del soggetto che materialmente pone in essere le operazioni di trattamento su istruzione del titolare o del responsabile, ove nominato. L'approccio utilizzato è di carattere funzionale, ovvero orientato ad un'analisi dei diversi ruoli soggettivi che intervengono nell'attività di trattamento con maggiore o minore responsabilità a seconda del grado di influenza di questi sulle decisioni inerenti le attività di trattamento medesime. È stata innanzitutto approfondita la figura del "titolare" con riguardo a profili diversi, quali la componente soggettiva; la possibilità di una responsabilità plurima, nonché le differenze con le altre figure che intervengono nel trattamento. Con riguardo alla figura del "responsabile", sono stati evidenziati gli aspetti legati alla "nomina" da parte del titolare, soprattutto con riferimento alle ipotesi, in crescente aumento, di deleghe "multilivello o estese" proprie delle strutture organizzative complesse. In questo contesto, il documento ha affrontato i diversi scenari in cui si prevede l'intervento di titolari e responsabili del trattamento, da soli o congiuntamente con altri, con vari gradi d'autonomia e di responsabilità, sottolineando l'esigenza di attribuire le responsabilità in modo da garantire un'adeguata osservanza delle norme in materia di protezione dei dati.

Parere 8/2010 sul diritto applicabile (WP 179)

Il testo, nell'illustrare i principali problemi applicativi connessi all'art. 4 della Direttiva n. 95/46/CE, ha individuato alcune possibili soluzioni anche pratiche dei casi più complessi di conflitti tra leggi astrattamente applicabili. Sono stati quindi analizzati i diversi criteri di collegamento della direttiva. In particolare è stata chiarita la portata effettiva del principio di stabilimento, nonché l'interpretazione da fornire al "grado di coinvolgimento" dello stabilimento situato nel territorio di uno Stato membro rispetto all'attività di trattamento posta in essere dal titolare ed al concetto di "strumenti situati sul territorio di uno Stato membro". Infine sono state proposte alcune possibili soluzioni, sia con riferimento al caso in cui il titolare disponga di stabilimenti situati in diversi Stati membri dell'Unione europea (suggerendo l'utilizzo del criterio dello stabilimento "principale" del titolare del trattamento, accompagnato dall'auspicata armonizzazione delle legislazioni nazionali di protezione dei dati), sia nell'ipotesi di titolare stabilito in un Paese terzo. In quest'ultimo

caso, è stato proposto di ricorrere innanzitutto al criterio del *cd.* "*targeting*", che consiste nell'individuazione dell'ambito dei destinatari potenziali per le attività di trattamento poste in essere dal titolare (ad es., servizi forniti solo a soggetti residenti nell'UE; informazioni fornite solo nelle lingue dell'UE) e, in via residuale, al criterio di collegamento rappresentato dagli "strumenti situati nel territorio dello Stato" (*cd.* "*means*"), già previsto dal vigente testo della direttiva;

b. Accountability

Parere 3/2010 sul principio di responsabilità (WP 173)

Il parere è principalmente volto a contribuire al processo di revisione della Direttiva n. 95/46/CE, rafforzando il ruolo del titolare del trattamento, anche mediante una sua maggiore responsabilizzazione, nel garantire il rispetto delle regole di protezione dei dati. Il nuovo approccio si propone di creare specifiche responsabilità in capo al titolare in ordine all'attuazione della normativa in materia di *privacy*, differenziando gli obblighi di diligenza (e conseguentemente gli adempimenti) in base al rischio effettivo del trattamento. Più nello specifico, il parere si sofferma sui due elementi fondamentali di cui il principio di *accountability* dovrebbe comporsi:

- il rispetto da parte di tutti i titolari del trattamento di uno *standard* minimo di protezione dei dati (in particolare, attraverso l'attuazione di "*privacy policy*" interne, l'istituzione di "*privacy officers*" e di sistemi di formazione del personale dipendente) e di meccanismi di verifica della loro efficacia (*audit* interni ed esterni);
- la possibilità, su base volontaria, in capo al titolare, di rispettare *standard* di protezione che vadano oltre i parametri minimi individuati dalla legge (ad es., determinazione di tempistiche più brevi di riscontro alle istanze di accesso degli interessati; adozione di misure di sicurezza più stringenti rispetto ai parametri minimi fissati dalla legge, ecc.).

Un ruolo di fondamentale importanza, infine, dovrebbe essere riconosciuto alle autorità di protezione dei dati personali sia in relazione all'individuazione dei parametri da rispettare (anche nella prospettiva di individuare sistemi di certificazione dell'*accountability*), sia in ordine ai sistemi di controllo e di verifica (con il possibile potenziamento dei relativi poteri sanzionatori);

c. Pubblicità comportamentale e protezione dei dati personali *online*

Parere 2/2010 sulla pubblicità comportamentale *online* (WP 171)

