20. LE RELAZIONI INTERNAZIONALI

Per quanto riguarda l'evoluzione del quadro delle relazioni comunitarie ed internazionali, l'evento principale e più atteso è senz'altro l'entrata in vigore, il 1° dicembre, del Trattato di Lisbona.

Con il Trattato la protezione dei dati personali acquista un nuovo e diverso ruolo. Il Trattato infatti richiama espressamente ed ingloba nel quadro giuridico europeo le disposizioni della Carta dei diritti fondamentali, che, com'è noto, all'art. 8 ha introdotto il diritto fondamentale delle persone alla tutela dei propri dati personali, affiancandolo all'art. 7 che riguarda il diritto alla riservatezza.

Trattandosi di un diritto fondamentale, cambia l'interpretazione degli strumenti giuridici adottati in materia: la Direttiva n. 95/46/CE, che contiene i princìpi armonizzati, esce definitivamente dal contesto in cui è nata - il mercato interno - per assumere pienamente il ruolo di strumento giuridico di riferimento per le istituzioni europee ogni volta che esse intendano legiferare su aspetti che possano avere un impatto sul diritto alla protezione dei dati. Quindi dovranno essere considerate e rispettate le disposizioni della direttiva non solo per i trattamenti di dati personali svolti nell'ambito di attività economiche, ma anche per quelli rientranti nel settore pubblico e finora considerati non coperti dal diritto comunitario.

Questa indicazione è ulteriormente rafforzata dal fatto che l'entrata in vigore del Trattato comporta la fine della divisione in pilastri dell'ordinamento comunitario e prevede che, in materia di trattamento dei dati personali, sia assicurato un quadro di riferimento tendenzialmente unico.

Finora, il quadro armonizzato di princìpi costituito dalla Direttiva n. 95/46/CE e dalla Direttiva n. 2002/58/CE valeva solo nell'ambito del *cd.* "primo pilastro" che, nel garantire la libera circolazione dei dati personali tra i paesi dell'Unione europea, assicurava agli individui un elevato livello di tutela. Nessun principio esiste al momento per quanto riguarda i trattamenti di dati che si svolgono nel *cd.* "secondo pilastro" (politica estera e di sicurezza comune), anche se il Trattato prevede l'adozione di specifiche regole.

Nel *cd.* "terzo pilastro" è stata adottata una decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, che dovrà essere attuata dai paesi dell'Unione entro la fine di novembre 2010.

Tuttavia le sue disposizioni non sono rivolte a disciplinare i trattamenti di dati all'interno dei singoli paesi, ma solo a dettare regole comuni, peraltro ispirate al principio del minimo denominatore. Tali disposizioni sono state fortemente criticate dal Parlamento europeo e dalle autorità nazionali ed europee di protezione dei dati, soprattutto con riferimento al trasferimento di dati da un paese Ue ad un Paese terzo ed al successivo uso dei dati scambiati.

Un ulteriore e favorevole effetto dell'entrata in vigore del Trattato è dato dal maggiore ruolo riconosciuto al Parlamento europeo, che diviene un vero codecisore anche nell'area sopra indicata; ciò che favorisce l'interlocuzione con le autorità di protezione dei dati personali riunite nel Gruppo Art. 29 e nel *Working Party on Police and Justice* (*Wppj*). Sono già evidenti i primi effetti su alcuni accordi internazionali negoziati in settori particolarmente delicati: il Parlamento ha richiesto il parere delle autorità di protezione dei dati ed ha successivamente negato il suo appoggio all'accordo-ponte Ue-Usa per l'uso dei dati *Swift*, negoziato dal Consiglio e dalla Commissione e concluso proprio in concomitanza con l'entrata in vigore del Trattato. Situazioni analoghe si sono verificate per quanto riguarda gli accordi con Stati uniti, Australia e Canada concernenti l'uso dei dati personali dei passeggeri aerei.

Si tratta per lo più di accordi stipulati "a porte chiuse" senza il coinvolgimento del Parlamento europeo, che, almeno in Italia, non sono sottoposti a ratifica parlamentare né a consultazione del Garante. Anche in questo caso il Trattato, tramite il Protocollo sul ruolo dei Parlamenti nazionali, consentirà ad essi una partecipazione più attiva.

In parallelo alle attività legate all'entrata in vigore del Trattato di Lisbona, la Commissione europea ha aperto una stagione di riflessione sull'attualità dei princìpi della Direttiva n. 95/46/CE soprattutto in relazione alle sfide tecnologiche ed alla globalizzazione, lanciando una consultazione pubblica cui le autorità di protezione dei dati hanno voluto contribuire con un importante documento congiunto WP29 e *Wppj* sul futuro

della *privacy* (*v. par.* 20.2.) in cui, pur dando un giudizio di sostanziale tenuta delle regole, si sottolinea l'esigenza di migliorare l'applicazione della direttiva, rendendo effettivi i suoi princìpi e raggiungendo una applicazione realmente armonizzata. Il documento evidenzia tuttavia anche aspetti più critici, che richiedono una riflessione non limitata all'orizzonte europeo, come la disciplina dei flussi internazionali di dati e gli aspetti legati all'uso di nuove tecnologie (*Rfid, Cloud computing*).

