contributo alla consultazione pubblica del 2006). Tale proposta è stata, però, successivamente bocciata dal Consiglio e dal Parlamento europeo.

Il Gruppo ha pubblicato quindi un parere (WP 150 del 15 maggio 2008) indirizzato in via primaria alla Commissione europea, ma rivolto anche al Parlamento ed al Consiglio. In sintesi, il parere sottolinea la necessità di garantire più efficacemente la sicurezza delle reti e facilitare l'esercizio dei diritti degli utenti. In particolare, esso condivide alcune delle osservazioni contenute nel documento pubblicato sullo stesso tema dal Garante europeo per la protezione dei dati (10 aprile 2008); i Garanti concordano sull'opportunità di guardare alle reti in una prospettiva più ampia, data la natura sempre più spesso "mista" (pubblica/privata) delle reti di comunicazione elettronica, nonché sulla valutazione positiva di alcuni emendamenti proposti dalla Commissione – soprattutto il chiarimento relativo all'applicabilità delle disposizioni della direttiva a tecnologie quali l'*Rfid*, in quanto utilizzino "reti di comunicazione elettronica disponibili al pubblico" per veicolare i segnali di trasmissione, e l'attribuzione del diritto di intraprendere azioni legali in caso di violazioni della normativa nazionale (*ad es.*, in materia di *spam*) anche a soggetti non direttamente colpiti, ma comunque direttamente interessati, quali i fornitori di servizi Internet.

Il Gruppo art. 29 ha proposto, tuttavia, ulteriori emendamenti che riguardano, in modo particolare, l'estensione dell'obbligo per i fornitori di servizi di comunicazione di notificare violazioni e/o rischi per la sicurezza delle reti a tutti gli *"utenti"* dei servizi di comunicazione elettronica (anziché ai soli *"abbonati"* a tali servizi); ciò dovrà avvenire secondo un approccio equilibrato che tenga conto dei costi e dell'impatto che tali notifiche possono esplicare sull'attività dei fornitori (*ad es.*, in termini di danno di immagine). Inoltre, il Gruppo ha segnalato l'opportunità di ampliare la definizione di *"sistemi di chiamata"* contenuta nella Direttiva 2002/58/Ce (art. 13) includendovi i sistemi di *"comunicazione"* (per tenere conto degli sviluppi tecnologici legati, ad esempio, alla tecnologia *Bluetooth*, il cui funzionamento è difficilmente assimilabile ad una *"chiamata"* sul terminale dell'utente); ciò consentirebbe di garantire una protezione più efficace nei confronti delle comunicazioni indesiderate. Per lo stesso motivo, l'estensione del *"diritto di intra-*

prendere azioni legali" dovrebbe comprendere le violazioni dell'articolo 5.3 della direttiva, ossia l'uso e l'installazione, per esempio, di *spyware*. Il parere ricorda, inoltre, l'esigenza di garantire l'applicazione del principio di necessità (o minimizzazione) nell'utilizzo e nella gestione dei servizi di comunicazione elettronica, attraverso la realizzazione dell'approccio definito *"privacy by design"*, nonché l'obbligo per i *provider* di assicurare, più in generale, la riservatezza delle comunicazioni a prescindere dalla configurazione fisica delle reti utilizzate per la trasmissione di tali comunicazioni – quindi tenendo conto di eventuali accordi tecnologici stipulati con soggetti o imprese di Paesi terzi rispetto ai flussi di dati in partenza dall'Ue.

L'iter comunitario è successivamente proseguito con l'adozione da parte del Parlamento europeo, il 24 settembre 2008, delle proposte di modifica del pacchetto comunicazioni elettroniche. Riguardo alla Direttiva 2002/58/Ce, il Parlamento ha seguito solo parte delle indicazioni contenute nel parere del Gruppo articolo 29; peraltro, alcune delle proposte presentate dai gruppi parlamentari introducevano obblighi ulteriormente stringenti (*ad es.*, relativamente alla segnalazione di rischi o violazioni reali della sicurezza in rete da parte dei *provider* di servizi di comunicazione elettronica). Come accennato, il Parlamento ha respinto la proposta di costituire un'autorità unica europea incaricata di vigilare e legiferare sulla sicurezza delle reti di comunicazione elettronica. Le modifiche del Parlamento, inoltre, proponevano di estendere il campo di applicazione della direttiva ai *"servizi della società dell'informazione"*, e non ai soli servizi di comunicazione elettronica accessibili al pubblico, e consentivano agli *Isp* di utilizzare i dati di traffico anche per finalità connesse alla *"sicurezza"* delle reti e delle comunicazioni.