Il Gruppo si è pronunciato sulle garanzie specifiche da applicare al settore della pubblicità comportamentale su Internet. Si tratta, in particolare, di forme di *marketing* che prevedono il tracciamento degli utenti durante la navigazione in rete e la creazione di profili, poi utilizzati per messaggi pubblicitari personalizzati. Nel parere si sottolinea innanzitutto che i fornitori di reti pubblicitarie, ai sensi dell'art. 5, par. 3, della direttiva e-*privacy* (Direttiva n. 2002/58/CE, recentemente modificata dalla Direttiva n. 2009/136/CE), possono collocare marcatori (*cookie*) o dispositivi analoghi nelle apparecchiature terminali degli utenti e raccogliere informazioni tramite tali dispositivi soltanto con il previo consenso informato degli utenti. Oltre a stabilire l'obbligo di introduzione di meccanismi di "*opt in*" preliminare che assicurino l'accettazione, da parte dell'interessato, del monitoraggio del comportamento di navigazione ai fini dell'invio di pubblicità personalizzata, il parere fornisce indicazioni sul generale obbligo di trasparenza in relazione agli scopi ed alle modalità del trattamento, ai diritti degli interessati (tra l'altro, accesso, rettifica e cancellazione dei dati) ed ai corrispondenti obblighi per editori e fornitori di reti pubblicitarie. Il Gruppo, tramite le autorità nazionali, ha poi avviato la consultazione delle parti interessate, in particolar modo fornitori di reti pubblicitarie e fornitori di *browser* sui profili tecnici, con lettere il cui testo è disponibile sul sito *web* del Gruppo Art. 29.

Parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel *marketing* diretto (WP 174)

L'associazione europea di operatori di *marketing FEDMA* ("*Federation of European Direct and Interactive Marketing*") ha predisposto una bozza di codice di condotta, relativa all'utilizzo dei dati personali per le attività di *cd.* "*marketing online*", sottoponendola al Gruppo Art. 29 per una pronuncia ai sensi dell'art. 27 della Direttiva n. 95/46/CE. La messa a punto del testo è stata alquanto complessa, avendo richiesto oltre quattro anni di lavoro, in contraddittorio con il sottogruppo appositamente costituito in seno al Gruppo Art. 29. In considerazione delle modifiche da ultimo apportate da *FEDMA* al codice di condotta, in conformità alle prescrizioni indicate nel parere WP 171 del 2010 sulla pubblicità comportamentale *online*, nonché alla Direttiva n. 2002/58/CE come recentemente modificata, il Gruppo

Art. 29 ha espresso, il 13 luglio 2010, parere favorevole sulla compatibilità del codice di condotta europeo con i princìpi e le norme in materia di protezione dei dati personali;

d. Decisioni di adeguatezza di Paesi terzi

Parere 6/2010 sul livello di protezione dei dati personali nella Repubblica orientale dell'Uruguay (WP 177)

Su richiesta della Commissione europea, il Gruppo Art. 29 ha valutato il livello di protezione dei dati esistente in Uruguay, giungendo ad un giudizio di adeguatezza ai sensi dell'art. 25, comma 6, della Direttiva n. 95/46/CE che consente il trasferimento di dati personali dall'Unione europea. In particolare, è stato rilevato un impianto normativo che si ispira a quello introdotto dalla direttiva, con particolare riferimento all'ambito di applicazione (la legge in materia di protezione dei dati si applica sia al settore pubblico sia a quello privato), alle modalità del trattamento ed ai requisiti di qualità dei dati;

e. Clausole contrattuali *standard*

FAQ sulle clausole contrattuali *standard* (WP 176)

In materia di "*standard contractual clauses*" sono state adottate alcune "*frequently asked questions*" (*FAQ*) dedicate all'attuazione della Decisione 2010/87 della Commissione ed in particolare al nuovo *set* di clausole "*controller to processor*". Il testo, con lo scopo primario di garantire maggiore armonizzazione nel recepimento della decisione da parte delle autorità nazionali ed un'applicazione uniforme delle clausole da parte dei titolari del trattamento, si propone di chiarire alcune specifiche problematiche, soprattutto con riferimento ai trasferimenti di dati da *controller* a *processor* stabilito nell'Unione europea, con *subprocessor* stabilito in un Paese terzo. Sono state inoltre esaminate alcune criticità interpretative, in particolare in materia di designazione del *subresponsabile*, di utilizzo di un unico contratto da parte di un responsabile che affidi il trattamento al medesimo *subresponsabile* per conto di differenti titolari, di adozione delle clausole a prescindere dalla effettiva designazione di *subresponsabili*, dell'obbligo di deposito/notifica delle clausole contrattuali tipo alle autorità di protezione dati.

f. Trasferimenti di dati UE-Stati Uniti a fini di cooperazione giudiziaria e di polizia, per il contrasto del terrorismo e di reati gravi