In proposito, sia la risoluzione adottata nella Conferenza di primavera svoltasi il 23 e 24 aprile ad Edimburgo sia, in modo più corale ed ambizioso, la predisposizione ed adozione di una serie di princìpi definiti *"standard internazionali"* in materia di *privacy*, testimoniano l'impegno profuso dalle autorità per essere in prima fila nel dibattito, ed il loro ruolo proattivo rispetto all'individuazione di problemi e possibili soluzioni.

Un altro importante contributo fornito alla Commissione, al Parlamento ed al Consiglio dalle autorità europee di protezione dei dati ha riguardato l'adozione del nuovo programma quinquennale di lavoro in materia di polizia e sicurezza, il *cd. "programma di Stoccolma"*, per il quale si rinvia al paragrafo dedicato alla cooperazione nel settore libertà, sicurezza e giustizia.

L'attenzione delle autorità resta comunque ferma, come ben mostrano i pareri adottati dal Gruppo Art. 29 e dal *Wppj*, sul quadro giuridico generale esistente, per valutarne la tenuta e migliorarne l'attuazione ovvero per rendere più effettiva la cooperazione tra le autorità stesse, ad esempio, nello svolgimento di attività comuni di accertamento, come l'azione di *enforcement* del WP29 relativa alla direttiva sulla *data retention*, le altre svolte nell'ambito delle autorità comuni di controllo Schengen, EUROPOL, Dogane ed EURODAC, nonché l'adozione ed attuazione delle azioni indicate nel manuale dal *Wppj*.

Il Garante ha partecipato alle diverse attività menzionate, sia nei gruppi di lavoro sia in cooperazione tra e con le autorità europee e mondiali di protezione dei dati personali come sarà meglio descritto *infra*.

In alcuni casi ha anche svolto, come per il Gruppo di lavoro polizia e giustizia, un ruolo di stimolo e propositivo determinante, testimoniato dalla rielezione del presidente del Garante italiano alla sua direzione.

20.1. LE CONFERENZE DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Spring Conference 2009

Il 23 e 24 Aprile si è tenuta a Edimburgo la Conferenza di primavera delle autorità di protezione dei dati personali, dedicata a *"Come migliorare la protezione dei dati"* attraverso iniziative volte a rafforzare e rendere effettive le garanzie previste dalle norme vigenti. Prendendo spunto da un'analisi della Direttiva n. 95/46/CE e delle diverse ipotesi di revisione, i relatori hanno dibattuto sui punti di forza e debolezza della normativa attuale e sugli approcci sinora adottati per potenziarla. Il mutamento del contesto ha fatto sorgere problemi complessi di ridefinizione del significato della protezione dei dati, del tipo di regole effettivamente necessarie e del ruolo che devono svolgere le autorità per la *privacy* con riferimento alle nuove "sfide" tecnologiche e globali. La sessione presieduta dal presidente dell'Autorità italiana è stata dedicata agli obiettivi che l'attività dei regolatori deve porsi per garantire effettivamente la protezione dei dati a livello individuale e sociale.

Nella Dichiarazione finale i Garanti hanno evidenziato il patrimonio di esperienza e conoscenza che l'Europa può e deve apportare alla ricerca di soluzioni ed approcci sempre più condivisi per garantire la tutela dei dati personali a livello mondiale. La Dichiarazione ha evidenziato la necessità di guardare ai molti punti in comune che già contraddistinguono il quadro normativo europeo e internazionale. Ma soprattutto ha raccomandato ai soggetti coinvolti (pubblici, privati e istituzionali) di mettere a punto norme e *standard* che - a partire dai princìpi di protezione dati già affermati - siano in grado di garantire e promuovere i diritti e le libertà fondamentali; di sviluppare nelle tecnologie approcci che prevedano la *privacy* come elemento essenziale (*privacy by design*); di realizzare una efficace protezione dei dati personali tenendo in considerazione i rischi per i singoli e per la società nel suo complesso.

Nell'ambito della Conferenza ampio è stato il contributo fornito dal Gruppo di lavoro polizia e giustizia. In primo luogo è stato presentato ed approvato il rapporto di attività 2007-2008 del *Working Party on Police and Justice* (*Wppj*), e sono stati illustrati i risultati raggiunti e le iniziative future. Inoltre è stata adottata una risoluzione sugli accordi bilaterali e multilaterali stipulati fra paesi europei e non-europei in materia di cooperazione giudiziaria e di polizia (*cd.* "terzo pilastro").

