alla conclusione che i meccanismi stabiliti nel codice di autoregolamentazione adottato nell'aprile 2011 dalla *European Advertising Standards Alliance (EASA) e dall'Internet Advertising Bureau Europe* (*IAB*), non sono in linea con il requisito del consenso preventivo (*opt-in*) per l'installazione di *cookies* a fini diversi dalla prestazione del servizio di comunicazione o di un servizio espressamente richiesto dall'utente (art. 5, par. 3, Direttiva n. 2002/58/CE). Tuttavia, vengono segnalate varie possibilità tecniche per l'espressione di tale consenso (fra cui una opportuna configurazione dei parametri di navigazione internet, *"browser settings"*, anche attraverso il suggerimento italiano di appositi dispositivi *"plug-in"* configurabili a seconda dello specifico *browser*, o la creazione di *opt-in cookies*), evidenziando alcuni elementi positivi ma migliorabili (ad esempio l'uso di un'icona per l'informazione iniziale dell'utente, da sviluppare in linea con il principio della *"layered information notice"*, sostenuto dal Gruppo Art. 29 nel proprio parere WP 100).

Inoltre (anche attraverso uno scambio di corrispondenza con IAB) è stata sottolineata la portata non esaustiva degli strumenti di autodisciplina a tutela dei princìpi sanciti nell'art. 5, par. 3 della Direttiva.

Parere 13/2011 sui servizi di geolocalizzazione tramite *smart mobile devices*

Il parere in tema di geolocalizzazione e servizi mobili intelligenti (smartphones) (WP 185 del 16 maggio 2011), è volto a chiarire i profili di responsabilità dei gestori telefonici e dei produttori/distributori di applicazioni (*apps*) per i dispositivi mobili. Questi contengono infatti una vasta gamma di informazioni riservate, anche sensibili, quali i dati relativi alla posta elettronica, alle immagini private, alla cronologia di navigazione internet, alla rubrica telefonica. Sulla base di una dettagliata analisi tecnica, alla quale seguono considerazioni di ordine giuridico rispetto all'applicazione delle Direttive nn. 2002/58/CE e 95/46/CE, il Gruppo raccomanda ai produttori di *software* ed ai fornitori di applicazioni di geolocalizzazione, titolari del trattamento dei dati personali raccolti attraverso tali sistemi, di assicurare informative adeguate, l'esercizio dei diritti degli interessati e la messa a disposizione di strumenti *"user-friendly"* per definire il livello di dettaglio della localizzazione (cosiddetta "granularità" del servizio). Inoltre, pur riconoscendo che in talune circostanze (ad esempio in presenza di aree urbane densamente popolate) l'associazione fra i codici di accesso dei singoli dispositivi (che sono identificatori univoci dell'apparecchio) e i dati di localizzazione non

consente necessariamente di identificare una persona fisica determinata, il Gruppo sottolinea la necessità di considerare le informazioni in oggetto alla stregua di dati personali, a meno che il titolare possa dimostrare in modo ragionevole che i dati raccolti non sono personali.

Nel corso del 2011 sono stati poi adottati il parere relativo ai cd. "contatori intelligenti" (*smart meters*) nel settore delle forniture di gas, elettricità ed altri servizi (WP 183 del 4 aprile 2011) ed il parere sulla nuova proposta di *privacy impact assessment* relativo alle tecnologie *RFID* (WP 180 dell'11 febbraio 2011).

Parere 12/2011 sui "contatori intelligenti"

Il parere sui contatori intelligenti presuppone la definizione di un concetto chiave quale l'*"energy fingerprint"*, che fa riferimento al fatto che le modalità di consumo di energia proprie di ciascun utente, possono, in talune circostanze, costituire un dato identificativo dell'interessato, in analogia a quanto avviene con il concetto di *"browsing fingerprint"* per i servizi della società dell'informazione erogati sulla rete internet. Il Gruppo ha suggerito al riguardo di prevedere specifiche garanzie di protezione dati nell'ambito dei contratti di fornitura di energia, nonché un più ampio ricorso al principio di *"Privacy by Design"* nella progettazione di tali dispositivi. Si è sottolineato che le raccomandazioni formulate, riguardanti anche la responsabilità del trattamento dei dati e la più puntuale individuazione dei fondamenti di legittimità del trattamento, si basano sulle conoscenze attualmente disponibili, e che interventi ulteriori da parte del Gruppo potrebbero rendersi necessari per valutare aspetti di futura emersione (specie rispetto all'attuazione del principio di *"Privacy by Design"*).

