialistico del settore sanitario: è il caso, in particolare, della valutazione concernente la qualità dei dati contenuti nelle cartelle (completezza e accuratezza), della definizione dei criteri di responsabilità (civile, penale e amministrativa) dei soggetti partecipanti al sistema e della messa a punto di meccanismi per la risoluzione di possibili controversie (*ad es.*, in tema di accesso alle cartelle). Sul punto, il Gruppo non ha ritenuto di indicare come preferibile una specifica articolazione del sistema (su base centralizzata, decentralizzata, o di tipo misto), sottolineando che la scelta ultima spetta al legislatore nazionale; tuttavia, sono stati indicati i possibili rischi e benefici nei singoli casi, nell'ottica della protezione dei dati.

22.1.1. *Le iniziative sul trasferimento dei dati verso i Paesi extraeuropei*

Accordi Pnr

L'elemento di maggiore rilevanza concernente il "pacchetto" di strumenti giuridici negoziato dalla Commissione e dal Consiglio Ue con le autorità statunitensi (*Department of Homeland Security-Dhs/Bureau of Customs and Border Protection*) per consentire il trasferimento dal territorio europeo ad autorità degli Usa i dati personali relativi a passeggeri (dati Pnr) su voli aerei diretti o in transito negli stessi Stati Uniti è stata indubbiamente la sentenza della Corte di giustizia delle Comunità europee del 30 maggio 2006. Con questa decisione la Corte, accogliendo il ricorso presentato dal Parlamento europeo, ha invalidato tali strumenti (decisione di adeguatezza della Commissione e accordo fra Consiglio dell'Unione europea e il Dhs degli Usa). La Corte di giustizia ha negato la validità della base giuridica della decisione del 2004 con cui la Commissione europea aveva giudicato "adeguato" (ai sensi della direttiva n. 95/46/Ce) il sistema di garanzie associato al trattamento dei dati Pnr da parte degli Stati Uniti. Secondo la Corte, infatti, non si tratterebbe di materie che rientrano nell'ambito di applicazione della direttiva europea sulla protezione dei dati, giacché i dati dei passeggeri, per quanto raccolti da privati (le compagnie aeree) in rapporto ad attività (prenotazione e vendita di biglietti) che rientrano nel medesimo ambito di applicazione della direttiva, sono poi trasferiti e trattati in territorio statunitense per finalità connesse alla tutela della sicurezza pubblica e alle

22

attività di polizia. Poiché queste ultime risultano escluse espressamente dall'applicazione delle norme della direttiva, la Corte ha ritenuto che venga meno il presupposto stesso dell'accordo e della decisione di adeguatezza.

La Corte, pertanto, non si è pronunciata sui problemi legati ai *deficit* di protezione sostanziale che il Parlamento europeo aveva indicato anche in base ai pareri resi dai Garanti. La sentenza, nell'annullare la decisione, consentiva peraltro di continuare ad applicare gli accordi esistenti, per evitare un vuoto normativo, fino al 30 settembre 2006.

Alla sentenza hanno fatto seguito intensi negoziati fra la Commissione europea e rappresentanti del *Bureau of Customs and Border Protection* (Cbp), finalizzati a definire un nuovo testo dell'accordo prima del termine fissato dalla Corte di giustizia, così da evitare un vuoto giuridico e le inevitabili gravi ripercussioni sui diritti dei cittadini e sulle attività dei vettori aerei.

Si è così riaperta la discussione sul tema più generale del bilanciamento fra esigenze di sicurezza e tutela di diritti fondamentali quali il diritto alla protezione dei dati personali. Tanto il Parlamento europeo quanto il Gruppo art. 29 si erano già mostrati molto critici nei confronti dei negoziati ed del loro risultato. In particolare, il Gruppo aveva pubblicato, tra il 2002 e il 2004, quattro pareri nei quali giudicava insufficienti le garanzie offerte dagli Stati Uniti, soprattutto rispetto alle categorie di dati oggetto di trasferimento (eccessive), al periodo di conservazione dei dati (eccessivo), alle modalità di utilizzazione dei dati stessi (non del tutto chiare), e all'informativa fornita ai passeggeri (il Gruppo ha pertanto proposto un modello *ad hoc* per le compagnie aeree). Inoltre, sia il Gruppo sia il Parlamento avevano sottolineato l'esigenza che le competenti autorità americane si impegnassero a realizzare (come previsto dall'accordo) il passaggio da un sistema di accesso diretto ai dati delle compagnie (cosiddetto *"pull"*) ad un sistema per cui sono le compagnie a fornire al Cbp i dati da quest'ultimo richiesti (cosiddetto *"push"*).

In questo contesto, il Gruppo ha riassunto le preoccupazioni sopra ricordate e indicato alcune linee-guida in due pareri, adottati il 14 giugno ed il 27 settembre 2006 (Wp 122 e Wp 124).

Nel primo, si sottolineava l'inopportunità di accordi bilaterali fra i Paesi Ue e gli Stati Uniti, per evitare disarmonie di trattamento fra i cittadini europei, nonché la necessità che il nuovo eventuale accordo paneuropeo garantisse almeno lo stesso livello di tutela di quello annullato, possibilmente tenendo presente alcune delle richieste più volte avanzate anche dal Parlamento europeo (attuazione del sistema *"push"*, ormai tecnicamente possibile; divieto di utilizzare i dati Pnr per finalità diverse da quelle per cui sono comunicati; riduzione delle categorie di dati oggetto di trasferimento). Si ribadiva, inoltre, la necessità di adottare un approccio coerente a livello mondiale rispetto al trasferimento di dati relativi a passeggeri di voli aerei, per garantire la sicurezza del traffico aereo e il rispetto dei diritti umani, anche perché richieste analoghe a quelle delle autorità statunitensi sono pervenute da Canada ed Australia e da altri Paesi.