Considerata l'esistenza di troppe difformità nelle garanzie fissate da tali accordi per quanto riguarda la protezione dei dati, i Garanti hanno chiesto agli Stati di garantire livelli uniformi di tutela anche attraverso l'inserimento di clausole-*standard* concernenti la protezione dei dati personali. La Conferenza ha anche adottato il "manuale" elaborato dal *Wppj* per definire alcuni criteri applicabili alle attività di ispezione e monitoraggio concernenti la materia del "terzo pilastro". La Conferenza ha infine rieletto all'unanimità per un secondo mandato il Presidente, prof. Francesco Pizzetti, dopo aver dato atto dell'importante lavoro svolto.

World Conference delle autorità di protezione dei dati

Dal 4 al 6 novembre 2009 si è svolta a Madrid la *31ma Conferenza internazionale delle autorità di protezione dei dati*, con la partecipazione di 50 Paesi. Fra i temi più rilevanti all'ordine del giorno devono essere ricordati: il contemperamento fra proprietà intellettuale e diritto alla *privacy* su internet; la ricerca del giusto equilibrio tra sicurezza, sorveglianza e libertà; la difesa dei minori riguardo all'uso dei loro dati personali soprattutto nei *social network*; i flussi internazionali di dati nel rispetto delle garanzie per i cittadini.

Il presidente dell'autorità italiana ha presieduto una specifica sessione dedicata alle soluzioni possibili per contemperare proprietà intellettuale, diritti delle imprese e tutela degli utenti.

Durante la Conferenza è stata approvata un'importante risoluzione sugli *standard* internazionali in materia di *privacy*, che contiene un primo pacchetto di regole e princìpi condivisi a livello mondiale.

Attraverso gli *standard* vengono definiti una serie di princìpi, diritti, obblighi e meccanismi procedurali che ciascun ordinamento è chiamato ad assicurare in tema di *privacy* e protezione dei dati, nel settore pubblico e in quello privato.

I princìpi condivisi possono essere così sintetizzati: liceità, correttezza e proporzionalità del trattamento di dati personali; rispetto del principio di finalità; trasparenza dei trattamenti; qualità e sicurezza dei dati; salvaguardia dei diritti di accesso, rettifica, cancellazione e opposizione da parte degli interessati; responsabilità del titolare anche per i trattamenti affidati a soggetti esterni; rafforzamento delle tutele per i dati sensibili; obbligo di assicurare il rispetto di questi *standard* nei trasferimenti internazionali di dati;

garanzia di un controllo indipendente affidato ad autorità autonome ed imparziali provviste di adeguati poteri e risorse; potenziamento di approcci proattivi e preventivi basati sull'impiego di tecnologie, su valutazioni preventive di impatto-*privacy*, su controlli di qualità. Secondo la risoluzione, gli *standard* potranno costituire un'utile base di partenza per promuovere l'ulteriore armonizzazione delle garanzie in materia di *privacy*, soprattutto per quanto riguarda i flussi internazionali di dati. I princìpi generali a tutela della protezione dei dati riaffermati nella risoluzione hanno il pregio di poter essere accettati anche da autorità di Paesi non Ue che hanno una diversa cultura della protezione dei dati, favorendo in tal modo una tutela globale.

Tra le altre significative risoluzioni approvate dalla Conferenza figurano quella sulla tutela della *privacy online* dei minori e quella sulla creazione di un sito *web* della Conferenza internazionale per favorire la circolazione internazionale dei documenti e delle informazioni in materia di protezione dati.

Nel corso della Conferenza è stato attribuito ad Ilita (Autorità israeliana per la tutela dei dati personali) lo *status* di membro della Conferenza ed è stata accettata la candidatura di Israele per l'organizzazione della prossima conferenza mondiale.

Altre conferenze

Il 14 maggio 2009 si è tenuta a Bruxelles una importante conferenza *"Towards the Evaluation of the Data Retention Directive"* in cui si è avuto il primo confronto fra i centoquaranta partecipanti appartenenti a tutti i settori interessati (autorità di *law enforcement*, autorità di protezione dati, settore privato, *ong*) relativamente all'attuazione della Direttiva n. 2006/24/CE e in particolare alla valutazione prevista dall'art. 14 entro il 15 settembre 2010.

Sempre a Bruxelles il 19-20 maggio 2009 si è tenuta una conferenza organizzata dalla Commissione europea, dal titolo: *"Personal Data: More Use, More Protection?"* volta a raccogliere stimoli e suggerimenti ai fini della consultazione pubblica lanciata dalla Commissione sullo stato di attuazione della Direttiva n. 95/46/CE e sull'eventuale opportunità di una sua revisione. La Conferenza intendeva approfondire il tema della protezione dei dati nel mondo globalizzato e alla luce delle nuove tecnologie, con particolare riferimento ai temi dell'accesso ai dati da parte di autorità pubbliche e soggetti privati,

dei flussi di dati transfrontalieri nel *cd. "cloud computing"* e delle aspettative degli individui, del mondo del *business* e della società nel suo complesso rispetto alle tematiche in esame. Il presidente dell'Autorità è intervenuto nella sessione sul diritto all'oblio. Dopo aver rappresentato il quadro normativo, internazionale ed europeo, in cui può essere rintracciato tale diritto, ha mostrato come le nuove tecnologie abbiano contribuito all'emersione di nuove dimensioni dell'oblio, favorendo la dispersione del controllo da parte dell'interessato sulla propria sfera informativa. A tal proposito, il Prof. Pizzetti ha ricordato la tematica dei motori di ricerca e della particolare difficoltà di cancellare i dati personali (anche dalla copia *cache*), facendo riferimento alle decisioni dell'autorità italiana in materia di archivi *online* dei giornali e di pubblicazione delle decisioni di autorità pubbliche. Ha concluso ripercorrendo le sfide rappresentate dalla nuove tecnologie, sottolineando la necessità di sviluppare un nuovo approccio fondato su princìpi armonizzati a livello internazionale.