Accordo quadro UE-USA in materia di protezione dati: lettera del Gruppo Art. 29

Con riferimento al *cd.* "accordo quadro" ("*umbrella agreement*") tra Unione europea e Stati Uniti sulla protezione dei dati personali, il Gruppo Art. 29 il 19 novembre 2010, con un parere in forma di lettera ha precisato che l'accordo dovrebbe rappresentare una cornice comune di requisiti per la protezione dei dati personali, per tutti i trattamenti diretti al contrasto delle attività criminali (inclusi i trattamenti aventi ad oggetto dati provenienti da soggetti privati). Il Gruppo, inoltre, ha criticato la clausola dell'accordo che pone l'eccezione relativa ai trattamenti di dati per scopi di "sicurezza nazionale" (trattamenti per i quali viene così esclusa l'applicabilità dalle regole generali previste dall'accordo quadro), auspicandone una riformulazione che eviti la possibilità di interpretazioni estensive. Per quanto concerne il rapporto dell'accordo quadro con quelli già in vigore tra Stati Uniti e Unione europea e Stati membri ("accordi settoriali"), il Gruppo ha proposto l'applicazione retroattiva dall'accordo quadro agli accordi esistenti unitamente, in certi casi, ad un regime transitorio della durata massima di 3 anni. Sono stati inoltre rilevati altri punti critici quali: il rispetto dei diritti contemplati dalla Direttiva n. 95/46/CE, dalla Decisione-quadro 2008/977/GAI e dalle relative disposizioni nazionali di recepimento; la previsione di una clausola ostativa al trasferimento dei dati personali nei casi in cui sia prevista l'applicazione della pena di morte; l'effettiva garanzia dei diritti degli interessati (accesso, rettifica, cancellazione), tenendo conto del ruolo e delle funzioni delle autorità di protezione dati nazionali; il diritto degli interessati a ricorrere in via amministrativa e giurisdizionale avverso le decisioni relative al trattamento che li riguardino; il divieto di trasferimenti di tipo "massivo"; le condizioni e i limiti per il trasferimento ulteriore dei dati; i tempi di conservazione dei dati, adeguati e proporzionali alle finalità pubbliche perseguite; la durata limitata nel tempo dell'accordo e le possibilità di proroga, controllo e revisione congiunta dello stesso, da effettuarsi previo esame da parte della delegazione comune ("*joint review team*"), nella quale siano rappresentate le autorità di protezione dati nazionali.

Accordo sul trasferimento di dati finanziari: lettere del Gruppo Art. 29

Per quanto concerne i trasferimenti transatlantici di dati finanziari, si segnala l'intensa attività svolta dal Gruppo Art. 29, e dal sottogruppo "*Financial Matters*", in merito all'accordo tra Unione europea e Stati Uniti sulla trasmissione dei dati di messaggistica

finanziaria. Per rendere più effettiva la protezione dei dati personali nell'ambito dell'accordo, il Gruppo Art. 29, congiuntamente al Gruppo di lavoro polizia e giustizia (*WPPJ*), ha adottato il parere in forma di lettera del 27 gennaio 2010, sull'accordo "ponte" ("*Interim Agreement*"), e il parere del 25 giugno 2010, sempre in forma di lettera, sulla bozza dell'accordo "*TFTP2*". Con quest'ultima lettera, in special modo, è stata sottolineata l'importanza che l'accordo non limiti i poteri di intervento delle autorità nazionali per la protezione dati e garantisca l'effettività dei diritti degli interessati. Sempre con riferimento all'accordo tra UE e Stati Uniti per la trasmissione ed il trattamento di dati finanziari *TFTP* (*Swift*), in data 5 agosto 2010 il Gruppo ha inviato al Commissario responsabile per gli Affari interni la lettera sulla partecipazione delle autorità di protezione dati alla procedura per la revisione ed il controllo dell'attuazione dell'accordo ("*joint review mechanism*"). Essa indica le autorità del Belgio e dei Paesi Bassi come rappresentanti delle autorità nazionali di protezione dati nella delegazione dell'Unione europea per la revisione dell'accordo ("*European Union review delegation*") ed evidenzia alcune criticità concernenti, in particolare, il ruolo di EUROPOL, di cui non sono chiari i poteri e l'esercizio delle funzioni di controllo al momento dell'approvazione delle richieste di dati da parte del Dipartimento del tesoro degli Stati Uniti. Le autorità dichiarano inoltre di volere esercitare, con la necessaria indipendenza e con pieni poteri, il proprio ruolo di supervisione del rispetto delle garanzie previste dall'accordo *TFTP* in termini di protezione dati. I testi delle lettere sono disponibili sul sito *web* del Gruppo.

g. Dati dei passeggeri aerei e accordi *PNR*

Parere 7/2010 sulla comunicazione della Commissione europea sull'approccio globale ai trasferimenti dei dati *PNR* verso Paesi terzi (WP 178)

Il Gruppo ha espresso la propria posizione in merito alla Comunicazione del 21 settembre 2010 della Commissione europea sull'approccio globale ai trasferimenti dei dati *PNR* verso Paesi terzi (COM(2010) 492). Il Gruppo, pur apprezzando l'iniziativa, volta a definire misure minime di salvaguardia per la protezione dei dati personali, ha manifestato perplessità in merito alla necessità e proporzionalità di tale trattamento per finalità di "*law enforcement*" nel contrasto alle attività di terrorismo. In particolare, si è evidenziato che lo scambio di dati *PNR* deve essere

considerato nel più ampio contesto del trattamento dei dati relativi ai passeggeri, che include, tra l'altro, anche i *cd.* "dati *API*" (*Air Passenger Information*), di cui alla Direttiva n. 2004/82/CE, i quali potrebbero, in alcuni casi, essere di per sé sufficienti a perseguire lo scopo di "*law enforcement*".