Nel parere del settembre 2006, alla vigilia del termine per l'adozione di un nuovo accordo, le autorità hanno prospettato le conseguenze di un eventuale vuoto giuridico ricordando i poteri di cui sono investite e che non avrebbero potuto esimersi dall'esercitare in base alle leggi nazionali, in caso di assenza di un'adeguata base giuridica per il trasferimento dei dati come richiesto dalla direttiva. Si chiedeva, inoltre, maggiore chiarezza sul fatto che gli "*Undertakings*" (Impegni) del Dhs/Cbp (i quali costituiscono parte integrante del "pacchetto" Pnr) continuassero o meno ad essere applicati; infine, veniva lamentata l'inerzia da parte delle autorità statunitensi rispetto al passaggio dal sistema *"pull"* al *"push"* nonostante la fattibilità tecnica di tale modifica.

Il 6 ottobre 2006 è stato adottato dalla Commissione e dal Dhs il nuovo testo dell'accordo, poi firmato dal Consiglio Ue il 16 ottobre, che prevede il passaggio dal sistema *"pull"* al sistema *"push"* (pur non indicando il termine temporale per l'adeguamento) lasciando invariato l'impianto complessivo. Il Dhs ha accompagnato l'accordo con una lettera che contiene alcune "precisazioni" sull'ambito di applicazione dell'accordo stesso e sull'interpretazione che il Dhs dà di alcune disposizioni. Quest'ultima lettera ha suscitato numerose perplessità nelle autorità di protezione dati perché in realtà incide, modificandoli, sui principali aspetti regolati negli impegni americani (passaggio al sistema *"push"*, conservazione dei dati, loro successiva comunicazione, aumento dei dati richiedibili). Il Gruppo ha nel contempo deciso di definire una più generale analisi del quadro giuridico associato ai trasferimenti di dati relativi a passeggeri verso Paesi terzi ed ha adottato un *cd. "strategy paper"* in materia.

Per quanto concerne il Pnr-Usa, occorre inoltre segnalare che il Gruppo art. 29 ha adottato un ulteriore parere nel mese di febbraio 2007 (Wp 132) in cui ha riformulato i testi delle informative che le compagnie aeree e gli altri soggetti che effettuano prenotazioni aeree sono tenuti a fornire ai passeggeri rispetto ai trattamenti di dati in questione. Il Gruppo ha sottolineato l'esigenza di rendere disponibili le due versioni dell'informativa (quella breve, contenente le informazioni essenziali alla luce della direttiva n. 95/46/Ce, e quella lunga, sotto forma di *"Faq"*, ossia di quesiti più frequenti) in momenti e secondo modalità diverse a seconda del mezzo prescelto per la prenotazione: presso agenzie di viaggio, prenotazione telefonica, prenotazione *on-line* attraverso Internet.

Pnr e malattie trasmissibili

A margine del discorso sul Pnr e, più in generale, su quello relativo alla raccolta e trasferimento dei dati dei passeggeri verso gli Stati uniti, il Gruppo art. 29 ha adottato il Wp 121 su "Pnr e malattie trasmissibili". Si tratta di un parere espresso su una proposta di legislazione che il Dipartimento della sanità e dei servizi umani degli Stati Uniti d'America ha pubblicato, come d'uso, nel Registro federale, per raccogliere, in un periodo fissato, osservazioni e commenti ai fini della successiva adozione dell'atto. La proposta riguarda la prevenzione del contagio e della diffusione di malattie trasmissibili negli Stati Uniti e intende modificare il *"Public Health Service Act"*. Una parte delle disposizioni concerne i passeggeri in arrivo dall'estero. Le modifiche proposte nella sezione relativa alle informazioni sui passeggeri introducono l'obbligo per ciascuna compagnia aerea o di navigazione che effettui un viaggio internazionale verso un aeroporto o un porto degli Stati Uniti di chiedere ad ogni passeggero e membro dell'equipaggio una serie di informazioni, che includono numeri da contattare in caso d'emergenza, indirizzo *e-mail*, numero di passaporto o numero del biglietto, con l'indicazione del Paese o dell'organizzazione che lo hanno rilasciato, nome dei compagni di viaggio o del gruppo di cui si fa parte, informazioni relative al volo o allo scalo, volo di ritorno (data, numero della compagnia) e numeri di telefono aggiornati (in ordine di preferenza: cellulare, telefono fisso, cercapersone o recapito telefonico sul luogo di lavoro).

Si prevede inoltre la possibilità di richiedere altri dati non specificati, eventualmente in possesso della compagnia aerea o di navigazione, se necessari per prevenire l'introduzione, la trasmissione o la propagazione di malattie trasmissibili.

La proposta, se attuata, imporrebbe alcuni obblighi generali alle compagnie aeree e di navigazione europee e, in particolare, l'applicazione delle seguenti misure:

- la raccolta e la conservazione per sessanta giorni nell'Ue di una serie di dati relativi a tutti i passeggeri che si recano negli Stati Uniti in aereo attualmente non compresi nei dati Pnr delle compagnie, né nel loro sistema di controllo delle partenze (Dcs), come *ad es.* i numeri da contattare per le

emergenze, gli indirizzi *e-mail*, le persone che li accompagnano e informazioni sul volo di ritorno per poterli rintracciare successivamente;
- l'invio in formato elettronico di queste informazioni direttamente al direttore del Centro per la prevenzione e il controllo delle malattie (Cdc) statunitense nelle dodici ore successive alla richiesta.

Il Gruppo ha ritenuto che, pur essendo la lotta contro le malattie trasmissibili un importante obiettivo, occorre comunque rispettare il diritto fondamentale alla protezione dei dati personali, nonché, con riferimento alle misure adottate, il principio di proporzionalità. Per quanto riguarda i viaggi internazionali e l'imposizione di obblighi di trattamento dei dati personali su soggetti privati, quali le compagnie aeree e di navigazione, le autorità per la *privacy* hanno confermato di preferire soluzioni globali piuttosto che richieste e misure imposte unilateralmente. Si tratta di un punto di vista già espresso in precedenti pareri, in particolare quelli relativi alle richieste, avanzate da diversi Paesi, di fornire i dati dei passeggeri per la lotta contro il terrorismo e altri gravi crimini a carattere transnazionale.