Motori di ricerca

Sempre nel contesto delle nuove tecnologie, alla luce dei recenti sviluppi relativi alla nuova *"Privacy Policy"* di *Google*, in particolare, con riferimento alla previsione di un'informativa unica valida per tutti i servizi offerti che presenta aspetti non del tutto chiari quanto al possibile raggruppamento anche dei dati personali raccolti per tali servizi in un unico *"repository"* centrale, il Gruppo ha chiesto a *Google Inc.* una pausa di riflessione segnalando l'intenzione di ottenere ulteriori delucidazioni in merito (lettera del 2 febbraio 2012). I Garanti hanno inoltre sostenuto l'autorità irlandese nell'attività di audit da essa condotta nei riguardi di *Facebook Ireland ltd.*, la filiale irlandese di *Facebook*, responsabile dei trattamenti di dati personali concernenti cittadini o soggetti stabiliti nell'Ue, i cui sviluppi sono costantemente monitorati in modo congiunto.

In tema di trasferimento di dati verso Paesi terzi, su richiesta della Commissione europea, che dovrà esprimersi con una decisione sul punto, il Gruppo ha adottato un parere favorevole alla valutazione di adeguatezza del livello di protezione offerto dalla Nuova Zelanda (WP 182 del 4 aprile 2011).

Parere 11/2011 sul livello di protezione dei dati personali nella Nuova Zelanda

Il Gruppo ha inoltre continuato ad occuparsi del trasferimento e trattamento dei dati in ambito finanziario.

In particolare, con il parere 14/2011 (WP 186 del 13 giugno 2011), è stato affrontato il tema della tutela dei dati personali nel contesto della prevenzione dei fenomeni del riciclaggio di denaro e del finanziamento del terrorismo e sono state fornite raccomandazioni per i soggetti coinvolti nella regolamentazione e nell'*enforcement* a scopo di prevenzione di tali fenomeni.

Parere 14/2011 sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo

Per quanto riguarda la cooperazione amministrativa internazionale nel settore della vigilanza sulle società di revisione contabile, tra le autorità competenti dell'Ue e quella degli Stati Uniti (*Public Companies Account Oversight Body - PCAOB*), è stata indirizzata alla Commissione europea una lettera-parere (13 dicembre 2011), volta a fornire indicazioni sul rispetto dei requisiti di protezione dei dati personali nel contesto della cooperazione amministrativa, ai sensi della Direttiva n. 2006/43/CE (cd. ottava direttiva) sul controllo della revisione dei conti, anche al fine di valutare gli accordi per la protezione dei dati personali ("data protection arrangements") tra le autorità di vigilanza del settore.

Lettera del 13 dicembre 2011 sui trasferimenti internazionali di dati allo *US Public Accounting Oversight Body - PCAOB*

È stato poi portato all'attenzione del Gruppo il tema della compatibilità della legge degli Stati Uniti, denominata *"Foreign Account Tax Compliance Act - FATCA"*, che entrerà in vigore il 1° gennaio 2013, con la legislazione di protezione dati europea. Obiettivo della *FATCA* è il contrasto all'evasione fiscale "offshore" (incluso il territorio dell'Unione europea) ad opera di *"US persons"* che abbiano effettuato investimenti in Europa. La Commissione europea ha chiesto al Gruppo Art. 29 di formulare una lettera/parere sulle criticità poste dai trattamenti di dati personali conseguenti all'applicazione della legislazione *FATCA*, in particolare con riferimento alla base giuridica, alla legittimità del trattamento, alla tipologia dei dati personali richiesti, ai soggetti coinvolti e alla possibilità di *"onward transfer"*, ossia di ulteriori trasferimenti dei dati. Il problema è in corso di esame da parte del Gruppo, anche alla luce dei possibili futuri accordi in materia tra Stati Uniti e Stati membri dell'Unione europea.