Conformemente alla procedura di codecisione, si è quindi avuta, il 28 novembre 2008, l'adozione della proposta modificata del Consiglio Ue relativa al pacchetto normativo in oggetto. Il Consiglio ha recepito solo una parte degli emendamenti del Parlamento ed ha tenuto conto in misura ridotta delle osservazioni contenute in un documento di compromesso presentato dalla Commissione il 7 novembre 2008. In base al testo del Consiglio, le principali modifiche al testo attuale della Direttiva 2002/58/Ce riguarderebbero gli obblighi di notifica delle violazioni della sicurezza che coinvolgano dati personali (limi-

tate alle violazioni *"gravi"*, non meglio definite, secondo un meccanismo in tre tempi che prevede anche la notifica alle autorità di protezione dati, e solo con riguardo agli *"abbonati"* interessati); l'estensione della possibilità di trattare dati di traffico per non meglio precisati *"scopi di sicurezza"* (secondo quanto indicato nel nuovo comma 6a dell'articolo 6); l'estensione della possibilità di ottenere tutela (giuridica o di altra natura) contro violazioni degli obblighi concernenti le comunicazioni indesiderate (*spam*: articolo 13) a tutte le persone fisiche e giuridiche, compresi quindi gli stessi fornitori dei servizi di comunicazione elettronica, e con riguardo agli *"utenti"* di tali servizi (non soltanto, dunque, agli *"abbonati"* come attualmente previsto). Il Consiglio ha specificato l'ambito delle comunicazioni indesiderate (indicando che *"electronic mail"* comprende anche *Sms* e *Mms*). La Commissione europea, attraverso il Commissario Reding, si è espressa negativamente su tale proposta di compromesso, ritenuta troppo timida; il Garante europeo ha successivamente reso pubblico un secondo parere sulle proposte di modifica (9 gennaio 2009) contenente numerose e dettagliate osservazioni, in buona parte critiche.

Anche il Gruppo art. 29 ha adottato un nuovo parere, il 10 febbraio 2009, relativo al testo licenziato dal Consiglio e, in parte minore, agli emendamenti proposti dal Parlamento europeo.

I Garanti plaudono all'estensione (proposta dal Parlamento europeo) dell'ambito di applicazione della direttiva ai *"servizi della società dell'informazione"*; inoltre, chiedono di chiarire sia le modalità di notificazione delle violazioni della sicurezza dei sistemi telematici, sia i soggetti coinvolti (suggerendo di indirizzare la notifica anche agli utenti solo in caso di violazioni che comportino *"conseguenze avverse"* per la protezione dei loro dati personali), sia il concetto di *"grave"* violazione della sicurezza informatica. Peraltro, il parere giudica superflua e potenzialmente lesiva della *privacy* individuale l'introduzione, da parte del Consiglio, del comma 6a nell'art. 6 della direttiva; tale comma prevederebbe la possibilità di trattare dati di traffico *"per scopi di sicurezza delle reti e delle informazioni"* non meglio precisati. Vengono ritenuti inopportuni anche alcuni emendamenti proposti dal Parlamento europeo (e non accettati dal Consiglio) quali, in particolare, la previsione di ritenere la configurazione di *default* dei programmi di navigazione (*browser*) come

manifestazione del consenso espresso dell'interessato rispetto alla ricezione di, ad esempio, *cookies* o altri programmi; quanto all'obbligo di segnalare alle autorità di protezione dati le richieste di accesso ai dati di traffico telematico da parte delle autorità giudiziarie e di polizia, che il Parlamento proponeva di introdurre su base automatica nei confronti dei *provider*, il Gruppo ha ritenuto preferibile chiedere la predisposizione di un rapporto annuale, redatto sulla base di criteri comuni e uniformi, così da consentire alle singole autorità di valutare la necessità di accertamenti ulteriori. Fra gli aspetti del testo del Consiglio sui quali il Gruppo esprime il proprio apprezzamento, occorre ricordare la possibilità per le persone giuridiche di far valere i propri diritti in caso di comunicazioni indesiderate ed i chiarimenti, contenuti nei *"considerando"* aggiunti al testo della direttiva, relativi alla natura di *Sms*, *Mms* ed altre modalità di comunicazione elettronica.

Enforcement

Il Gruppo ha conferito mandato al sottogruppo *Enforcement* di impostare l'attività di verifica relativa all'applicazione della direttiva sulla conservazione dei dati a fini di lotta alla criminalità (Direttiva 2006/24/Ce sulla *data retention*). Sono stati designati come *rapporteurs* l'autorità italiana e quella cipriota. Superate le iniziali difficoltà sull'impostazione dell'azione di *enforcement* (la direttiva non è stata attuata ancora in molti paesi), il sottogruppo ha acquisito, attraverso le autorità di protezione dei dati, informazioni di base sull'organizzazione del settore, sul tipo di società – nazionali o transnazionali – che erogano i servizi, sui poteri delle autorità stesse di supervisione e controllo dei trattamenti di dati. Successivamente ha definito i criteri per la selezione delle società fornitrici di reti e di servizi di comunicazioni elettroniche cui rivolgersi. Il campione selezionato sarà chiamato a fornire adeguata risposta alle domande formulate in un apposito questionario comune. Nel caso specifico il Gruppo ha scelto un campione rappresentativo limitato nel numero e formulato questioni molto precise soprattutto sulla sicurezza dei dati e dei sistemi. La prima fase a livello nazionale sarà basata sulla somministrazione di un questionario, conciso e preciso, e sarà seguita da una seconda fase di controllo *in loco* delle risposte fornite, ove ritenuto necessario dall'autorità di protezione dei dati. L'azione si svolgerà nel corso del 2009 e dovrebbe concludersi, con il rapporto finale e le considerazioni del Gruppo art. 29, nei primi mesi del 2010.