Il parere, esaminate attentamente le disposizioni previste nella nuova proposta di legge statunitense, ha riscontrato infine il contrasto non soltanto con la direttiva n. 95/46/Ce, ma anche col regolamento sanitario internazionale Oms del 2005.

Caso Swift

Swift (*Society for Worldwide Interbank Financial Telecommunication*) è una società, con sede in Belgio, di cui si servono da decenni le banche ed i soggetti operanti nel settore finanziario di tutti gli Stati europei per i trasferimenti internazionali di valuta, anche in Paesi al di fuori dell'Ue, come gli Stati Uniti. Nel corso del 2006, il Gruppo art. 29 è stato chiamato a valutare, in particolare, le modalità con cui Swift e le istituzioni finanziarie che di Swift si servono hanno gestito le richieste formulate da autorità federali statunitensi che, nel quadro della lotta contro le attività terroristiche, più volte avevano chiesto e ottenuto di accedere ad informazioni contenute nelle transazioni finanziarie.

L'analisi condotta dal Gruppo, attraverso una lunga e complessa istruttoria, ha portato all'adozione di un parere nel mese di novembre 2006 (Wp 128), nel quale si è stabilito che Swift e le istituzioni finanziarie sono contitolari del trattamento in questione, seppure per aspetti distinti; pertanto, sia l'una che le altre debbono assicurare il rispetto delle norme europee e nazionali in materia di protezione dei dati.

A giudizio del Gruppo, Swift e le istituzioni finanziarie hanno violato le disposizioni della direttiva n. 95/46/Ce poiché non hanno informato adeguatamente i clienti della possibilità che i loro dati fossero trasferiti negli Stati uniti d'America per le finalità sopra ricordate, anche con riguardo all'esistenza di un *data-base* cosiddetto di *"mirroring"* (speculare) in cui sono riversate tutte le transazioni effettuate da Swift e che si trova in territorio americano già da molti anni. In particolare, la società ha proceduto a fornire le informazioni richieste dalle autorità statunitensi senza consultare né le autorità nazionali di protezione dati, né altri soggetti competenti, mentre le istituzioni finanziarie che della Swift si servono hanno omesso di vigilare adeguatamente sul rispetto delle norme di protezione dati da parte della stessa società.

Il documento sottolinea, inoltre, che il trasferimento dei dati personali dei clienti alle autorità federali statunitensi è stato effettuato senza alcun valido fondamento giuridico e con un grave *deficit* di trasparenza che non ha consentito il controllo indipendente da parte delle autorità per la *privacy*.

I Garanti hanno invitato Swift e le istituzioni finanziarie ad adottare rapidamente tutte le misure necessarie, nei rispettivi ambiti, per porre rimedio alla situazione, riservandosi in caso contrario l'applicazione di tutte le sanzioni previste dalle norme nazionali in materia. Inoltre, anche le banche centrali dei singoli Stati membri dovranno fare chiarezza sul proprio ruolo in quanto autorità di vigilanza rispetto all'operato di Swift.

Il Gruppo ha continuato a seguire gli sviluppi del caso e all'inizio del 2007 ha deliberato di inviare una lettera al vice Presidente della Commissione europea, Franco Frattini, al Presidente del Parlamento europeo e al Presidente del Consiglio dell'Unione europea. Nella lettera, intesa soprattutto a fornire elementi di valutazione al vice Presidente Frattini nel quadro dei negoziati condotti da quest'ultimo con le autorità americane per conto della Commissione relativamente ad una possibile soluzione paneuropea, il Gruppo ha manifestato alcune perplessità in merito ai risultati conseguiti nei mesi successivi all'adozione del parere sopra descritto.

Si è sottolineata, pertanto, la necessità di intraprendere azioni immediate, affinché il sistema dei pagamenti sia pienamente rispettoso dei principi sanciti dalla direttiva n. 95/46/Ce e tutti i soggetti coinvolti si conformino a quanto prescritto. Inoltre, si ricorda come la questione sia suscettibile di complicarsi ulteriormente alla luce del ruolo che Swift sarà chiamata a svolgere nell'ambito del nuovo sistema unico europeo dei pagamenti (Sepa) –in particolare perché l'utilizzo di tale società anche in questo ambito potrebbe comportare, in prospettiva, la possibilità per le autorità statunitensi di accedere ad informazioni su trasferimenti interbancari effettuati all'interno del territorio Ue o del territorio dei singoli Stati membri. La lettera menziona anche la proposta adesione al *Safe Harbor* da parte di Swift, giudicandola una soluzione insufficiente in quanto non coprirebbe i trattamenti da essa effettuati per finalità connesse alle attività giudiziarie e di polizia (che esulano dall'ambito di applicazione del *Safe Harbor*).

Richiesta *standard* per l'approvazione di Bcr

Nel corso del 2006, il Gruppo art. 29 è tornato a pronunciarsi sullo strumento delle Bcr per il trasferimento all'estero dei dati personali ai sensi dell'art. 26, comma 2, direttiva n. 95/46/Ce.

Come noto, la disciplina delle Bcr è stata definita mediante alcuni provvedimenti del Gruppo, e segnatamente dal documento Wp 74 e dai successivi pareri Wp 107 e Wp 108, che hanno fissato una procedura di coordinamento tra le autorità nazionali qualora una richiesta di valutazione di Bcr venga contestualmente portata all'attenzione di diverse autorità, al fine di uniformare quanto più possibile documentazione e allegati da presentare per ottenere l'approvazione delle Bcr.

All'esito di alcuni incontri di lavoro del sottogruppo di esperti nazionali sulle Bcr provenienti da diverse autorità nazionali per la protezione dati, compresa quella italiana, in cui si è valutato in più occasioni un documento sottoposto all'attenzione del Gruppo art. 29 da parte di una associazione internazionale di imprese, il Gruppo stesso si è nuovamente pronunciato sul punto nel 2007 mediante l'approvazione del documento Wp 133, con il quale è stata raccomandata l'adozione da parte dei soggetti interessati di un modello *standard* di richiesta per l'approvazione di Bcr in tutti i Paesi dell'Unione europea. Tale modello richiama le linee-guida ed i principi già a suo tempo espressi con i citati provvedimenti degli anni scorsi.