Binding corporate rules - BCR

In materia di *binding corporate rules* (*BCR*) il lavoro si è concentrato sulla definizione di un nuovo modello di *BCR*, chiamato *"BCR for data processor"*, ispirato alle *"BCR for controller"*, che dovrebbe consentire i trasferimenti transfrontalieri di dati all'interno di una società multinazionale di servizi. Il sistema è concepito secondo un doppio schema: il cliente (titolare) sottoscrive un contratto generale di servizi (*Service Level Agreement - SLA*) con la società multinazionale (responsabile); tra le clausole contrattuali sono ricomprese le *"BCR for processor"* (allegate allo *SLA*) tramite le quali la società multinazionale ha la possibilità di "sub-appaltare" le attività di trattamento (o alcune fasi di esso) alle proprie consociate, anche stabilite in Paesi terzi, senza necessità di ulteriori formalità (autorizzazioni *ad hoc*, *standard contractual clauses*, ecc.). Lo schema di *"BCR for processor"* ricalca quello delle *"BCR for controller"* nei suoi princìpi fondamentali: efficacia vincolante delle *BCR*, clausola del terzo beneficiario a favore dell'interessato; clausola di responsabilità con attrazione della giurisdizione nell'Unione europea; rispetto dei princìpi della Direttiva n. 95/46/CE; impegno per il gruppo multinazionale a dotarsi di un sistema di *training*, a disporre di una struttura specializzata nella gestione delle segnalazioni degli interessate a svolgere audit periodici sul rispetto dei princìpi di protezione dati.

Nell'ambito dell'attività volta a semplificare gli oneri a carico delle imprese interessate, è stata discussa l'opportunità di elaborare dei modelli base di *"audit"* e *"training"*. Gli schemi sono attualmente in corso di perfezionamento e saranno verosimilmente resi pubblici nel corso del 2012.

"Terrorist Finance Tracking Program", cd. TFTP2

Il Gruppo ha inoltre proseguito la discussione sul monitoraggio dell'attuazione dell'accordo sulla trasmissione dei dati di messaggistica finanziaria tra Unione europea e Stati Uniti (*"Terrorist Finance Tracking Program"*, cd. *TFTP2*), che ha visto, tra l'altro, il controllo da parte di EUROPOL delle richieste di trasferimento di dati finanziari dall'Unione europea al Dipartimento del Tesoro degli Stati Uniti.

È stato oggetto di approfondito esame, in particolare, il rapporto relativo alla revisione congiunta, svoltasi a Washington il 17 e 18 febbraio 2011 (*"Commission report on the joint review of the implementation of the Agreement"*). Il rapporto è stato formulato dal team per l'Unione europea (composto anche dalle autorità del Belgio e dei Paesi Bassi) e sottoposto, per integrazioni, al team degli Stati Uniti.

Sempre sull'attuazione dell'accordo *TFTP2*, si segnala il rapporto sull'ispezione effettuata dall'Autorità di controllo comune (ACC) EUROPOL (su cui, v. anche par. 18.3. e Relazione 2010, p. 229). Al riguardo si osserva che i compiti aggiuntivi attribuiti ad EUROPOL in virtù dell'accordo *TFTP* tra l'Unione europea e gli Stati Uniti determinano una correlativa espansione della competenza dell'Autorità di controllo comune, al fine di verificare la legittimità anche dei trattamenti di dati personali effettuati ai sensi di tale accordo.

Nella lettera del 7 giugno 2011 al Dipartimento del Tesoro degli Stati Uniti sull'interpretazione dell'accordo *TFTP2*, il Gruppo pone il problema di come garantire l'effettivo esercizio del diritto d'accesso degli interessati ai dati oggetto di trattamento in base all'accordo, e delle modalità da seguire, in particolare, per quanto concerne l'accertamento dell'identità del richiedente. È stato infatti stato rilevato che le richieste di accesso, trasmesse al Dipartimento del Tesoro degli Stati Uniti, possono essere ritenute inammissibili se non sufficientemente dettagliate e comunque non conformi alle regole procedurali stabilite dallo stesso Dipartimento. Nella lettera si esprime, tra l'altro, l'intento di raggiungere un *common understanding* con gli Stati Uniti sull'applicazione dell'accordo *TFTP2*.