20.2. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

L'attività del Gruppo Art. 29 si è orientata secondo le tre linee fondamentali individuate nel programma di lavoro adottato per il biennio 2008-2009: miglioramento dell'efficacia delle disposizioni contenute nella Direttiva n. 95/46/CE, studio dell'impatto delle nuove tecnologie e sviluppo di una visione globale (trasferimenti internazionali di dati e impatto della globalizzazione). Rientra nel primo obiettivo il lavoro di interpretazione della Direttiva n. 95/46/CE soprattutto con riferimento alle nozioni di *"data controller"* e di *"data processor"*. L'analisi, approfondita nell'ambito di uno specifico gruppo di lavoro, è sfociata in un testo che, oltre a meglio determinare gli elementi caratterizzanti delle diverse figure, ne specifica le singole peculiarità in vista dell'allocazione della responsabilità, dell'individuazione dei rispettivi ruoli in caso di attività di *outsourcing*, nonché delle ipotesi di contitolarità del trattamento. In tale linea, è stato inoltre approfondito il concetto di *"legge applicabile"* per meglio definire l'ambito di applicazione della normativa europea in materia di protezione dei dati personali, soprattutto in relazione ai trattamenti che assumono carattere transnazionale. L'obiettivo è quello di individuare

i "confini" della normativa in questione, anche al fine di semplificare gli oneri gravanti su operatori aventi sedi dislocate in diversi Stati membri dell'Ue.

Il sottogruppo specificamente dedicato all'attività di *enforcement* ha proseguito nella verifica dell'applicazione della Direttiva n. 2006/24/CE alla conservazione dei dati a fini di lotta alla criminalità. Come anticipato nella *Relazione 2008* (*cfr.* pag. 244), le Autorità degli Stati membri hanno provveduto ad inviare un identico questionario alle società fornitrici di reti e servizi di comunicazioni elettroniche. Alcuni Paesi, compatibilmente con i poteri attribuiti alle singole autorità, hanno poi effettuato anche ispezioni *in situ*, per verificare la correttezza delle informazioni ricevute. All'esito di queste attività ciascuna Autorità ha redatto un *National Report* evidenziando lo stato dell'arte in ciascun Paese e le maggiori criticità. I risultati complessivi saranno sintetizzati in un documento adottato dalla Assemblea Plenaria del WP29 che rivolgerà le raccomandazioni agli operatori del settore e potrà essere tenuto in considerazione dalla Commissione in vista della valutazione prevista dall'art. 14 della Direttiva n. 2006/24/CE entro il 15 settembre 2010.

Altrettanto intenso è stato il lavoro condotto in materia di nuove tecnologie. Particolare attenzione è stata rivolta all'utilizzo dei *social network*, alle attività di trattamento poste in essere dai motori di ricerca (in particolare con riferimento ai tempi e alle modalità di conservazione dei dati), al servizio fornito da *Google Street view*. Il lavoro di approfondimento è stato arricchito da audizioni dei titolari del trattamento e ha condotto all'individuazione di specifiche raccomandazioni in materia. Analoga attenzione hanno suscitato le tematiche legate alle attività del *cd. "marketing comportamentale"*, soprattutto in considerazione del massiccio uso, in questo settore, di attività di profilazione degli utenti.

Con riferimento ai trasferimenti internazionali di dati il Gruppo, su richiesta della Commissione europea, si è espresso positivamente sull'adeguatezza delle legislazioni di Andorra ed Israele in materia di protezione dei dati. Intensa, inoltre, è stata la riflessione in materia di *binding corporate rules*, che ha prodotto buoni risultati in termini di accelerazione dei tempi di definizione della procedura europea di cooperazione tra autorità. Analoga attenzione è stata rivolta al settore delle *Standard contractual clauses*, mediante un

parere, espressamente richiesto dalla Commissione europea, sullo schema di proposta volto alla definizione di un nuovo set di clausole da titolare a responsabile.