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

Anche nel 2006, il *trend* crescente nelle proposte di atti legislativi e regolamentari nel *cd.* "terzo pilastro" è stato ampiamente confermato, pur incontrando rallentamenti per quanto riguarda la messa in funzione dei *data-base* centralizzati, come il Vis ed il Sis; solo alla fine del dicembre 2006, infatti, il regolamento relativo al Sis II è stato pubblicato sulla *Gazzetta ufficiale dell'Unione europea*, mentre i lavori per la definizione della decisione sul Sis II e del Vis sono tuttora in corso.

22

Il ritardo è certamente da ricondurre in parte alla mancata adozione di principi per il trattamento dei dati personali nel terzo pilastro, elemento richiamato dal programma dell'Aja come necessario quadro di riferimento per le attività di cooperazione tra forze di polizia e magistratura al fine di prevenire e reprimere reati. Tali principi, fatti propri dalla Commissione europea nella forma di una proposta di decisione-quadro, sono stati oggetto diverse modifiche nel corso dell'esame da parte del Consiglio, nell'ambito di un dibattito che non vede al momento chiari esiti positivi per ciò che concerne un quadro adeguato di efficaci garanzie. La presidenza tedesca, che guida l'Unione nel primo semestre del 2007, ha previsto la presentazione di una nuova proposta in materia, insieme ad un'altra proposta tendente ad introdurre nell'ordinamento comunitario le forme di cooperazione più incisive definite tra alcuni Stati attraverso la firma della *cd.* "Convenzione di Prüm".

Come si è già avuto modo di rilevare, nonostante la positiva scelta di collocare all'interno della Direzione generale giustizia, libertà e sicurezza della Commissione europea il segretariato del Gruppo art. 29, per le procedure di elaborazione e per la frammentarietà delle competenze in materia in seno all'Unione, di fatto alcune nuove iniziative europee di regolazione che riguardano i dati personali non sono tutte tempestivamente vagliate dalle autorità di protezione dei dati; alcune in quanto riguardano materie di terzo pilastro e, altre, perché non sono esclusivamente collocabili in uno dei pilastri comunitari.

Le autorità di protezione dei dati hanno da tempo segnalato il progressivo venir meno di preventivi "momenti istituzionalizzati" che favorissero la necessaria valutazione dell'impatto che tali misure erano destinate a produrre sui diritti fondamentali della persona e, più specificamente, sulla tutela dei dati personali. In tal senso, la presidenza di turno austriaca ha inteso riattivare in qualche modo uno dei gruppi di lavoro il cui mandato specifico nel Consiglio dell'Ue era la protezione dati nel "primo pilastro". Tuttavia questo gruppo, pur essendo potenzialmente atto ad occuparsi di qualunque questione avente un impatto sulla tutela dei dati, in realtà non ha ricevuto un mandato definito; né, la sua composizione è stata allargata alle autorità di protezione dei dati personali.

Nel terzo pilastro, in mancanza di principi comuni e di un organismo almeno "parallelo" al Gruppo art. 29, le attività sono attualmente portate avanti, ciascuna per gli aspetti di specifica competenza attribuiti dalle convenzioni cui si riferiscono, dalle Autorità comuni di controllo Schengen, Europol e Dogane. Un'attività di supervisione si svolge anche, a livello europeo, per Eurodac, coordinata dal Garante europeo per la protezione dei dati (Edps) che ne è l'autorità di controllo, ma i trattamenti che si svolgono nella banca dati centrale sono considerati "di primo pilastro" in quanto finalizzati all'applicazione delle norme in materia di riconoscimento dello *status* di rifugiato.

Per far fronte a questo stato di cose nel settembre 2004, in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati, a Wroclaw, era stata approvata una risoluzione in cui si chiedeva che le istituzioni dell'Ue promuovessero un *forum* nel quale i Garanti europei possano discutere le implicazioni degli sviluppi del terzo pilastro sulla protezione dei dati. Fino alla creazione di tale *forum*, le iniziative del terzo pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune sarebbero state esaminate da un gruppo di lavoro delle autorità europee per la *privacy*, il *cd. "Working party on police"*.

Questo gruppo ha quindi l'incarico di predisporre, per l'approvazione nel corso della *Spring Conference*, le bozze di pareri e risoluzioni relative alle proposte maggiormente impegnative sotto il profilo della protezione dei dati.

Nel corso del 2006 sono emerse numerose indicazioni a favore di una maggiore

stabilità del *Working party on police*, che era presieduto dall'autorità di protezione dei dati del Paese che ospita la *Spring Conference* e assistito dal segretariato delle autorità comuni di controllo.

L'attività dell'Acc Schengen ha continuato ad essere legata prevalentemente agli sviluppi del Sis e al funzionamento dell'attuale sistema.

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

Considerato che il testo delle proposte presentate dalla Commissione per l'istituzione del nuovo sistema informativo Schengen, il *cd.* "Sis II", ha subito notevoli modifiche nel corso della discussione presso i gruppi competenti del Consiglio, l'Acc Schengen ha ritenuto di adottare un secondo parere in materia dopo quello, molto articolato, dell'ottobre 2005. I lavori si sono concentrati su alcuni specifici aspetti che destano maggiore preoccupazione, segnatamente per poter attirare l'attenzione del Parlamento europeo chiamato ad adottare i testi regolamentari in codecisione. Il parere è stato adottato nel settembre 2006.

I punti centrali espressi nel parere riguardano:

- la preoccupazione sull'indefinitezza delle finalità del Sis II con la possibilità, quindi, di un uso indiscriminato ed una moltiplicazione degli accessi ai dati contenuti nel sistema;
- la necessità che le successive disposizioni applicative siano adottate tenendo conto del loro impatto sui diritti delle persone e, in particolare, che l'Acc sia chiamata a contribuire nella fase attuativa e in quella transitoria per quanto riguarda la gestione del sistema centrale (C-Sis);
- l'inserimento nel sistema di dati biometrici (impronte digitali) e la possibilità di introdurre funzione di ricerca basate su tali dati;
- la necessità di garantire una elevata qualità di dati e, pertanto, di definire idonee modalità per aggiornare e correggere i dati, ove necessario, anche su richiesta di autorità diverse da quella che ha introdotto i dati;
- l'accesso (e le modalità per consentirlo) di Europol ed Eurojust ai dati contenuti nel Sis II.