Trattamento dei dati dei passeggeri aerei (*Pnr*)

Diverse le attività svolte in connessione alle vicende *Pnr*.

Pnr Usa: il Gruppo art. 29 ha approvato il nuovo testo dell'informativa breve, lunga ed extrabreve per le compagnie aeree e le agenzie di viaggio, anche ai fini delle prenotazioni effettuate telefonicamente, in rapporto al nuovo accordo *Pnr* del luglio 2007.

La visita negli Usa per la revisione congiunta dell'applicazione degli accordi non si è effettuata, perché la nuova amministrazione americana ha chiesto tempo per prepararsi. Peraltro non è chiaro quale presenza e ruolo assumeranno nella delegazione europea le autorità di protezione dei dati personali.

Pnr europeo: continuano i lavori di *follow up* del parere congiunto adottato nel dicembre 2007 dal Gruppo art. 29 e dal *Working Party on Police and Justice* (*Wppj*) sulla proposta di *"proposta di decisione-quadro"* che istituisce un sistema europeo di raccolta ed analisi delle informazioni che obbliga i vettori aerei a mettere a disposizione delle autorità competenti per la prevenzione e repressione dei reati in anticipo rispetto all'effettuazione dell'imbarco i dati dei passeggeri raccolti fin dal momento della prenotazione del volo. Da segnalare il parere legale dell'ufficio giuridico del Consiglio, che ha indicato l'opportunità di modificare la base giuridica scelta per la redazione della proposta di decisione-quadro sul *Pnr* europeo e di garantire un migliore rispetto dei diritti di protezione dati; in questo caso, il servizio giuridico suggerisce una modifica della Direttiva 95/46/Ce che estenda il suo ambito di applicazione ai trattamenti di terzo pilastro. I lavori di analisi e discussione della proposta sono in corso presso il Consiglio, che intenderebbe mantenere la base giuridica scelta. Il Gruppo ha deciso la preparazione di un secondo parere, sempre congiuntamente al *Wppj*.

Follow-up Pnr Canada: la revisione congiunta dell'applicazione degli accordi si è svolta nell'autunno del 2008 con la collaborazione delle autorità canadesi.

La delegazione era formata anche da rappresentanti delle autorità di protezione dei dati personali. Nell'occasione, anche su sollecitazione scritta rivolta dal Gruppo alla Commissione per chiedere chiarimenti e sottolineare che le attività di *matching*, controlli, *ecc.* previste dal *Memorandum* non sembrano essere conformi all'accordo *Pnr* raggiunto fra Ue e Canada, è stato sollevato anche il problema del *Memorandum of understanding* Canada (*Passenger Protect Program*) / Compagnie aeree europee.

Il Gruppo ha anche adottato un documento che fissa alcuni *standard* generali rispetto al trasferimento di dati relativi a passeggeri (*Pnr*) (WP 151). Il documento si era reso necessario considerate le crescenti richieste di tali dati formulate da diversi Paesi (quali India, Corea, Australia) e le conseguenti pressioni sulle compagnie aeree. Il documento potrebbe servire non solo per i negoziatori comunitari (Consiglio e Commissione) con i Paesi summenzionati, ma anche per influenzare l'Icao a migliorare i global *standard* già elaborati.

Il Gruppo ha anche espresso dubbi e perplessità in una lettera alla Commissione relativamente alle richieste americane di un nuovo sistema di controllo degli ingressi (Esta: *Electronic System for Travel Authorization*).

Il sistema prevede che chi intende recarsi negli Usa invii in anticipo un formulario elettronico contenente gli stessi elementi oggi richiesti in formato cartaceo. Il passaggio da un sistema cartaceo ad uno elettronico, anche per gli effetti sulla legge applicabile, presenta alcune criticità, evidenziate alla Commissione per consentirle le opportune iniziative prima che la proposta entri in vigore.

Anche per quanto riguarda l'introduzione in Europa di un analogo sistema, che sembra potersi evincere dal sopra ricordato pacchetto di iniziative per il rafforzamento dei controlli alle frontiere esterne, il Gruppo ha inviato una lettera al Commissario Barrot per richiamare l'attenzione della Commissione sulla necessità di valutare l'effettiva applicazione di disposizioni comunitarie già in essere prima di procedere all'introduzione di ulteriori obblighi in materia di raccolta e trattamento dei dati relativi a passeggeri.