Sistema europeo per il tracciamento delle transazioni finanziarie a scopo di antiterrorismo - *EU TFTP*

Il Gruppo Art. 29 è stato anche consultato sull'istituendo sistema europeo per il tracciamento delle transazioni finanziarie a scopo di antiterrorismo (cd. *EU TFTP*, basato sulla raccolta e l'analisi dei dati di messaggistica finanziaria). Al riguardo, in relazione alla Comunicazione della Commissione europea [COM(2011) 429] sul programma di monitoraggio delle transazioni finanziarie *EU TFTP*, con lettera del 22 settembre 2011 alla Commissaria Malmström, è stata sottolineata la vaghezza del contenuto della Comunicazione stessa in merito alla futura architettura e alle funzioni del sistema informativo e sono state segnalate sia la possibile sovrapposizione con altri strumenti esistenti intesi a perseguire il medesimo obiettivo, sia le criticità derivanti dall'adozione di un sistema *TFTP* del tutto nuovo, da utilizzare come strumento europeo per finalità di contrasto del terrorismo.

Parere 10/2011 sul sistema di *PNR* europeo

Il parere del Gruppo sulla proposta di direttiva della Commissione europea, che istituisce un sistema europeo di utilizzo dei dati del codice di prenotazione (*PNR*) ai fini di prevenzione, accertamento, indagine ed esercizio dell'azione penale nei confronti dei reati di terrorismo e di altri reati gravi (WP 181 del 5 aprile 2011), ha analizzato principalmente la

necessità e la proporzionalità del sistema oltre che le modalità di trattamento previste. Riprendendo argomentazioni già formulate nel parere adottato congiuntamente con il *Wppj* sul precedente testo (lettera-parere del 18 dicembre 2007), non si sono ritenute sufficientemente dimostrate né la necessità del sistema, né la sua utilità specifica rispetto all'obbligo per le stesse compagnie di fornire in anticipo i dati *API* (*Advance Passenger Information*) dei passeggeri. Quanto alla proporzionalità, perplessità si esprimono in particolare sui rischi di una raccolta indiscriminata di dati a prescindere da reali esigenze legate alla commissione di reati, sulla notevole ampiezza del campo di applicazione e del margine di manovra lasciato agli Stati membri, sulla lunghezza del periodo e sulle modalità di conservazione dei dati, sul vasto numero di dati richiesti, inclusi quelli sensibili, nonché sul ruolo e le responsabilità delle *"Passenger Information Unit"* (*PIU*) nel trattamento dei dati.

Si segnala, infine, che il Gruppo si è espresso anche in merito agli accordi *PNR* con Stati Uniti/Canada/Australia, con lettera del 19 gennaio 2011, inviata alla Commissaria responsabile per gli Affari interni della Commissione europea, Cecilia Malmström. Nel testo si sottolineano i punti critici già evidenziati nei precedenti interventi del Gruppo (v. Relazione 2010, p. 222) ovvero: in primo luogo la non dimostrata necessità di ricorrere ai dati *PNR* per le finalità di cui agli accordi; i tempi di conservazione dei dati da parte delle autorità di *law enforcement*; i presupposti e le modalità per il trasferimento dei dati e per l'accesso agli stessi; il trasferimento ulteriore dei dati (*onward transfer*) ad altre autorità e/o Stati terzi; il controllo, la durata e la revisione congiunta degli accordi.

Parere 1/2012 su epSOS

Per quanto concerne i dati sanitari, il Gruppo si è occupato del progetto epSOS (*Smart Open Services for European Patients*) in materia di protezione dei dati personali, per l'interoperabilità nel settore della sanità elettronica, co-finanziato dalla Commissione europea, al quale partecipano 47 soggetti (tra cui ministeri della salute e aziende private) in rappresentanza di 20 Stati membri (e di 3 Stati extra-Ue: Svizzera, Turchia e Norvegia). L'obiettivo principale è la creazione di un sistema di *e-health* (comprensivo della relativa infrastruttura di *Information Technology-IT*) che consenta di accedere, in maniera sicura e nel rispetto della *privacy*, alle informazioni sanitarie dei pazienti. L'interscambio di dati avviene mediante una rete informatica composta da *National Contact Point– "NCP"* (circa

uno per ogni partecipante) i quali svolgono il ruolo di interfaccia nazionale nei confronti dei *Point of Care - "POC"* (medici, strutture sanitarie, farmacie, veicoli di emergenza, ecc.) situati nello Stato membro estero e aderenti al progetto epSOS. Il *NCP* è considerato il principale referente del funzionamento del progetto, poiché ha competenza a contrarre con gli organismi sul territorio ed ha il compito di curare il rispetto delle regole in materia di sicurezza e riservatezza dei dati trasferiti.