h. "*Enforcement*" sulla direttiva *data retention*

Rapporto 1/2010 sull'azione di *enforcement* (WP 172)

Il Gruppo, basandosi sui lavori del sottogruppo "*Enforcement*", di cui il Garante è stato *rapporteur*, ha approvato il 13 luglio 2010 il rapporto sull'azione di "*enforcement*" relativa alla direttiva *cd.* "*data retention*". Il rapporto è il risultato della valutazione, da parte delle autorità per la protezione dei dati personali, delle risposte ai questionari rivolti alle principali società attive nel settore delle comunicazioni elettroniche e degli esiti degli accertamenti condotti "sul posto" dalle autorità di protezione dati. È stata confermata, in particolare, l'esigenza di una migliore definizione del campo di applicazione della direttiva e del periodo di conservazione dei dati; nella specie riduzione del periodo "massimo" e introduzione di un termine "unico". È stata altresì ribadita la necessità di una trasmissione dei dati più sicura e preceduta da un'adeguata valutazione dei rischi specifici, nonché una definizione maggiormente armonizzata sia delle procedure per la comunicazione dei dati alle autorità competenti in materia di *law enforcement*, sia di alcuni concetti essenziali, ancorché ancorati al diritto nazionale, quali la nozione di "*serious crime*".

i. Protezione dati e tecnologie *RFID*

Privacy Impact Assessment RFID (WP 175 e WP 180)

Dopo un primo parere negativo del 13 luglio 2010 (WP 175) sulla prima proposta della *cd.* "*business community*" in materia di "*privacy impact assessment*" per le tecnologie *RFID* (applicazioni basate sull'identificazione a radiofrequenza), il Gruppo Art. 29 ha approvato la "*revised industry proposal*" l'11 febbraio 2011 (WP 180). In sostanza, in base al citato documento, gli operatori *RFID*, prima di utilizzare tali tecnologie, si impegnano a: 1) definire con chiarezza i fattori di rischio; 2) tener conto delle possibilità che le persone continuino a portare etichette *RFID* anche oltre l'area sorvegliata predefinita; 3) rispettare i princìpi per la disattivazione delle etichette *RFID* nel settore del commercio al dettaglio. Il processo di "*privacy impact*

assessment" (*PIA*) prevede, in particolare, una fase di pre-valutazione, per la classificazione delle tecnologie *RFID*, nonché una fase di valutazione dei rischi. Il Gruppo Art. 29 continuerà ad ogni modo i contatti con gli operatori economici interessati, anche al fine di valutare se la metodologia di *PIA* approvata dal Gruppo Art. 29 sia di fatto applicata dai produttori di *RFID*.

l. Protezione dati e tutela dei diritti di proprietà intellettuale

Lettera al Commissario Mr. Karel de Gucht sull'accordo anticontraffazione (*ACTA*)

Il Gruppo ha adottato il 15 luglio 2010 il parere in forma di lettera indirizzato al Commissario della Direzione generale commercio della Commissione europea, responsabile del negoziato dell'accordo *ACTA*, avente come principale obiettivo il contrasto delle violazioni dei diritti di proprietà intellettuale. Nel ricordare che le Parti contraenti hanno confermato, con dichiarazione congiunta del 16 Aprile 2010, l'esclusione dell'utilizzo del principio "*Three Strikes Out Scheme*" (ovvero la disconnessione da Internet dell'utente identificato per tre volte come autore di presunte violazioni del diritto di *copyright*), il Gruppo ha espresso contrarietà all'introduzione della "*Notice-and-Take-Down Procedure*" in base alla quale, nel caso di segnalazioni di violazioni del diritto di *copyright*, i fornitori di servizi *online* possono bloccare l'accesso ai contenuti scaricati dagli utenti, e sono tenuti a comunicare al titolare del diritto d'autore informazioni sull'identità del presunto autore della violazione. Infine, nelle conclusioni, ha sottolineato l'importanza di assicurare la tutela del *copyright* con misure necessarie e proporzionali, garantendo, al contempo, il diritto alla riservatezza delle parti coinvolte.

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

Working Party on Police and Justice (*WPPJ*)