I regolamenti sul Sis II sono stati adottati e pubblicati nella *Gazzetta ufficiale* dell'Unione europea. nel mese di dicembre 2006, mentre la relativa decisione non è stata ancora formalmente adottata.

Un ulteriore punto controverso, connesso ai precedenti, riguarda le modalità per il trasferimento dei dati dal Sis al Sis II, in particolare con riferimento alla translitterazione dei nomi. Al riguardo l'Acc ha adottato un parere rivolto alla Commissione europea.

L'Acc ha poi avviato un'azione comune per verificare in ciascuno dei Paesi partecipanti la regolarità delle segnalazioni inserite nel sistema con riferimento all'art. 99 della Convenzione (*cd.* "sorveglianza discreta"). Le verifiche dovranno essere svolte seguendo uno schema unico, elaborato in forma di questionario, prevedendo anche controlli *in situ*. Il segretariato, come nella precedente azione comune svolta per verificare la legittimità delle segnalazioni inserite nel sistema ai fini della non ammissione (in base all'art. 96 della Convenzione), redigerà poi un documento complessivo. Al fine di acquisire i necessari elementi il Garante ha deciso l'apertura di accertamenti formali.

È stato altresì presentato il rapporto di attività dell'Acc Schengen, che copre il biennio gennaio 2004-dicembre 2005.

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

L'Autorità comune di controllo su Europol ha elaborato la terza relazione di attività che copre il biennio da novembre 2004 ad ottobre 2006, non ancora pubblicata.

Nella relazione, l'Acc ha ricordato come il quadro generale di riferimento veda un incremento dell'attività di Europol e, quindi, un incremento dei dati raccolti ed analizzati; di conseguenza, ha considerato che la stessa collocazione di Europol potrebbe mutare, considerata l'intenzione di integrare meglio questo organismo tra

22

quelli dell'Unione e la predisposizione di una proposta di decisione per la sua "comunitarizzazione".

L'Acc conferma il ruolo fondamentale che la periodica conduzione d'ispezioni *in loco* delle attività Europol assume per verificare la liceità dei trattamenti di dati effettuati nei diversi archivi e far sì che la stessa Acc sia messa in grado di ottemperare al mandato ricevuto.

Nel marzo del 2006 si è svolta l'annuale ispezione su Europol. L'ispezione ha focalizzato la sua attenzione sul sistema di informazione Europol, sui seguiti dati alle raccomandazioni formulate dall'Acc nelle precedenti ispezioni e sul contenuto dei *file* di analisi.

L'Acc ha verificato l'alto grado di adeguamento da parte di Europol alle raccomandazioni formulate, anche se ha reiterato alcune preoccupazioni, in parte ascrivibili non alla sola Europol, ma anche al modo con cui gli Stati membri svolgono le attività richieste dalla Convenzione. L'Acc pertanto, in relazione a queste ultime, ha richiesto alle autorità nazionali che la compongono di effettuare delle verifiche rispetto alle azioni che i Paesi debbono assicurare in base alla Convenzione.

L'Autorità comune di controllo ha inoltre adottato alcuni pareri, quattro dei quali legati ad aspetti tecnici connessi all'entrata in vigore di alcune disposizioni parzialmente modificative dell'originaria Convenzione resi al Consiglio di amministrazione di Europol.

Un primo parere riguarda la proposta di decisione per attuare il nuovo art. 6a della Convenzione, che disciplina il trattamento dei dati che restano al di fuori dei sistemi informatizzati di raccolta delle informazioni (dati da vagliare ai fini della ammissibilità); un secondo parere è relativo alle regole applicabili agli archivi di analisi; un terzo parere analizza la partecipazione di Europol alle squadre investigative comuni, laddove l'Acc ha ribadito le sue preoccupazioni in materia ed ha ricordato il necessario rispetto dell'art. 10 della Convenzione; il quarto parere riguarda i meccanismi di controllo per il richiamo delle informazione nel sistema.

L'Acc si è inoltre espressa sulle modalità per l'accesso di Europol al Sis ed al Vis.

Un ulteriore aspetto considerato nell'attività svolta è quello relativo alla richiesta di Europol di poter definire un approccio diverso e più generale per l'apertura di *file* di analisi. La possibilità di creare una cornice più ampia nel corso delle indagini relative allo sfruttamento dell'immigrazione illegale, secondo la richiesta di Europol, è stata lungamente discussa in senso all'Acc. Il parere espresso dall'Acc, nel consentire questo nuovo approccio al trattamento dei dati, definisce le condizioni per il loro uso, accettate da Europol: tra esse, sono particolarmente rilevanti quelle che attengono alle finalità del sotto-*file* specifico, alle categorie dei dati, alle regole per i dati sensibili, alle limitazioni all'accesso e alle procedure trasparenti d'informazione dell'Acc, che ha per di più limitato a tre anni la possibilità di uso dei *file*, al termine del quale una nuova valutazione andrà effettuata.

Conferenza Europol

È stata inoltre organizzata una conferenza, svoltasi a Bruxelles il 17 ottobre per presentare pubblicamente il lavoro dell'Acc ad otto anni dalla sua istituzione e per discutere sul futuro di Europol. Alla conferenza sono stati invitati, considerato il contesto del trattamento dei dati da parte di Europol, che non ha funzioni operative di polizia, avvocati e giuristi che operano a livello europeo, parlamentari europei e persone che lavorano nelle istituzioni europee nei settori interessati oltre ai rappresentanti di Europol e delle autorità di protezione dei dati personali.