Nel parere del Gruppo (WP 189 del 25 gennaio 2012), particolare attenzione è stata rivolta all'esigenza di individuare esattamente il titolare ed il responsabile del trattamento, nonché eventuali forme di contitolarità dello stesso. Inoltre, sono state fornite indicazioni relativamente alle modalità di acquisizione del consenso (affinché si specifichi quando esso riguardi la partecipazione al progetto e quando, invece, sia rivolto al singolo trattamento sanitario richiesto), all'informativa (che dovrà indicare in maniera chiara le caratteristiche tecniche del trasferimento di dati all'interno del sistema) e alle misure di sicurezza (che dovranno garantire un elevato livello di protezione dei dati nell'ambito dell'intero processo di interscambio degli stessi).

Infine, quanto agli aspetti problematici legati al sempre maggiore uso della biometria nell'ambito delle nuove tecnologie (ad esempio, la diffusione delle tecniche di riconoscimento facciale, vocale, ecc.), il Gruppo sta predisponendo un nuovo parere generale, ed uno più specifico relativo al riconoscimento facciale, che dovrebbe essere approvato nel corso del 2012.

È stato altresì riattivato il sottogruppo *WADA* (*World Anti-Doping Agency*), che, in occasione della revisione del codice mondiale antidoping, fornirà indicazioni alla Commissione europea sulla protezione dei dati personali nel contesto della lotta al doping nelle attività sportive professionali.

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

Working Party on Police and Justice (Wppj)

Nel 2011 il *Wppj* ha proseguito, sotto la presidenza italiana, le attività avviate in base al "Programma di lavoro" approvato nel 2009, ed ha condotto un'approfondita riflessione sul proprio ruolo e sulle modalità utili a garantire un migliore coordinamento con il Gruppo

Art. 29, alla luce dell'unificazione del quadro normativo di protezione dati, prevista dal Trattato di Lisbona, sia pure con i contemperamenti indicati nelle dichiarazioni ad esso allegate.

Al riguardo, le riunioni tenutesi presso la sede del Consiglio Ue a Bruxelles e l'intenso scambio di documentazione fra le delegazioni, hanno permesso di delineare un possibile quadro di competenze e collaborazione, anche sulla base delle richieste, formulate al *Wppj* in occasione della *Spring Conference* 2011, di valutare quali delle sue competenze potessero essere trasferite al Gruppo Art. 29, rispetto alle tematiche *ex*-III Pilastro ricadenti prevalentemente o esclusivamente nell'ambito dell'Ue. Sulla base di tali premesse, il *Wppj* ha stabilito di completare le attività già in corso e programmate aventi rilevanza paneuropea: analisi delle problematiche connesse allo scambio e trattamento di dati Dna fra autorità giudiziarie e di polizia a livello europeo, anche con riguardo all'utilizzo dei canali INTERPOL; individuazione degli ambiti di una possibile indagine coordinata paneuropea sulla base del metodo di analisi del rischio delineato nel "Catalogo" sviluppato dal *Wppj* in tema di cooperazione e supervisione (approvato dalla *Spring Conference* del 2009); potenziamento della cooperazione con il Consiglio d'Europa rispetto alla revisione della Convenzione n. 108/1981 e della Raccomandazione n. R(87)15 sul trattamento dei dati per fini di polizia. Peraltro, il *Wppj* ha stabilito di trasferire al Gruppo Art. 29 ogni competenza in merito alla valutazione dello stato di attuazione della decisione-quadro sulla protezione dei dati personali nell'*ex*-III Pilastro (decisione quadro 2008/977/GAI del Consiglio dell'Ue), ricadendo quest'ultima in un ambito esclusivamente legato all'Ue.

Relativamente all'indagine sul trattamento e scambio di dati Dna in ambito giudiziario e di polizia, le risposte al questionario circolato nel corso del 2010 e nei primi mesi del 2011, pur in presenza di un quadro parziale, hanno evidenziato numerose difformità a livello nazionale, anche con riguardo alle misure di sicurezza in essere. Il *Wppj* ha quindi iniziato ad elaborare possibili indicazioni operative omogenee, anche alla luce di esperienze sviluppate in altri ambiti internazionali (in particolare, INTERPOL).