Il Gruppo ha, inoltre, affrontato le tematiche delle centrali rischi pubbliche e private (con particolare riferimento alle attività di trattamento poste in essere da società di informazione creditizia) ed ha dato mandato al sottogruppo *Financial Matters* di approfondire l'impatto sulla protezione dei dati personali e sulla *privacy* delle disposizioni delle direttive europee adottate in materia di anti riciclaggio e prevenzione dell'uso del denaro per finanziare il terrorismo. Il sottogruppo ha inoltre contribuito a predisporre il parere, adottato dal WP29 congiuntamente al *Wppj*, inviato al Parlamento europeo in relazione allo schema di accordo ponte Eu-Usa sull'uso dei dati di messaggistica finanziaria (*Swift*), accordo successivamente rifiutato dal Parlamento.

Continua e costante attenzione è stata anche mantenuta, attraverso in particolare i lavori del sottogruppo *Traveller Data*, riguardo al trattamento dei dati dei passeggeri aerei in relazione ad accordi sull'uso di tali dati da parte di Paesi terzi (Australia, Canada, Stati Uniti) e ai problemi derivanti dall'introduzione del programma *e-Borders* nel Regno Unito, con le richieste di fornire in anticipo dati dei passeggeri colà diretti anche in relazione a voli intracomunitari ovvero a trasporti terrestri e marittimi (*Eurotunnel*).

Il Gruppo, sempre basandosi sui lavori del sottogruppo, ha fornito le sue osservazioni in merito all'introduzione dei *body scanner* negli aeroporti ed ha anche adottato un parere sul trattamento dei dati nell'ambito dei *duty free shop* presenti negli aeroporti.

Infine, il Gruppo ha partecipato, insieme al Gruppo polizia e giustizia, all'importante consultazione pubblica lanciata dalla Commissione europea in materia di *"Future of privacy"*, attraverso la definizione di un documento che, nel ribadire la validità dell'impianto normativo di base assicurato dalla direttiva del 1995, auspica l'introduzione di innovazioni in grado di potenziare e rendere più effettiva la tutela del diritto alla protezione dei dati personali.

Parere 5/2009 sui *social network online*

Con il parere in argomento il Gruppo Art. 29 ha chiarito che il mondo dei *social network* (*Sn*) non è sottratto alle tutele che la Direttiva n. 95/46/CE prevede rispetto al trattamento di dati personali. Gestori e utenti di questi servizi hanno specifiche

responsabilità, che il parere individua fornendo indicazioni in ordine alla legge applicabile, alla titolarità del trattamento e alle informazioni che devono essere date agli interessati.

Il Gruppo ha affermato, in particolare, che i gestori di tali piattaforme, anche di quelle gestite da Paesi extra-Ue, sono soggetti alle disposizioni della direttiva (e, quindi, delle leggi nazionali in materia), nella misura in cui il funzionamento dei *Sn* richieda l'utilizzo di "strumenti" situati fisicamente sul territorio dell'Ue (compresi i *cookie* che i *Sn* utilizzano per gestire la navigazione da parte degli utenti).

Si ricorda, inoltre, che il modello commerciale prevalente per i *social network* si basa sulla pubblicità presentata agli utenti, in maniera mirata, in base alle informazioni contenute nei profili-utente. Tutto ciò comporta numerosi trattamenti di dati personali e la necessità di una efficace tutela.

Particolare attenzione è stata dedicata all'individuazione del titolare del trattamento, che può identificarsi con il fornitore del servizio di *social network* e congiuntamente, a determinate condizioni, con l'utente che fruisce del servizio medesimo. Gli uni e gli altri hanno dunque specifiche e diverse responsabilità; per quanto riguarda i gestori, il documento ricorda gli obblighi di informativa agli utenti (i quali devono essere edotti sui rischi legati alla circolazione, talora inconsapevole, delle informazioni collocate nel proprio profilo), di conservazione limitata dei dati utilizzati per scopi amministrativi (*ad es.*, per aprire o chiudere un *account*), di messa a disposizione di strumenti efficaci per l'esercizio dei diritti degli utenti (accesso, rettifica), diritti che devono essere riconosciuti anche ai terzi i cui dati finiscano in un profilo *Sn*.

Fra le specifiche responsabilità degli utenti, prima fra tutte vi è quella di chiedere il consenso delle persone i cui dati siano fatti circolare, soprattutto se il numero di contatti e "amici" è particolarmente elevato e le informazioni non circolano all'interno di un gruppo chiuso. Sono indicati anche alcuni nodi problematici, come quello della verifica del consenso espresso dai minori, che costituiscono una fetta consistente degli utenti di questi servizi; sul punto il documento individua una possibile strategia basata su più strumenti (educazione, sensibilizzazione, soluzioni tecnologiche, autoregolamentazione), pur non nascondendo la difficoltà di trovare una risposta univocamente efficace.

Contributo alla consultazione pubblica del *DG MARKET* sul *report* dell'*Expert Group* in materia di *Credit Histories* (WP 164)

La Commissione aveva dato mandato ad un gruppo di esperti di approfondire, attraverso la predisposizione di un *report* poi sottoposto a consultazione pubblica, alcune tematiche in materia di circolazione e diffusione a livello europeo dei profili di credito che trovano largo impiego in particolare nell'ambito del credito al consumo.