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

Il Sistema informativo doganale (Sid) 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 un'autorità comune di controllo (*cd.* "Acc Dogane"), composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

L'Acc Dogane ha iniziato un lavoro di verifica del rispetto delle condizioni per la raccolta e trattamento dei dati personali, ancorché il sistema risulti per il momento poco utilizzato. Sotto la presidenza italiana, il segretariato dell'Acc ha svolto una prima visita presso l'unità centrale per verificare la congruità delle misure di sicurezza adottate. Si è poi deliberato di svolgere anche accertamenti a livello nazionale, sulla scorta di un questionario comune, che possa facilitare la comparazione delle risposta. Lo svolgimento di tali ultime attività è previsto entro il primo semestre del 2007.

Eurodac

È proseguita l'attività di coordinamento effettuata dal Garante europeo per la protezione dei dati personali (Edps). Nel corso della riunione di primavera, la prima delle due previste per il 2006, la Commissione europea ha presentato il rapporto annuale sullo stato delle attività in relazione alla gestione della banca dati Eurodac, con riferimento ai risultati raggiunti ed ai problemi rilevati. Un punto significativo, su cui la Commissione e l'Edps (che ha funzioni di supervisione del sistema) hanno richiamato l'attenzione e richiesto la fattiva collaborazione delle autorità nazionali di protezione dei dati, riguarda le *cd. "special search"*: si tratta di richieste di accesso ai dati che il regolamento Eurodac (art. 18) consente ai fini di permettere l'esercizio dei diritti alla persona interessata. In taluni casi e per taluni Paesi, tra cui l'Italia, gli accessi ai sensi dell'art. 18 sono piuttosto numerosi e, da controlli sommari, non sembrano avvenire per le ragioni indicate nel regolamento.

L'Edps ha svolto una prima ispezione al sistema, accertando questa incongruenza e presenterà all'inizio dell'anno prossimo una relazione al riguardo; ha inoltre sollecitato le risposte delle autorità di protezione dei dati per poter includere il quadro completo delle situazioni nazionali nella relazione. Partendo dalla richiesta dell'Edps, il Garante ha formalmente deliberato l'avvio di accertamenti in materia.

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

Case Handling Workshops

La XIII e la XIV edizione dei *"Case Handling Workshops"* hanno avuto luogo rispettivamente a Madrid (27-28 marzo 2006, presso l'autorità di protezione dei dati della Regione di Madrid) e ad Atene (13-14 novembre 2006, presso l'autorità greca per la protezione dei dati personali). I due incontri hanno offerto, ancora una volta, l'occasione per un vivo confronto tra le autorità dei Paesi dell'Ue (ai quali si sono aggiunti Romania e Bulgaria –nel 2006 non ancora membri dell'Unione–, Croazia, Liechtenstein e gli Stati dello Spazio economico europeo) su temi concreti legati all'applicazione delle disposizioni in materia di protezione dei dati. L'organizzazione prevede, accanto a due "sessioni plenarie", due sessioni parallele che intendono favorire una discussione approfondita sulle diverse questioni contemplate nel programma di lavoro.

Fra le questioni affrontate nelle plenarie, si ricordano, per quanto riguarda l'incontro di Madrid: l'*e-government* e le relative novità normative ed applicative a livello nazionale (codice identificativo unico, carta di identità elettronica, interconnessione di archivi pubblici, "carta del cittadino", *ecc.*); le strategie di comunicazione sviluppate dalle singole autorità, soprattutto nell'ottica di massimizzare le (scarse) risorse disponibili, diversificando le modalità comunicative a seconda del messaggio e del contesto anche con l'aiuto (giudicato indispensabile) di professionisti della comunicazione inseriti stabilmente nello *staff* delle autorità; il funzionamento dei cosiddetti *"front office"* (uffici relazioni con il pubblico) sviluppati da molte autorità e che, pur con alcune differenze nazionali, sembrano in grado di svolgere alcune delle funzioni di *"back office"*, ossia istruire pratiche e fornire risposte già "formali" ai quesiti presentati.

22

Anche nell'incontro di Atene il dibattito in sessione plenaria ha affrontato alcuni aspetti connessi a tematiche di *e-government*: in particolare, è stata approfondita la questione della comunicazione istituzionale che deve svolgersi nel rispetto della *privacy* dei cittadini, evitando, in particolare, le comunicazioni "chiaramente incompatibili" con finalità istituzionali quali, *ad es.*, quelle volte ad evidenziare i successi dell'amministrazione o il conseguimento di obiettivi contenuti in programmi elettorali. Nello stesso ambito è stato poi discusso il progetto dell'autorità greca di potenziare il proprio sito *web* trasformandolo in un "portale" di servizi al cittadino, anche attraverso la predisposizione di comunicazioni di posta elettronica che informino automaticamente gli interessati sullo stato di trattazione delle loro segnalazioni, o tramite la creazione di uno spazio *web* accessibile ai titolari del trattamento per verificare (in modo anonimo) l'idoneità delle misure adottate in materia di protezione dei dati personali.

La presentazione dei provvedimenti adottati dal Garante in materia di *e-ticketing* ha poi suscitato un vivace dibattito, anche alla luce di analoghe decisioni adottate da parte dell'autorità francese e delle applicazioni delle nuove tecnologie ai sistemi di pagamento relativi al pedaggio autostradale. Grande spazio è stato dedicato agli strumenti e alle strategie utili a migliorare l'operatività delle autorità di protezione dei dati e ridurre il carico di lavoro, sotto molteplici riguardi: elaborazione di metodologie per verificare la bontà delle autovalutazioni effettuate dai soggetti titolari di trattamento; definizione di criteri di priorità all'interno dei carichi di lavoro, sulla base delle esperienze sviluppate dalle singole autorità; utilizzo (giudicato preferibile) di strumenti come i provvedimenti generali applicabili a grandi categorie tematiche o di titolari e la pubblicazione di linee-guida che indichino gli approcci corretti in termini di protezione dei dati; ricorso ad ogni possibile strumento di semplificazione amministrativa (autorizzazioni generali, esenzioni da obblighi di notifica, introduzione del *privacy officer* all'interno delle aziende pubbliche e private).