L'attività del *WPPJ* nel 2010 è proseguita sotto la presidenza italiana, secondo il programma di lavoro biennale adottato nel 2009, percorrendo due binari fondamentali. Da un lato, è stata mantenuta l'attenzione agli sviluppi normativi in sede europea con riguardo ai flussi di dati verso gli Stati Uniti ed altri Paesi extraeuropei per finalità giudiziarie e di polizia; dall'altro lato, è proseguita un'attività, concentrata su alcuni temi ritenuti di parti-

colare delicatezza, di monitoraggio degli sviluppi in materia di "terzo pilastro" a livello europeo, con riferimento al quadro normativo introdotto dal Trattato di Lisbona. Nel primo ambito di attività, occorre ricordare il contributo alla Consultazione pubblica della Commissione europea sul progetto di accordo (*cd.* "*accordo quadro*") tra Unione europea e Stati Uniti in materia di protezione dei dati personali e scambio di informazioni per finalità di polizia e giudiziarie, presentato congiuntamente al Gruppo Art. 29, i cui contenuti sono stati successivamente sintetizzati in una Risoluzione adottata dalla Conferenza di primavera delle autorità di protezione dati tenutasi a Praga. Il punto fondamentale è che l'accordo, commendevole in quanto volto a garantire un approccio uniforme, dovrà fissare un quadro di princìpi che troveranno applicazione in ogni futuro strumento convenzionale adottato in materia. L'accordo quadro non costituirà, pertanto, la base giuridica dei trattamenti in oggetto, che dovrà essere individuata di volta in volta nei modi opportuni e con riguardo alle specifiche circostanze. Il documento sottolinea, inoltre, alcune criticità del progetto di accordo: in particolare, le incertezze relative ai meccanismi di ricorso esperibili dai cittadini europei in caso di trattamenti illeciti svolti negli Stati Uniti ed all'esercizio dei diritti di accesso previsti dalla Direttiva n. 95/46/CE e dalle normative nazionali di recepimento. Nella Risoluzione della citata Conferenza di Primavera, le autorità europee di protezione dati hanno sottolineato anche la necessità di garantire un controllo indipendente sull'applicazione dell'accordo e degli strumenti attuativi. Sempre con riguardo ai flussi di dati Unione europea - Stati Uniti, il *WPPJ* ha commentato, congiuntamente con il Gruppo Art. 29, il nuovo testo dell'Accordo *TFTP* (*Terrorist Financial Tracking Program, TFTP2*), condividendone le numerose riserve ed evidenziando le ambiguità dell'articolato. Sul versante intraeuropeo, il *WPPJ* ha contribuito al dibattito sulla possibile revisione del quadro giuridico in materia di protezione dati alla luce del Trattato di Lisbona, in primo luogo in relazione all'incontro organizzato il 14 luglio con la Commissione europea ed alla presentazione di due documenti da parte della Commissione: il "*Piano di Azione*" per l'attuazione del Programma di Stoccolma (COM 2010/171, riguardante il potenziamento delle attività di cooperazione giudiziaria e di polizia); la "*Panoramica degli strumenti esistenti per la gestione delle informazioni nell'area di Libertà, Sicurezza Giustizia*" (COM 2010/385).

In tale occasione, il *WPPJ* ha confermato la propria visione della futura articolazione istituzionale, volta ad attuare le disposizioni di un quadro normativo unico ("*comprehensive legal framework*") che superi la precedente ripartizione delle politiche comunitarie in "Pilastri". Il contributo del *WPPJ* si è focalizzato sulla necessità di assicurare un ruolo di efficace supervisione alle autorità nazionali anche in settori sinora sottratti (almeno in parte) alla loro competenza e di mirare all'effettiva uniformità dei princìpi di protezione dati anche per quanto riguarda le attività di cooperazione giudiziaria e di polizia. In merito ai citati documenti della Commissione relativi al potenziamento della cooperazione giudiziaria e di polizia, il *WPPJ* ha adottato un "*Position Paper*", inviato alle istituzioni europee ed alle competenti autorità nazionali, per segnalare le incongruenze all'interno del "*Piano di Azione*" e sottolineare la necessità dell'immediato coinvolgimento delle autorità di protezione dati europee nell'attuazione della *policy* della Commissione nell'area del *cd.* "terzo pilastro". Il *WPPJ* ha altresì rilevato che l'obiettivo di assicurare il rispetto dei diritti fondamentali alla protezione dei dati ed alla *privacy*, così come proclamato nelle citate Comunicazioni della Commissione, deve essere garantito anche con riguardo alle banche dati ed agli strumenti attualmente esistenti. Nello sviluppo di nuovi strumenti occorrerà poi tenere conto dei princìpi di necessità e proporzionalità, e quindi dell'obbligo di documentare l'esigenza reale di raccogliere ed analizzare dati e informazioni per scopi di cooperazione giudiziaria e di polizia. Il *WPPJ* ha richiamato l'attenzione sul trattamento dei dati per attività di profilazione in relazione al rischio di discriminazione e di stigmatizzazione, nonché sulla prassi di stipulare, in determinati settori, accordi bilaterali *ad hoc* idonei a generare disomogeneità e incertezza del diritto. Il *WPPJ* ha inoltre avviato l'analisi dell'utilizzo dei dati genetici contenuti nelle banche dati nazionali (banche dati *DNA*) per finalità giudiziarie e di polizia, per verificare l'osservanza dei princìpi del "catalogo" (manuale) in materia di attività di supervisione e controllo elaborato dal *WPPJ* ed approvato dalla Spring Conference di Edinburgo nel 2009 (v. *Relazione* 2009, p. 273). A tal fine, il Gruppo ha predisposto un apposito questionario, di cui sta esaminando le risposte.