20.2. LA COOPERAZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Da segnalare in particolare due elementi: da un lato l'intensificarsi e lo strutturarsi dei lavori del Gruppo di lavoro Polizia e giustizia (*Wppj*) sotto la guida del presidente del Garante; dall'altro, il crescente coordinamento con il Gruppo art. 29, volto a favorire una valutazione possibilmente completa degli aspetti di protezione dei dati personali delle iniziative che non si esauriscono nell'ambito di uno dei pilastri in cui si articolano le competenze dell'Unione: un caso classico riguarda l'uso dei dati dei passeggeri aerei, raccolti

per la prestazione del servizio di trasporto, ma oggetto di crescenti pressioni ed interventi normativi per rendere i relativi *database* di immediato e pieno accesso per le forze di polizia e giudiziarie a fini di *"valutazione del rischio"* e profilazione. Analogamente per i tabulati relativi alle utenze e al traffico telefonico e telematico.

Come si è già rilevato, per il modo di elaborazione e per la frammentarietà delle competenze in materia in seno all'Unione, molte nuove iniziative dell'Unione europea che riguardano dati personali sono tuttora sottratte al controllo delle autorità di protezione dei dati, alcune perché riguardano materie di terzo pilastro, altre perché non rientrano in modo netto in uno dei tradizionali pilastri dell'Ue.

Il Gruppo art. 29 ed il Gruppo di lavoro polizia e giustizia, oltre a rivolgersi al Parlamento europeo che svolge peraltro un ruolo ancora limitato nelle materie non facenti parti del *cd. "primo pilastro"* hanno, come ricordato sopra, cooperato ad iniziative congiunte.

Le autorità di protezione dei dati hanno segnalato con preoccupazione sempre maggiore il progressivo venir meno di *"momenti istituzionalizzati"* presso il Consiglio ed anche, in parte, presso la Commissione, che favorissero la necessaria valutazione dell'impatto delle nuove iniziative sui diritti fondamentali della persona e, più specificamente, sulla tutela dei dati personali; il ritardo dell'entrata in vigore del nuovo trattato non ha certamente giovato.

Tra le iniziative legislative in ambito europeo va finalmente registrata la decisione quadro sui princìpi per il trattamento dei dati personali nel terzo pilastro, elemento richiamato dal *"Programma de L'Aja"* come necessario di riferimento per le attività di cooperazione tra forze di polizia e magistratura, al fine di prevenire e reprimere reati (GU L350 del 30 dicembre 2008).

Il testo della decisione quadro tuttavia, come ricordato, è stato modificato *in pejus* durante la discussione in Consiglio, rispetto all'originaria proposta della Commissione, e non contiene più alcuna previsione circa la creazione di un organismo parallelo a quello del Gruppo art. 29 con ruolo indipendente e consultivo. Altri aspetti su cui le autorità di protezione dati hanno rilevato la debolezza dell'impianto normativo e delle tutele previ-

ste, riguardano: il campo di applicazione, limitato a disciplinare i soli scambi di dati tra i Paesi Ue e non direttamente applicabili ai trattamenti di dati nazionali, i meccanismi che consentono l'ulteriore trasferimento dei dati a Paesi ed organismi terzi, i diritti di accesso ed informazione delle persone interessate e le modalità del trattamento dei dati sensibili. Si tratta di aspetti di grande rilievo, suscettibili di incidere negativamente sul raggiungimento di quell'elevato livello di tutela che la decisione quadro dichiara di voler garantire agli interessati, ribaditi nel comunicato stampa del Gruppo polizia e giustizia, soprattutto allo scopo di ricordare che i princìpi devono essere coerenti in tutti gli Stati.

Va menzionato poi che nel terzo pilastro, a parte l'attività del Gruppo polizia e giustizia, è continuata l'attività in particolare delle Autorità comuni di controllo Schengen, Europol e Dogane, organismi di supervisione e controllo istituiti da specifiche convenzioni.

È continuata anche l'attività di supervisione a livello europeo sul funzionamento del sistema Eurodac, coordinata dal Garante europeo.

Questo modello di supervisione sarà applicato, una volta entrati in funzione, anche per il Vis (sistema informativo visti) – la cui entrata in funzione è prevista per la fine del 2009 – nonché per il SIS II che sarà invece operativo verso la seconda metà del 2010, essendo emersi problemi di notevole complessità.

Sulle modalità attuative del Vis sembra essere stato raggiunto l'accordo interistituzionale per assoggettare all'obbligo di fornire le impronte digitali i bambini a partire dai dodici anni, sia per la richiesta di visti, sia per altri tipi di documenti, attraverso la definizione di "modelli *standard*" europei e per disciplinare le procedure presso gli uffici consolari e gli altri uffici abilitati al rilascio dei visti di breve soggiorno (*cd. "visti Schengen"*).