Nel partecipare alla consultazione, il gruppo ha rilevato che il *report* non teneva nel debito conto i diritti degli interessati e, più in generale, non rifletteva in misura sufficiente gli obblighi derivanti dalla Direttiva n. 95/46/CE; il fatto che non in tutti Paesi dell'Ue esistano norme settoriali specifiche o codici di condotta che disciplinino la materia alla luce dei princìpi di protezione dati impone alla Commissione europea una particolare attenzione al fine di assicurare un approccio armonizzato e rispettoso dei diritti degli interessati. Le maggiori criticità, a giudizio del gruppo, riguardano la necessità di assicurare il diritto ad una informazione completa e precisa sulle finalità di utilizzo dei dati contenuti nei profili di credito, nonché il diritto d'accesso e di rettifica che dovrà essere esercitato gratuitamente soprattutto in considerazione della disponibilità di forme di accesso *online*. Nel *report* manca, inoltre, un'indicazione univoca sui dati che possono essere oggetto di trattamento per le finalità sottese alla creazione di questi profili; è chiaro che si tratta di un elemento essenziale per garantire un uso proporzionato e responsabile delle informazioni raccolte in base ai princìpi di proporzionalità e finalità, anche se sul punto emergono numerose divergenze fra le prassi e le norme nazionali. Anche la portata delle decisioni automatizzate dovrà essere ristretta, guardando al principio affermato nell'art. della Direttiva n. 95/46/CE, in particolare per quanto riguarda le conseguenze derivanti dall'attribuzione dei "punteggi" (*credit score*).

Adeguatezza del livello di protezione dei dati in Israele e Andorra (WP 165 e WP 166)

Su richiesta della Commissione europea, il Gruppo Art. 29 ha valutato il livello di protezione dei dati esistente in Israele e nel Principato di Andorra, giungendo in entrambi i casi ad un giudizio di adeguatezza, ai sensi dell'art. 25(6) della direttiva. Nei due Paesi esiste infatti un quadro di garanzie che, pur se operanti in modo diverso, nel complesso consentono il trasferimento di dati personali dall'Ue. In Israele, in particolare, vige un regime "misto" di *common law* e di tradizione continentale, per cui accanto ad una legge nazionale in materia (*Privacy Protection Act* del 1981) esistono *"Basic Laws"* che

sanciscono alcuni princìpi fondamentali (quali il principio di "proporzionalità" nell'attività di ogni soggetto pubblico o privato) oltre a precedenti giurisprudenziali che hanno fissato e ampliato questi princìpi anche con riguardo alla protezione dei dati. In Andorra vige invece un sistema di diritto continentale, con una legge del 2003 in materia di protezione dei dati personali che soddisfa sostanzialmente tutti i requisiti fissati nella direttiva, anche se con alcune eccezioni (compensate, peraltro, da altre normative settoriali). In entrambi i Paesi esistono autorità indipendenti incaricate di assicurare il rispetto della normativa, e il dibattito in corso (anche a livello parlamentare) sembra andare nella direzione di un ulteriore potenziamento della capacità di controllo e monitoraggio di tali autorità.

Parere 8/2009 sui dati dei passeggeri raccolti e trattati dai negozi *duty free* negli aeroporti e nei porti (WP 167)

Il Gruppo Art. 29 si è pronunciato con un parere sulle modalità di raccolta e utilizzo dei dati all'interno dei *cd.* "negozi *duty free*". Tali modalità sono risultate differenti tra gli Stati membri, e le direttive di riferimento relative al regime generale delle accise (92/12/CEE e successiva 2008/118/CE) non contengono alcun riferimento alla protezione dei dati personali nell'esercizio delle attività di *duty free.*

Al fine di avere una maggiore uniformità nella raccolta e nel trattamento dei dati, il Gruppo ha richiamato i negozi *duty free* negli aeroporti e nei porti ad applicare i princìpi della Direttiva n. 95/46/CE. Fermo restando l'attività di raccolta e conservazione dei dati riguardanti il regime di sospensione delle accise delle autorità doganali, regolate dalla Direttiva n. 2008/118/CE, il Gruppo ha ribadito, tra l'altro, che i passeggeri devono essere adeguatamente informati sulla raccolta, conservazione dei dati e finalità del trattamento e che tale raccolta deve essere limitata alla verifica del diritto all'esenzione delle imposte all'acquisto – e in nessun caso può essere utilizzata a fini di polizia.

Nel parere il Gruppo ha inoltre precisato che non deve essere possibile la raccolta e l'analisi dei dati al fine di identificare i comportamenti d'acquisto e che il periodo di conservazione dei dati deve essere uniforme per tutti gli Stati membri e limitato alla finalità di esenzione dell'accisa.