Il Gruppo ha poi monitorato la trasposizione a livello nazionale della decisione-quadro sulla protezione dati nel settore del terzo pilastro (Decisione 2008/977/GAI), valutando

lo "stato dell'arte" della disciplina del trattamento dei dati personali in ogni Stato membro e la prospettiva di uniformazione del quadro normativo.

Occorre, infine, fare riferimento al dibattito, apertosi nel corso del 2010 e proseguito nei primi mesi del 2011, sulla futura configurazione del rapporto fra *WPPJ* (che, si ricorda, è il gruppo di lavoro costituito dalla Conferenza di primavera e che riunisce le autorità di protezione dati europee, anche di Paesi non membri dell'Unione europea) e Gruppo Art. 29 (le cui competenze, prevalentemente connesse ai settore del *cd.* "primo pilastro", sono verosimilmente destinate ad ampliarsi in seguito alla revisione della Direttiva n. 95/46/CE secondo i princìpi introdotti dal Trattato di Lisbona). Si tratta di chiarire i termini della reciproca collaborazione tra i due Gruppi di lavoro onde evitare sovrapposizioni e garantire l'agevole transizione verso un sistema unitario di supervisione europeo in materia di protezione dei dati.

EUROPOL: l'attività dell'Autorità di controllo comune (ACC) e del comitato ricorsi

In relazione ad EUROPOL, fin dall'inizio del 2010, centrale è stata la discussione sulla definizione degli atti normativi necessari per assicurare la piena operatività della relativa Autorità di controllo comune nel mutato quadro giuridico (Decisione 2009/371/GAI del 6 aprile 2009, in vigore dal 1° gennaio 2010, che integra EUROPOL tra gli organismi dell'Unione europea).

La discussione si è focalizzata sull'organizzazione delle ispezioni nazionali e sul possibile coordinamento delle stesse, eventualmente sulla base del modus operandi approvato dal Gruppo di lavoro polizia e giustizia. Al riguardo, si è chiarito che il termine "ispezione" fa riferimento a due diverse attività: la prima, necessaria ai fini del completamento dell'ispezione annuale sugli archivi EUROPOL, consiste in accertamenti/verifiche puntuali sulla base delle specifiche segnalazioni inviate dal team ispettivo, tramite il segretariato dell'ACC, ad una o più autorità di protezione dati; la seconda, invece, consiste nell'esercizio del più generale ruolo di controllo delle autorità di protezione dati. Al segretariato è stato assegnato il compito di predisporre una bozza di modulo uniforme per le risposte da fornire al termine delle attività di accertamento/verifica di tipo puntuale.

L'Autorità di controllo comune, ricostituita a seguito dell'entrata in vigore della nuova base giuridica, ha tenuto la sua prima riunione il 9 marzo 2010, eleggendo il Presidente (la portoghese Cruz) ed il Vicepresidente (la slovena Pirc).

L'ACC ha approvato il rapporto sull'ultima ispezione annuale, svolta, nel marzo 2010, sugli archivi di lavoro per fini di analisi e sul sistema di informazione EUROPOL, integrato con le risultanze delle attività di verifica specifiche operate, su segnalazione, a livello nazionale.

Si ricorda, inoltre, che l'Autorità di controllo comune è tenuta a fornire un parere nell'ambito della procedura di approvazione da parte del Consiglio dell'Unione europea degli accordi negoziati tra EUROPOL e Paesi terzi. A riguardo l'ACC ha adottato pareri relativi alla conclusione di accordi sullo scambio di dati con la Repubblica di Macedonia e con Israele, con i quali, pur ravvisando l'opportunità di introdurre specifiche garanzie, si è formulato un giudizio globalmente positivo.

Per quanto riguarda la Colombia, dopo un primo parere negativo (del 9 marzo 2010), che ha evidenziato alcuni punti critici sull'adeguatezza dell'accordo in materia di protezione dati (applicazione delle misure di salvaguardia solo ai dati contenuti in banche dati, inquadramento giuridico dell'accordo nell'ambito della gerarchia delle norme dell'ordinamento colombiano, esercizio del diritto d'accesso da parte degli interessati, termini per la conservazione e la cancellazione dei dati), l'Autorità di controllo comune, con parere del 10 maggio 2010 ha espresso parere favorevole alla conclusione dell'accordo tra Colombia ed EUROPOL.

È stato poi adottato un parere favorevole in relazione al progetto di accordo tra EUROPOL ed il Principato di Monaco, ritenendo adeguato il livello di protezione dei dati personali offerto dal Principato nel quadro della cooperazione con EUROPOL.

Un parere fortemente critico è stato formulato, invece, sulla possibilità per EUROPOL di ricevere informazioni provenienti da parti private.

Nei giorni 18 e 19 ottobre 2010 si è tenuta, a L'Aja, la conferenza sulla protezione dei dati personali organizzata da EUROPOL con la Federazione russa. La Conferenza ha consentito di chiarire diversi aspetti relativi alla legislazione ed alla prassi amministrativa della Federazione russa nel campo della protezione dati, inclusi i poteri e l'organizzazione dell'autorità di supervisione sui trattamenti di dati personali (*Raskomnadzor*). Al termine dei lavori sono stati fissati alcuni punti condivisi, che saranno utili ad EUROPOL per negoziare eventuali accordi operativi per lo scambio di dati con la Federazione russa. Gli schemi di

accordo dovranno comunque essere sottoposti al parere dell'Autorità di controllo comune, che, in precedenti pareri, ha già sottolineato le perplessità e i punti critici per quanto riguarda, in modo specifico, il trattamento dei dati personali da parte delle autorità di polizia della Federazione russa.