L'Italia ha presentato, ed è tuttora in discussione presso il Parlamento, il disegno di legge di ratifica del *cd. "Trattato di Prüm"* (d.l. n. 586) che prevede tra l'altro l'istituzione della banca dati Dna. Nel frattempo, su forte pressione della presidenza di turno del Consiglio sono stati adottati e pubblicati i testi delle due decisioni del Consiglio che trasformano in iniziativa legislativa dell'Unione gran parte delle disposizione del Trattato di Prüm e delle disposizioni applicative (Decisione 2008/615/GAI del 23 giugno 2008 in GU L210 - Decisione 2008/616/GAI del 23 giugno 2008 in GU L210).

Le relative disposizioni entreranno in vigore nel luglio 2009.

Su tali temi il Garante ha elaborato spunti e proposte per garantire il necessario rispetto dei princìpi di protezione dei dati personali nell'elaborazione e nell'attuazione delle disposizioni suindicate.

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

Nel periodo considerato l'Acc ha continuato la sua attività sulla proposta di decisione per l'integrazione di Europol tra le strutture dell'Unione e sulla definizione del quadro generale di riferimento per lo svolgimento della sua attività e le norme attuative della proposta medesima.

Il testo della proposta ha tenuto nella giusta considerazione le osservazioni formulate dall'Acc, in particolare per quanto concerne le garanzie per l'accesso ai dati da parte degli interessati e l'esercizio effettivo dei diritti conferiti. Complessivamente gli aspetti relativi al trattamento dei dati personali da parte di Europol sono sostanzialmente immutati rispetto alle previsioni contenute nella Convenzione Europol. Il Consiglio ha raggiunto l'accordo sul testo che è stato quindi adottato senza discussione e pubblicato nel mese di aprile 2009 (Decisione 2009/371/GAI del 6 aprile 2009 in GU L121). L'entrata in vigore è prevista per il 1° gennaio 2010 e per quella data dovranno essere completate le modifiche per adattare le vigenti disposizioni alle nuove previsioni: si tratta ad esempio delle regole per l'apertura del *file* di analisi, per la trasmissione a Stati ed organismi terzi di dati nell'ambito di una procedura che richiede il parere dell'Acc Europol, ma che determinano anche la necessità per la stessa Acc di modificare il suo regolamento interno.

Per quanto in particolare riguarda il lavoro di supervisione, si conferma l'importanza dell'attività ispettiva, condotta annualmente, dell'Acc e affidata ad un gruppo che comprende esperti degli aspetti tecnologici.

L'ispezione si svolge di regola nel mese di marzo. Nel corso dell'ultima i partecipanti hanno focalizzato le verifiche sul contenuto e qualità dei dati trattati nei *file* di analisi e nel sistema di informazione Europol, sulla valutazione del funzionamento di quest'ultimo, sull'infrastruttura tecnica utilizzata e sull'attuazione delle raccomandazioni formulate dall'Acc nelle precedenti ispezioni. Con l'occasione sono stati svolti accertamenti sui dati detenuti da Europol relativi a procedure di ricorso aperte presso l'appo-

sito comitato dell'Acc, nonché nel funzionamento e contenuti dei progetti "*Check the web*" ed Oasis.

Dall'esito dell'ispezione e dagli accertamenti svolti anche in sede nazionale dalle autorità di protezione dei dati, incluso il Garante, è risultato che va maggiormente verificata la legittimità dell'inserimento di dati nel sistema di informazione Europol legata ad operazioni Frontex. Pertanto pur se l'Acc ha riconosciuto l'alto grado di adeguamento alle raccomandazioni formulate da parte di Europol, sono state rappresentate preoccupazioni per un uso del sistema che potrebbe essere non pienamente rispettoso delle regole esistenti.

L'Acc ha continuato a seguire, anche attraverso i risultati dell'ispezione, l'uso del sistema "*check the web*", un portale che mette a disposizione degli Stati partecipanti le informazioni ed i *link* ai siti *web* utili ai fini della lotta alla criminalità e l'uso di OASIS, progetto messo a punto per consentire analisi strategiche e di sistema al di là dei limiti imposti dai singoli *file* di analisi ritenuti troppo angusti.

Attività consultiva dell'Acc: l'Acc ha espresso parere sull'apertura di un *file* di analisi e su due richieste di autorizzare il direttore di Europol ad aprire negoziati con Paesi terzi per la trasmissione di dati personali. Nell'occasione l'Acc ha analizzato sulla base delle informazioni fornite da Europol il livello di adeguatezza dei due Paesi in questione, ravvisando problemi più importanti rispetto all'apertura di negoziati con uno di essi (la Russia); per l'altro, (Israele), invece, i pur rilevanti problemi riscontrati potrebbero incidere sulla stipula di un accordo per la trasmissione dei dati da Europol.