Contributo alla consultazione pubblica sul futuro della protezione dati (WP 168)

Il Gruppo Art. 29 ed il *Working Party on Police and Justice* hanno messo a punto congiuntamente un documento per rispondere alla consultazione pubblica aperta dalla Commissione europea nel luglio 2009 sul futuro della protezione dei dati come diritto

fondamentale. Il punto di vista delle autorità europee per la protezione dei dati è che l'impianto normativo di base assicurato dalla direttiva del 1995 sia ancora valido. E' tuttavia auspicabile che il legislatore europeo introduca alcune innovazioni e modifiche per rendere ancora più effettivo il diritto fondamentale alla protezione dei dati, ormai parte integrante del Trattato di Lisbona. In questa cornice dovrebbero essere ripensati alcuni concetti-chiave, come il consenso (che deve essere realmente libero ed informato), e dovrebbe essere sviluppato un quadro normativo unico che abbracci tutti gli ambiti nei quali si effettuano trattamenti di dati personali, compresi i trattamenti per finalità giudiziarie o di polizia.

Nel documento si chiede agli Stati nazionali di garantire che il diritto alla protezione dei dati sia rispettato anche quando il dato è trattato fuori dall'Unione europea, favorendo quindi la definizione di *standard* internazionali in materia, sul modello di quelli recentemente adottati dalla Conferenza internazionale di Madrid. Allo stesso tempo si chiede alla Commissione di fare chiarezza sugli *standard* di "adeguatezza" dei Paesi terzi ove si intendono trasferire i dati e di promuovere strumenti quali le "norme vincolanti d'impresa" con il supporto delle autorità nazionali di protezione dati.

Significativo è il richiamo alla necessità di garantire che i diritti di cui godono gli interessati siano esercitabili in modo semplice ed efficace: l'introduzione di *"class action"* (azioni collettive), un accesso più facile a rimedi di natura giudiziaria, sistemi alternativi per la risoluzione delle controversie, sono alcune delle proposte avanzate dalle autorità europee.

Viene proposta anche l'introduzione di un obbligo giuridico per i titolari di dimostrare di avere adottato tutte le misure previste dalla legge, trasformando la protezione dei dati in un elemento intrinseco e portante dell'organizzazione interna, sia in ambito pubblico che privato.

Largo spazio viene dedicato nel documento alle attività di cooperazione fra le autorità di protezione dati, con particolare riguardo alle "sfide" che attendono la protezione dati nell'area del cosiddetto "terzo pilastro". In questi ultimi anni, la cooperazione in materia giudiziaria e di polizia ha visto un forte potenziamento degli strumenti giuridici e tecnici finalizzati a consentire scambi di dati sempre più pervasivi ed estesi, senza che

a ciò si accompagnasse un ripensamento ed un'armonizzazione degli strumenti e delle norme a tutela della sfera privata dei cittadini. Su questo punto i garanti europei hanno chiesto ai legislatori europei e nazionali di invertire la tendenza, sviluppando un quadro giuridico armonizzato ed unificato, come previsto del resto anche nel *"programma di Stoccolma"* presentato dal Consiglio europeo dello scorso dicembre, in modo da muoversi nell'ottica del Trattato di Lisbona.

Altri documenti adottati dal Gruppo Art. 29

Si è riferito nella *Relazione 2008* (p. 139) dell'audizione dei principali gestori di motori di ricerca, da parte del WP29, sulle problematiche sorte a seguito del parere 4 aprile 2008 (WP 148) in materia di protezione dati, in relazione alle attività dei motori stessi (*cfr. Relazione 2007*, p. 164). Nel mese di ottobre il WP29 ha inviato a ciascun gestore le proprie osservazioni tramite lettere *ad hoc*. Le risposte, che daranno conto anche dell'adempimento alle indicazioni fornite dal WP29, saranno rese pubbliche.

Consultazione pubblica sull'impiego dei *body scanner* negli aeroporti - risposta del Gruppo Art. 29

Il WP29 nel mese di febbraio ha risposto alla consultazione pubblica lanciata dalla Commissione in materia di impiego dei *body scanner* negli aeroporti (*v.* Risoluzione del Parlamento europeo del 23 ottobre 2008 sull'impatto delle misure di sicurezza aerea e dell'impiego di *body scanner* sui diritti umani, la vita privata, la dignità personale e la protezione dei dati).

I Garanti europei, che su tale tema hanno lavorato in stretta collaborazione con l'EDPS (*European data protection supervisor*) hanno evidenziato una posizione fortemente critica rispetto all'impiego dei *body scanner*, soprattutto in relazione al principio di necessità, non essendo chiaro perché tali tecnologie dovrebbero garantire maggiormente la sicurezza rispetto all'utilizzo dei sistemi esistenti (perquisizioni manuali, *metal detector*).

Il Gruppo ha fatto presente che deve essere fatto un bilanciamento tra la necessità ed efficacia di tali sistemi e il loro impatto sulla *privacy* dei passeggeri. La Commissione, pur ribadendo il proprio interesse all'utilizzo di tale tecnologia, ha preso nota di tali posizioni critiche, espresse peraltro anche dal Parlamento europeo. La nuova proposta di regolamento sull'aviazione civile eviterà ogni riferimento all'utilizzo di tale strumento, e conterrà una disposizione che individui in maniera dettagliata le tipologie e le modalità di controllo dei passeggeri consentite.