Quanto ai nuovi compiti affidati ad EUROPOL dall'accordo sul trasferimento di dati relativi alla messaggistica finanziaria (*cd.* "accordo *TFTP2*") tra Stati Uniti e Unione europea, l'ACC ha deciso di svolgere una prima verifica, utilizzando il team di esperti per le ispezioni, per accertare quali dati sono richiesti dal Dipartimento del tesoro tramite EUROPOL ed a quali trattamenti sono sottoposti. In seguito a questa "*fact finding investigation*", potranno essere discussi ed analizzati gli aspetti di congruenza dell'attività svolta da EUROPOL nel contesto dell'accordo *TFTP2* con quanto previsto dalla Decisione EUROPOL.

La relazione sull'ispezione svolta presso EUROPOL è stata approvata nel corso della riunione straordinaria dell'Autorità di controllo comune svoltasi a Lubiana il 31 gennaio 2011 e, subito dopo, è stata messa a disposizione delle autorità di protezione dati partecipanti alla valutazione congiunta dell'accordo *TFTP2* in rappresentanza del Gruppo Art. 29.

Infine, si è tenuto il 1° febbraio 2011, sempre a Lubiana, l'incontro delle autorità di controllo comune EUROPOL, EUROJUST, Schengen e Dogane per valutare e discutere, tra l'altro, eventuali specifici contributi da offrire in relazione alla Comunicazione della Commissione del 4 novembre 2010 "*Un approccio globale alla protezione dei dati personali nell'Unione europea*", per quanto concerne, in particolare, gli aspetti di integrazione dell'area *cd.* "terzo pilastro" e le conseguenti modifiche delle forme di supervisione congiunta.

Altri punti di interesse in discussione hanno riguardato: la definizione delle strategie delle autorità di controllo comune in relazione alle forme di comunicazione da adottare per informare i cittadini sui compiti e sull'attività svolta, l'applicazione del principio di disponibilità, le modalità di connessione di EUROPOL al SIS.

Si segnala che è stato attivato, nel corso del 2010, il nuovo sito *web* dell'Autorità di controllo comune EUROPOL (*http://europoljsb.consilium.europa.eu*), nel quale sono disponibili, anche in italiano, i principali documenti adottati, nonché informazioni agli interessati su come esercitare i diritti di accesso e gli altri diritti connessi.

Altro aspetto di grande importanza attiene all'attività del comitato per i ricorsi dell'ACC. Si ricorda brevemente che un richiedente può esercitare il diritto di accesso alle informazioni che lo riguardano in possesso dell'EUROPOL, nonché ottenere che tali informazioni siano verificate, corrette o cancellate. Qualora ritenga che l'EUROPOL non abbia fornito una risposta soddisfacente, il richiedente può ricorrere avverso la decisione al comitato per i ricorsi, le cui decisioni sono definitive per tutte le parti coinvolte.

Al riguardo, si segnala che il Comitato ha ricevuto ed esaminato, in quanto ritenuti ammissibili, 3 ricorsi, sui quali una formale decisione è stata assunta nel corso della riunione di dicembre 2010.

Il Sistema informativo doganale (SID): *CIS - Supervision Coordination Group* e Autorità comune di controllo

L'8 marzo 2010 si è tenuta la prima riunione, convocata dall'EDPS, della nuova autorità di supervisione (*CIS - Supervision Coordination Group*) sul sistema informativo Dogane. Nell'incontro, i rappresentanti della Commissione europea e dell'OLAF hanno illustrato la nuova base giuridica per l'utilizzo del SID: il Regolamento (CE) n. 515/97 del 13 marzo 1997 (cfr., in particolare, art. 37), relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione della normativa doganale e agricola, nonché, nell'ambito della cooperazione giudiziaria e di polizia, la Decisione 2009/917/GAI del 30 novembre 2009, la cui entrata in vigore è prevista per il 27 maggio 2011.

In considerazione della sopravvenuta coesistenza di due forme di supervisione per un'unica banca dati (il SID - Sistema informativo doganale), si è ritenuto di definire modalità di cooperazione il più possibile integrate per evitare riunioni in tempi diversi dei due organismi di supervisione (ACC Dogane e *CIS - Supervision Coordination Group*).

Per quanto riguarda l'attività di verifica e controllo dei trattamenti dei dati nell'ambito del SID, è stato elaborato un questionario da completare a cura delle autorità competenti degli Stati membri (per l'Italia, Agenzia delle Dogane) per l'autovalutazione degli aspetti relativi all'idoneità delle misure di sicurezza adottate ed alla formazione del personale su tali misure.