Nella conferenza, tenuta a Bruxelles il 9 ottobre, per celebrare i dieci anni di attività dell'Acc, i risultati finora raggiunti e le sfide future, il presidente del Garante, quale presidente del Gruppo polizia e giustizia ha offerto diversi spunti sulle attività svolte nel settore giustizia, sicurezza e libertà, evocando possibili futuri scenari per la cooperazione tra le autorità di protezione dei dati nel settore.

Attività del Comitato ricorsi: il Comitato ha definito un caso basato su una richiesta di accesso e verifica dei propri dati. In ragione delle circostanze emerse il Comitato ha chiesto ad Europol di riconsiderare la decisione iniziale di non rivelare l'esistenza o meno di dati relativi all'interessato ed ha ottenuto che questi ottenesse una risposta chiara in

merito. Un altro caso è tuttora pendente. L'Acc ha quindi discusso ed approvato la relazione di attività relativa al biennio 2006-2008, in corso di pubblicazione.

Le attività dell'Acc, inclusi i pareri adottati e le iniziative svolte sono comunque disponibili anche in italiano sul sito dell'Acc.

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

In base alla Convenzione istitutiva, il Sistema informativo doganale (Sid) è formato da una base di dati centrale cui si può accedere tramite terminali in ogni Stato membro. Alla Commissione europea è affidata la gestione tecnica dell'infrastruttura del sistema.

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

L'Acc Dogane ha esaminato nel 2008 la bozza di rapporto sul funzionamento del sistema chiedendo di evidenziare alcuni aspetti di criticità emersi nell'ispezione svolta nel 2007, in particolare sui profili di sicurezza.

Le raccomandazioni dell'Acc richiedono di chiarire che ai fini del corretto adempimento degli obblighi del trattamento dei dati personali la responsabilità deve essere attribuita congiuntamente ad Olaf, l'organismo antifrode della Commissione europea, ed agli Stati membri; di migliorare la procedura per mantenere la registrazione dei diritti e credenziali attribuiti agli operatori e la valutazione periodica di queste, nonché una politica comune per la gestione delle *password* e il miglioramento della *management policy* del sistema per garantire la qualità e l'integrità dei dati. L'Acc ha anche richiesto di sviluppare azioni in materia di formazione del nuovo SIS basato sul *web*, fornendo la necessaria attenzione agli aspetti di protezione dei dati, preparando linee-guida ed istruzioni su aspetti specifici.

L'Acc ha inoltre completato la verifica del rispetto delle condizioni per la raccolta e trattamento dei dati personali iniziata lo scorso anno, sia con un *audit* sulla congruità delle misure di sicurezza adottate presso l'unità centrale, sia con la raccolta di informazioni a livello nazionale delle misure esistenti sulla scorta di un questionario comune; prima di intraprendere un'azione comune finalizzata a verificare la liceità dei trattamenti di dati personali, ha suggerito agli Stati di svolgere un ruolo più attivo per far individuare e se possibile, prevenire problemi di sicurezza.

A tal fine l'Acc ha sviluppato una sorta di *kit* di autovalutazione che il Regno Unito, la Grecia e la Slovacchia stanno sperimentando. Al termine della sperimentazione un nuovo questionario/*test* sarà messo a punto quale base, per le autorità di protezione dei dati, delle attività nazionali di supervisione.

Va infine segnalato che l'Acc sarà chiamata a fornire il suo parere su una proposta di atto comunitario, probabilmente una decisione, sull'uso delle tecnologie dell'informazione a scopi doganali che sostituirà la Convenzione indicata sopra.

Schengen

L'attività dell'Acc Schengen pur continuando a seguire gli sviluppi del SIS ed il passaggio dal vecchio al nuovo sistema, si è maggiormente incentrata sul funzionamento dell'attuale sistema.

L'integrazione di nove dei dieci Paesi entrati a far parte dell'Unione nel 2004 nel SIS e l'abolizione delle frontiere con questi nuovi Stati è il fatto più importante degli ultimi anni. Anche la Svizzera ed il Liechtenstein sono oggi considerati a pieno titolo nella cooperazione Schengen.

L'Acc Schengen ha pertanto ritenuto opportuno completare le verifiche nazionali sulla legittimità dei trattamenti di dati in relazione alle segnalazioni inserite nel SIS in base agli articoli 97 e 98, nonché procedere ad un aggiornamento della guida all'esercizio del diritto di accesso ai dati contenuti nel SIS, anche in vista dell'entrata in funzione del SIS II prevista per la seconda metà del 2010.

La Commissione europea, che avrà la responsabilità della gestione tecnica del SIS II sta predisponendo, con la collaborazione delle autorità nazionali di protezione dei dati, una campagna informativa per i cittadini.

L'Acc ha iniziato a seguire la migrazione dei dati dal SIS al SIS II e lo scenario futuro della supervisione e controllo (che passerà dall'Acc all'Edps con le autorità di protezione dati).