I temi approfonditi nel corso delle sessioni parallele comprendevano la protezione dei dati sul luogo di lavoro (accesso ai fascicoli personali dei lavoratori; controllo dell'utilizzo di strumenti di posta elettronica e bilanciamento fra interessi del datore di lavoro e diritto del dipendente alla tutela della propria *privacy*, in particolare nell'esperienza di alcuni Paesi scandinavi); il ruolo delle autorità di protezione dati nel bilanciamento fra diritto alla *privacy* e diritto di accesso ai documenti amministrativi; il diritto all'oblìo degli interessati rispetto al funzionamento di alcuni motori di ricerca; l'utilizzo della videosorveglianza in ospedali psichiatrici, luoghi di lavoro e condomìni; le attività delle "centrali rischi" e l'esigenza di una maggiore armonizzazione degli approcci nazionali in materia; le attività di sensibilizzazione messe in atto dalle autorità di protezione dei dati e l'esigenza di ripensare la strategia comunicativa ed operativa anche alla luce delle conclusioni raggiunte sul punto dalla Conferenza internazionale di Londra.

Gruppo internazionale sulle telecomunicazioni

Il Garante ha partecipato nel corso del 2006 alle due riunioni annuali *dell'International Working Group on Data Protection in Telecommunications* (Iwgdpt). Il gruppo, che coinvolge un numero consistente di rappresentanti delle autorità nazionali di controllo e organizzazioni private non solo europee, continua ad allargarsi a nuovi partecipanti, e nel 2006 ha visto la presenza anche di una delegazione cinese. Fra i temi più significativi affrontati dall'Iwgdpt devono essere annoverati l'ampio dibattito relativo ai profili tecnologici della cartella clinica elettronica che ha portato all'approvazione di un documento di lavoro sul tema, la riflessione sulle implicazioni in materia di *privacy* dell'utilizzo della tecnologia *Voip* (*Voice over Internet Protocol*) e l'approfondimento dedicato alle tecnologie di protezione dei diritti di proprietà intellettuale.

Nel documento sulle cartelle cliniche elettroniche il gruppo ha raccomandato di valutare attentamente le categorie di dati sanitari da inserire nei documenti, suggerendo di escludere i dati genetici e psichiatrici, e ribadendo il ruolo del consenso dell'interessato (autonomo, libero e informato) e la necessità di una stretta osservanza del principio di finalità. I dati devono essere esatti e aggiornati e il trattamento elettronico deve essere protetto da dispositivi di cifratura rafforzati e meccanismi di autenticazione sicura per l'accesso.

Nel documento sulla telefonia in rete, il gruppo ha richiamato anzitutto i rischi che tale tecnologia comporta con riferimento alla violazione della segretezza delle comunicazioni. I telefoni *Voip* sono tecnicamente dei *computer* connessi a Internet, e dunque sono esposti a tutti i rischi associati alla navigazione in rete, dal punto di vista della sicurezza e della riservatezza. Alcune raccomandazioni sono state rivolte ai legislatori nazionali, i quali dovranno garantire che i fornitori di servizi *Voip* assicurino gli stessi livelli di sicurezza e *privacy* offerti dai fornitori di servizi di telefonia classici. Un'altra serie di raccomandazioni è stata indirizzata ai fornitori di servizi e *software Voip* per segnalare la necessità di garantire: un'adeguata informativa dei clienti anche sui rischi del servizio, il rispetto del principio di necessità nel trattamento dei dati personali, la disponibilità di strumenti a tutela della *privacy* (come la soppressione della visualizzazione della linea chiamante) e un'utilizzazione dei dati relativi all'ubicazione limitata ai casi in cui siano veramente indispensabili.

Il documento dedicato alle tecnologie per la tutela della proprietà intellettuale (*Digital Rights Management*, Drm) in relazione alla *privacy* contiene alcune raccomandazioni rivolte soprattutto ai governi nazionali e ai produttori di *software*. Tali raccomandazioni mirano a sottolineare la necessità di non utilizzare le tecnologie Drm in modo tale da comprimere il diritto di accesso alle informazioni (a causa della indisponibilità dei documenti originali nei quali le informazioni sono contenute). Inoltre, l'impiego di queste tecnologie può comportare rischi per la *privacy* e la sicurezza dei sistemi informativi, soprattutto qualora esse siano utilizzate in ambito pubblico; ciò comporta la necessità di configurare i sistemi Drm in modo da tenere adeguatamente conto delle esigenze di comunicazione e dei vincoli normativi che valgono per i trattamenti effettuati in ambito pubblico.

Consiglio d'Europa

L'Autorità ha partecipato alla riunione annuale del Comitato consultivo della Convenzione n. 108/1981 (T-Pd). La discussione si è incentrata soprattutto sull'analisi svolta in un rapporto commissionato all'Università di Namur, cui si chiedeva di valutare l'attualità e l'applicabilità dei principi di protezione dei dati della stessa Convenzione alle reti mondiali di telecomunicazione. Ne è emersa la necessità di approfondire l'analisi di alcuni concetti che pertanto sono stati inseriti nel programma di lavoro del T-Pd per il biennio successivo. Si tratta, in particolare, del trasferimento dei dati all'estero, del concetto di profilazione, della nozione di titolare del trattamento *on-line* e dell'interpretazione del concetto di dato personale in relazione all'identità. È emersa altresì l'esigenza di aggiornare alcune raccomandazioni settoriali del Consiglio d'Europa, e in particolar modo la raccomandazione N R(89)2 dedicata al trattamento dei dati nei rapporti di lavoro.

La *Venice Commission* ha chiesto al segretario generale del Garante, Giovanni Buttarelli, di curare in vista della sessione di maggio 2007 a Venezia uno studio indipendente sulla sorveglianza nei luoghi pubblici e la protezione dei dati personali, al fine di evidenziare quali differenze si pongano rispetto ad altre forme di controllo come quello "umano" di polizia.