Il questionario di *self assessment* è stato inviato, con osservazioni anche sulla possibile revisione della struttura e dei quesiti, dal Garante al Segretariato della ACC, che esaminerà

e confronterà le risposte fornite dalle autorità competenti dei diversi Stati aderenti al sistema informativo doganale.

Riguardo l'organizzazione dell'ispezione al SID centrale (C.CIS) a Bruxelles, è previsto un gruppo ispettivo composto da un rappresentante del segretariato dell'Autorità di controllo comune e da altri tre rappresentanti.

Il Sistema informativo Schengen: valutazione Schengen dell'Italia e attività dell'ACC

Il 27 gennaio 2010 si è svolta la valutazione Schengen dell'Italia per gli aspetti relativi alla protezione dei dati personali riferiti alla sezione nazionale del Sistema informativo Schengen (N.SIS).

Nel corso della visita presso il Garante sono state illustrate l'organizzazione e la struttura dell'autorità, i poteri e le competenze, nonché le modalità di esercizio del ruolo di supervisione e controllo sui trattamenti di dati personali nel settore polizia e giustizia. Inoltre, sono stati trattati i temi dell'esercizio dei diritti di accesso, rettifica e cancellazione da parte degli interessati e della cooperazione con le altre autorità di protezione dei dati dei Paesi Schengen con specifico riferimento a richieste riguardanti segnalazioni inserite nel sistema informativo da altri Paesi.

Il gruppo di esperti ha altresì approfondito, presso la sede di N.SIS e Divisione SIRENE del Ministero dell'interno, l'esame dell'organizzazione di tali servizi e delle modalità di esercizio del diritto di accesso.

All'esito di tale procedura, il Gruppo di esperti ha espresso una valutazione nel complesso positiva ed ha formulato alcune raccomandazioni, in linea con le prescrizioni emanate dal Garante, volte a intensificare le misure di sicurezza poste a tutela di dati e sistemi.

Inoltre, si segnala che il 3 maggio 2010 si è tenuta, presso il Consiglio dell'Unione europea, la riunione del "*Working Party on Schengen Evaluation*", relativa, tra l'altro, alla presentazione del rapporto (formalmente adottato nella riunione di giugno) redatto dal gruppo di esperti a conclusione della visita svolta in Italia a gennaio. Il rapporto contiene, in particolare, specifiche raccomandazioni, rivolte sia al Garante sia al Ministero dell'interno. Il citato *Working Party* ha contestualmente dato l'avvio al monitoraggio dell'attuazione, da parte del Ministero dell'interno, delle raccomandazioni previste dal rapporto.

A margine, è in corso l'attività di revisione delle modalità con le quali si procede alle

valutazioni Schengen per i singoli Paesi. A tal fine, la Commissione europea ha presentato il 19 novembre 2010 una proposta di regolamento per il successivo esame da parte del Consiglio dell'Unione europea. Il Ministero dell'interno ha svolto una prima riunione di coordinamento per analizzare i primi nove articoli del testo il 15 dicembre 2010.

Per quanto riguarda la composizione dell'ACC, nel mese di marzo l'Autorità comune di controllo Schengen ha rinnovato i vertici eleggendo, come presidente, la tedesca Angelika Schriever-Steinberg e come vicepresidente, lo svizzero Jean Philippe Walter.

In relazione all'attività di controllo sul Sistema d'informazione Schengen, l'ACC ha programmato il nuovo calendario di verifiche da svolgere con riguardo alle segnalazioni inserite nel SIS. A tal fine, il Segretariato ha predisposto una *checklist* per le verifiche, basata sulle raccomandazioni formulate dalla stessa autorità comune di controllo. Per l'anno 2011, l'ACC si propone, in modo specifico, di effettuare attività di verifica sugli inserimenti nel SIS di segnalazioni su richiesta delle autorità giudiziarie.

Inoltre, le delegazioni sono state invitate a fornire elementi sul seguito dato alle raccomandazioni formulate dall'ACC al termine dell'azione comune sulla verifica della correttezza dell'inserimento nel SIS di segnalazioni *ex* art. 96 della Convenzione (stranieri segnalati ai fini della non ammissione). Sulla base degli elementi ricevuti l'ACC ha adottato il *report* ("*Report of the Schengen Joint Supervisory Authority on the follow-up of the recommendations concerning the use of Article 96 alerts in the Schengen Information System*").

L'Autorità di controllo comune ha inoltre deciso di completare le verifiche con riferimento alle segnalazioni inserite nel SIS *ex* art. 95 della Convenzione (persone ricercate per arresto a fini di estradizione). A tal fine, il Segretariato sta predisponendo il modello di questionario da sottoporre alle competenti autorità nazionali.

Sono invece ancora in corso di definizione le modalità e la tempistica per la valutazione del *follow-up* dell'attività di controllo delle segnalazioni inserite nel SIS in base all'art. 99 della Convenzione (dati relativi a persone o veicoli inseriti a fini di sorveglianza discreta o controllo specifico).

È stata poi valutata l'opportunità di svolgere una nuova campagna informativa sui diritti degli interessati in relazione ai Sistemi informativi Schengen. Si ricorda che l'Autorità di