L'Acc ha inoltre adottato un parere in relazione all'attuazione dell'articolo 102 a) della Convenzione.

È stato altresì predisposto ed approvato il rapporto di attività, che copre il triennio 2005-2008 (*Schengen Joint Authority - Activity Report - Dec. 2005 - Dec. 2008*).

In relazione all'azione comune di verifica in ciascuno dei Paesi partecipanti della rego-

larità delle segnalazioni inserite nel sistema con riferimento all'art. 99 della Convenzione (sorveglianza discreta e controllo specifico), il Garante ha ampliato l'attività di verifica rispetto a quanto deliberato dall'Acc. A conclusione della parte nazionale dell'accertamento, è stato adottato un provvedimento con le prescrizioni ritenute necessarie a conformare il trattamento alle disposizioni della Convenzione. Si nota tuttavia una certa difficoltà da parte del Ministero dell'interno ad adeguarsi alle prescrizioni del Garante, in particolare per quanto riguarda la corretta individuazione dei casi in cui possono essere inserite nel SIS segnalazioni basate su questo articolo, che fa riferimento al concetto di *"reati particolarmente gravi"* assunto come non esistente in Italia. Altri aspetti tuttora aperti concernono la supervisione delle misure di sicurezza: si attende il completamento della migrazione in altra sede di tutto il sistema per procedere ad una verifica *in loco.*

Eurodac

L'attività di coordinamento del Garante europeo per la protezione dei dati personali, dopo l'adozione del primo rapporto, prosegue con gli approfondimenti necessari a valutare le procedure seguite dagli Stati sia per definire l'età (dodici anni) oltre la quale le impronte possono essere inserite nel sistema, sia per informare le persone dell'uso che sarà fatto delle impronte, nonché sulle modalità di trattamento dei dati in *Dublinet.*

Al termine degli accertamenti svolti (*v. Relazione* 2007, *pp.* 168-169) è stato adottato un *provvedimento* [doc. *web* n. 1537606] contenente le prescrizioni considerate per conformare il trattamento alle norme vigenti. Molte raccomandazioni formulate nel rapporto del Garante europeo sono state riprese dal Garante e fatte oggetto di apposita prescrizione.

Anche in questo caso gli accertamenti sono stati estesi alla procedura di applicazione della Convenzione di Dublino, che prevede la possibilità di rinvio del richiedente asilo ad altro Paese laddove risulti esistente una segnalazione di questo Paese.

Il Garante è intervenuto in particolare per verificare l'uso delle *cd. "ricerche speciali"* (richieste di accesso ai dati che il regolamento Eurodac consente permettere l'esercizio dei diritti della persona interessata). A seguito dell'intervento del Garante l'uso di tali categorie è cessato, risultando essere frutto di un errore. Tuttavia, il mancato esercizio da parte degli interessati del diritto di accesso ai propri dati determina incertezza sulla compren-

sione delle informazioni fornite per iscritto e sull'utilizzo di tale facoltà. Il *provvedimento* adottato dal Garante richiede specificamente che l'informativa sia data nei modi e nei tempi più idonei a far comprendere gli obiettivi e l'impatto del trattamento dei dati ed a consentire il pieno esercizio dei diritto di accesso e degli altri diritti collegati.

Altre prescrizioni hanno riguardato l'adeguamento delle misure di sicurezza.

La Commissione europea ha presentato all'inizio di dicembre due proposte di regolamento (Com (2008)825 e Com (2008)242) per modificare il quadro giuridico esistente, facendo seguito all'attività di valutazione svolta in relazione alla gestione della banca dati Eurodac ed alle procedure di asilo.

Un punto particolarmente delicato dell'agenda della Commissione, che non ha formato oggetto per il momento di una proposta di iniziativa legislativa specifica, concerne la possibilità per le forze di polizia di accedere ad Eurodac; le autorità di protezione dei dati personali hanno avuto modo di occuparsi di tale questione attraverso l'attività del *Working Party Police and Justice* (*v. infra*).

Working Party on Police and Justice

L'attività del Gruppo di lavoro polizia e giustizia è proseguita con grande intensità nel 2008 consolidando, sotto la presidenza del presidente del Garante, l'efficiente cooperazione tra le autorità di protezione dei dati europee ed accrescendo l'incisività dell'azione svolta. Molta attenzione è stata posta per cercare di accreditare la voce del Wppj nelle sedi appropriate e soprattutto stimolare ed intensificare i contatti con il Parlamento europeo, da sempre sensibile al tema del rispetto dei diritti che segue in particolare attraverso la Commissione Libe.

Pur essendo ancora un organismo informale, con le opportune sinergie con le Acc sopra ricordate e la possibilità di fare riferimento al segretariato comune di queste il Wppj ha tenuto quattro riunioni plenarie nel corso dell'anno; ciò ha permesso di decidere le azioni da intraprendere ed adottare i relativi atti in tempi sufficientemente brevi. La strutturazione di appositi sottogruppi, secondo quanto previsto dal regolamento interno, ha anche consentito di poter contare su prime bozze di elevato livello qualitativo.