Giornata sulla protezione dei dati personali

Un altro tema sul quale si è concentrato il T-Pd durante il 2006 è stato l'organizzazione del *Data Protection Day*. Dopo aver chiesto alle delegazioni nazionali, attraverso un questionario, di pronunciarsi sull'idea (nata nell'ambito dell'attività di

awareness raising), e di fornire suggerimenti sulle iniziative da intraprendere, è stato deciso di lasciare ampia flessibilità agli Stati nell'organizzazione dell'evento, fissato per il giorno 28 gennaio, data commemorativa dell'apertura alla firma della Convenzione n. 108 (28 gennaio 1981). Il Consiglio d'Europa ha dedicato una pagina *web* specifica all'occasione, riportando le iniziative nazionali e il supporto di numerosi organismi internazionali, fra cui la Commissione europea, l'Edps, Europol, Interpol ed altri.

La formalizzazione di un diritto fondamentale alla protezione dati è stato un altro argomento che ha impegnato il T-Pd nel corso del 2006. Il gruppo ha riflettuto sull'opportunità di elaborare uno strumento specifico del Consiglio d'Europa, con l'intento di far rientrare tale diritto nella giurisdizione della Corte europea dei diritti umani. Due sarebbero le opzioni disponibili a tale scopo: un protocollo addizionale alla Convenzione europea dei diritti dell'uomo, che distingua il diritto alla protezione dei dati dal "tradizionale" diritto alla tutela della vita privata, oppure un protocollo addizionale alla Convenzione n. 108/1981 che preveda la competenza della Corte europea dei diritti umani rispetto alle violazioni della stessa Convenzione. Sul tema è stato chiesto al T-Pd di approfondire la riflessione, sia in riferimento ai lavori preparatori della Carta dei diritti fondamentali dell'Unione europea, sia in relazione alla giurisprudenza in materia di protezione dei dati elaborata dalla Corte di Strasburgo.

Ocse

Il *Working Party on Information Security and Privacy* (Wpisp) in seno all'Ocse ha dedicato nel 2006 una particolare attenzione ai temi legati alla *privacy*, anche al fine di fornire un contributo alla Conferenza ministeriale del 2008 (deliberata dal Consiglio dell'Ocse il 13 luglio 2006) che sarà dedicata al tema *"Il futuro di Internet"*. Durante tale conferenza una sessione (*"Privacy in a Participatory Web"*) sarà dedicata all'impatto delle innovazioni tecnologiche, dei processi gestionali e dell'utilizzo di Internet sulla sicurezza e sulla *privacy*.

La conferenza potrebbe rappresentare il punto di partenza per un ripensamento delle linee-guida Ocse del 1980 alla luce delle nuove tecnologie, nella consapevolezza della necessità di un quadro unitario in materia di protezione dati. Sulla base di un questionario compilato dalle delegazioni nazionali, è stato approvato il rapporto sull'applicazione transfrontaliera delle normative sulla *privacy*, dal quale è emerso che l'aumento dei flussi transfrontalieri di dati e dei rischi ad essi connessi in termini di garanzie comporta la necessità di migliorare la cooperazione nelle attività di implementazione delle normative stesse.

È altresì emerso che, rispetto all'anno di adozione delle linee-guida (1980), la maggioranza dei paesi Ocse è oggi dotata di autorità di controllo con poteri simili e ambiti di intervento sostanzialmente sovrapponibili. Queste autorità, tuttavia, si confrontano con problemi sempre maggiori nella gestione del contenzioso con componenti transnazionali, mentre gli strumenti giuridici nazionali e regionali non sono sufficienti a far fronte ai problemi di un mondo globalizzato. Gli esiti del rapporto hanno indotto il Wpisp a continuare a lavorare sul tema dell'*enforcement*, e il segretariato, coadiuvato da un gruppo di volontari di cui ha fatto parte anche l'Autorità italiana, ha redatto una bozza di raccomandazione del Consiglio, accompagnata da uno strumento operativo che faciliti la cooperazione nei casi applicativi che rivestono carattere transfrontaliero. La raccomandazione, pur essendo uno strumento di *soft law*, impegnerebbe gli Stati membri e potrebbe essere condivisa anche da Paesi non membri dell'Ocse.

Le tecnologie *Rfid* e le sue implicazioni rappresentano l'altro tema rilevante per la protezione dei dati su cui si è concentrato il gruppo nel corso del 2006. Il documento elaborato in materia, non ancora approvato in modo definitivo, si propone

di fornire una panoramica dettagliata dei rischi connessi all'impiego dei sistemi a radiofrequenze, aggravati nei casi di convergenza con altre tecnologie, come Internet. Dal punto di vista della protezione dei dati, gli aspetti più problematici sono legati all'invisibilità della raccolta, al tracciamento inconsapevole e alla possibilità di controllo nei casi di interconnessione attraverso il *web*.

Per altro verso, e-*authentication, identity management*, crittografia e sicurezza delle reti sono stati all'ordine del giorno delle riunioni, soprattutto in vista dell'organizzazione di numerosi seminari nel sud-est asiatico. In questo quadro si pone anche il rafforzamento della collaborazione con l'attività dell'Apec.

Infine, dalle risposte ai questionari diffusi tra i Paesi membri nel 2006 non è emersa la necessità di una revisione immediata delle linee-guida sulla sicurezza e sulla crittografia.

Cooperazione bilaterale

Nel 2006 è proseguita la collaborazione fra il Garante e l'autorità rumena di protezione dei dati, formalizzata anche attraverso un accordo bilaterale firmato dai presidenti delle due autorità in occasione della Conferenza internazionale di Londra. Nel mese di settembre il presidente del Garante si era recato a Bucarest, su invito dell'autorità rumena, per perfezionare i termini di tale accordo e approfondire la conoscenza dei meccanismi di funzionamento dell'autorità. Oltre ad un supporto costante fornito nel corso dell'anno per le vie brevi (*e-mail*, scambi di informazioni), nel mese di luglio è stata organizzata una visita di funzionari del Garante presso l'autorità rumena per discutere di problematiche connesse all'attività ispettiva e di trattazione del contenzioso (con il sostegno finanziario del programma Taiex). All'inizio del 2007 si è tenuto anche un incontro fra funzionari dell'autorità rumena e rappresentanti del Garante per illustrare alcuni aspetti problematici connessi al trasferimento di dati verso Paesi terzi.