Attualmente è stata costituita, presso la Commissione europea, una *Task force* sull'utilizzo dei *body scanner* (a cui partecipano anche il Gruppo Art. 29 e l'EDPS) al fine di definire un rapporto che determini una posizione comune in tutti gli Stati membri; l'Unione europea ha infatti rinviato l'adozione delle misure attinenti all'utilizzo dei *body scanner* in tutti gli aeroporti dell'Unione, in attesa di maggiori dettagli sugli aspetti legati all'efficacia, ai rischi per la salute e alla compatibilità con le libertà individuali.

Va ricordato che in Italia a metà febbraio è stato dato il via libera alla sperimentazione dei *body scanner* in alcuni aeroporti (Malpensa, Fiumicino, Venezia). In particolare, nei voli diretti in Usa saranno sperimentati due tipi di *body scanner*: quello a onde millimetriche e quello a raggi infrarossi.

Trattamento dei dati dei passeggeri

Sono continuate con impegno le attività relative al tema del trattamento dei dati dei passeggeri aerei, anche attraverso l'azione del sottogruppo *Traveller Data*. Alcune di queste attività sono state già ricordate come, ad esempio, il parere adottato in materia di trattamento dei dati nei *duty free shop* ed il contributo in merito all'introduzione di *body scanner* negli aeroporti.

Pnr Usa: nel corso della visita alla sede di *Amadeus*, l'unico dei quattro sistemi di prenotazione e gestione dei voli operanti a livello mondiale situato in territorio europeo, sono emersi alcuni aspetti che rendono necessario ed urgente verificare come gli Usa adempiono agli impegni assunti nell'Accordo stipulato nel 2007.

Sono quindi continuate le pressioni per l'attuazione della visita negli Usa per la revisione congiunta dell'applicazione degli Accordi, che si è finalmente svolta nel mese di febbraio 2010.

Alla revisione congiunta ha partecipato un rappresentante del WP29. Il sottogruppo *Traveller Data* ha contribuito alla predisposizione delle domande da sottoporre alla delegazione Usa. Nel frattempo il Gruppo ha espresso al Parlamento europeo, in risposta ad una richiesta del presidente della Commissione Libertà pubbliche, i dubbi e le perplessità maturate sui termini dell'Accordo, anche in vista di un suo rinnovo.

Analoghe lettere sono state inviate per quanto concerne gli Accordi per la trasmissione dei dati *Pnr* ad Australia e Canada, quest'ultimo peraltro scaduto.

Ciò deriva dall'esigenza, una volta entrato in vigore il Trattato di Lisbona, di sottoporre gli Accordi in vigore al Parlamento europeo; al riguardo la Commissione LIBE ha richiesto di conoscere il parere dei Garanti europei in relazione alla corrispondenza delle previsioni ivi contenute con i princìpi vigenti in materia di protezione dei dati personali e *privacy*.

Pnr europeo: i lavori sono stati congelati, anche se nel *"programma di Stoccolma"* viene riaffermata la volontà di pervenire all'adozione di un *Pnr* europeo, che peraltro potrebbe non essere limitato all'obbligo dei vettori aerei che operano voli verso il territorio europeo di trasmettere in anticipo i dati di cui man mano dispongono sulle intenzioni di viaggio, bensì anche comprendere voli intraeuropei e nazionali ed anche altri mezzi di trasporto terrestri e marittimi, in qualche modo seguendo il modello *e-Borders* introdotto dal Regno Unito anche come controllo integrato delle frontiere. Analoga sorte per la possibile introduzione di un sistema di autorizzazione preventiva al viaggio, sulla falsariga del sistema Esta introdotto dagli Stati Uniti.

Eborders: l'introduzione del sistema da parte delle autorità britanniche ha determinato l'obbligo per le compagnie aeree e per altri vettori marittimi e terrestri di trasmettere in anticipo rispetto all'effettuazione del viaggio i dati personali dei passeggeri, inizialmente limitati ai dati registrati al momento delle operazioni di imbarco (*cd. "Api"*).

Tutte le compagnie, incluse quelle operanti voli diretti nel Regno Unito dagli altri Paesi dell'Unione, sono state richieste a pena di sanzione di "partecipare al programma". Ciò ha avuto immediate ripercussioni con richieste inviate al Garante ed alle omologhe autorità garanti europee di conoscere se questo avrebbe o meno violato le disposizioni nazionali in materia di protezione dei dati personali.

Il Garante e molte altre autorità, alla luce del diritto nazionale e delle disposizioni adottate in attuazione della Direttiva n. 95/46/CE, hanno valutato non esistere una idonea base giuridica ed hanno chiesto alla Commissione europea di studiare gli aspetti della questione, inclusa la possibile violazione del principio di libera circolazione affermato dal Trattato dell'Unione, in modo da trovare una soluzione comune. Finora la questione non è stata risolta.