L'attività del Wppj, seppur con le limitazioni richiamate, consente alle autorità di protezione dei dati di esprimersi anche in mancanza di un quadro legale definito a livello

europeo e di esplorare, con sempre maggior successo, le possibilità di sviluppare azioni (reazioni) congiunte con il Gruppo art. 29 sui temi che presentano una duplice valenza.

Il Wppj sempre per facilitare l'adempimento dei compiti attribuitigli dalle *Spring Conference* di Cipro ha adottato un programma di lavoro per il 2008 anche introducendo nuovi argomenti, quali ad esempio gli approfondimenti sugli accordi bilaterali tra gli Stati europei in materia di cooperazione giudiziaria e di polizia in materia penale (lotta al terrorismo, alla criminalità, allo sfruttamento dell'immigrazione illegale o alla pedo-pornografia) che prevedano forme di trasmissione di dati personali; le disposizioni nazionali di attuazione della Convenzione del Consiglio d'Europa sul *cybercrime* che possono avere un importante impatto nell'applicazione dei princìpi introdotti dalla decisione quadro sulla protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale (*v. supra, par.* 20).

Nella *Spring Conference* di Roma, il Wppj ha presentato una prima informale sintesi dell'attività svolta e la bozza di regolamento interno, che è stata formalmente approvata. Nella stessa occasione il Wppj ha presentato la dichiarazione poi adottata dalla stessa Conferenza relativa alla proposta sulla strategia europea di sorveglianza generalizzata dei viaggiatori (*v. Relazione* 2007, *p.* 161).

Altri temi trattati:

- la conservazione ed utilizzo a fini di polizia dei dati *Api* e *Pnr* raccolti da vettori aerei per fornire servizi commerciali. Dopo l'adozione di un parere congiunto con il Gruppo art. 29 (WP 145), trasmesso alla Commissione ed al Consiglio Ue, il Wppj si è riservato di intervenire nuovamente sul punto. Si è riferito nella *Relazione* 2007 (*p.* 169) delle posizioni critiche assunte dal Gruppo sull'argomento, che resta prioritario nell'agenda europea.

  Su richiesta italiana è inoltre stato sollevato il problema della compatibilità con la Direttiva 2004/82/Ce, ed in generale con gli obblighi derivanti dal diritto comunitario, delle richieste – formulate a pena di sanzione – ai vettori aerei di fornire dati *Api* (e *Pnr*) relativi a passeggeri di voli intracomunitari;
- il potenziamento della cooperazione transfrontaliera, con particolare riguardo al

contrasto del terrorismo e della criminalità transnazionale ("*progetto di decisione del Consiglio sul Trattato di Prüm*"). Come si è detto (*v. supra, par.* 20.2) sono state pubblicate nella *Gazzetta Ufficiale* della Unione europea il 6 agosto 2008 sia la decisione che reca disposizioni in materia di scambio di informazioni fra autorità giudiziarie e di polizia (*cd. "Trattato di Prüm"*), sia l'atto che ne fa applicazione (atti n. 615 e 616); le relative disposizioni dovranno essere applicate dagli Stati a partire dal luglio 2009. La discussione per la ratifica e l'entrata in vigore del Trattato di Prüm è in corso presso il Parlamento.

- il *cd. "Pacchetto Frattini"*, di cui si è riferito nella *Relazione* 2007 (*v. p.* 170).

Sulla base dei risultati del questionario interno si è deciso di continuare a lavorare ad uno strumento comune per lo svolgimento di *audit* ed ispezioni nel settore, sottoposto per la definitiva approvazione alla *Spring Conference* del 2009, tenutasi ad Edimburgo, (23-24 aprile).

Il Wppj ha avviato, inoltre, sulla base di questionari predisposti dall'autorità italiana, un'attività di approfondimento e verifica dell'impatto a livello nazionale della ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica ed un inventario degli accordi bilaterali (o multilaterali) stipulati in materia di *law enforcement* dai singoli Stati nazionali.

Il Wppj ha definito ed approvato il primo rapporto annuale di attività, presentato per la definitiva adozione alla *Spring Conference* di Edimburgo.

Nell'occasione la relazione del presidente si è soffermata anche sul seguito del programma di lavoro per il 2008/2009 (con particolare riguardo all'impatto del Trattato di Lisbona sulla materia attinente al *"terzo pilastro"* ed all'attività delle autorità di protezione dati, all'entrata in vigore del nuovo quadro di princìpi relativi al trattamento dei dati nella cooperazione di polizia e giustizia ed all'impatto sugli accordi bi e multilaterali in vigore tra i Paesi dell'Unione).

La *Spring Conference* ha anche rinnovato il mandato del presidente del Garante italiano quale Presidente del WPPJ.