L'analisi condotta in base ai criteri delineati nel "Catalogo" ha portato ad individuare nei trattamenti di dati relativi a soggetti non sospettati di reati (conoscenti e/o contatti personali di sospetti e/o criminali) un'area di particolare delicatezza per quanto riguarda le attività di

polizia e giudiziarie, tenuto conto della sensibilità delle informazioni potenzialmente raccolte e dell'assenza o dell'opacità di disposizioni normative sul punto. Il *Wppj* ha quindi elaborato, in via provvisoria, una lista di quesiti e tematiche sulle quali chiedere specifiche delucidazioni attraverso un'eventuale indagine paneuropea.

Il *Wppj* ha seguito attentamente il dibattito in seno ai competenti gruppi di lavoro del Consiglio d'Europa (Comitato consultivo cd. *T-PD*) con riguardo sia alla revisione (modernizzazione) della Convenzione n. 108/1981 sia all'analisi della Raccomandazione R(87)15; molte delegazioni del *Wppj* avevano già fornito indicazioni attraverso il questionario che il Consiglio aveva fatto circolare fra le autorità nazionali competenti, nel corso del 2011, per valutare lo stato di attuazione della Raccomandazione e le relative problematiche (v. *infra*).

Nei prossimi mesi le attività sopra descritte dovranno trovare compiuta conclusione e le autorità europee di protezione dati (riunite nella *Spring Conference* 2012) dovranno pronunciarsi sul futuro del *Wppj*. Resta indubbio il contributo fornito da quest'ultimo nel monitorare possibili criticità nel settore della cooperazione giudiziaria e di polizia in materia penale, indicando anche soluzioni o strumenti armonizzati utili a garantire la salvaguardia dei diritti riconosciuti ai cittadini europei.

Riunioni congiunte delle autorità di controllo comune (ACC) EUROPOL, EUROJUST, Schengen, Dogane

Dell'incontro congiunto delle autorità di controllo comune EUROPOL, EUROJUST, Schengen e Dogane svoltosi il 1 febbraio 2011 si è riferito nella Relazione 2010 (p. 229).

Si è svolta a Bruxelles, nei giorni 1° e 2 marzo 2011, la successiva riunione delle ACC, nella quale è stato deciso di concentrare l'analisi programmatica, già iniziata nella riunione di Lubiana, sugli elementi necessari per una buona supervisione, senza bloccarsi su questioni nominalistiche.

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

Una riunione straordinaria dell'ACC EUROPOL si è tenuta il 31 gennaio 2011 a Lubiana per approvare il rapporto dell'ispezione svolta presso EUROPOL da un ristretto gruppo di esperti per acquisire informazioni sull'attività svolta nel quadro dell'accordo *TFTP2* Ue-Stati Uniti. Il documento è stato redatto con classifica di sicurezza "Segreto Ue" e non è pertanto accessibile nemmeno agli stessi componenti dell'ACC. Per esigenze di trasparenza è stato redatto un comunicato dando atto delle operazioni compiute e descrivendo gli elementi che possono essere resi pubblici (v. anche par. 18.2. e Relazione 2010, p. 229).

Grande attenzione è stata riservata dal Parlamento europeo al rapporto presentato sull'ispezione ed è stata evidenziata la questione dell'accesso ai documenti dell'ACC.

L'Acc EUROPOL ha poi svolto una seconda ispezione, a distanza di un anno dalla precedente, per verificare lo stato di attuazione delle prescrizioni impartite e lo stato del trattamento dei dati. Anche questo secondo rapporto, una volta approvato dall'ACC, sarà soggetto alle stesse regole di segretezza e sarà comunque redatto un comunicato pubblico sui risultati.

Anche mediante incontri con i responsabili di EUROPOL, è stata analizzata la proposta di far confluire gli attuali archivi di analisi in due contenitori più ampi, dedicati rispettivamente al terrorismo ed al crimine organizzato. In particolare, il 4 maggio 2011, presso la sede di EUROPOL a l'Aja, si è tenuto l'incontro tra i responsabili di EUROPOL, il segretariato comune delle ACC e i componenti del sottogruppo *Analytical Work File* (*AWF*) dell'ACC EUROPOL, per ottenere le informazioni necessarie per comprendere le ragioni della proposta e valutare come essa possa essere considerata in linea con le previsioni della Decisione EUROPOL (Decisione 2009/371/GAI del Consiglio dell'Ue).

Conseguentemente, EUROPOL ha evidenziato la compatibilità della proposta con il quadro legale esistente, con riferimento all'architettura dei nuovi *AWF*, (archivi di lavoro per fini di analisi), ai compiti e alle responsabilità, alle modalità di accesso e alle misure di sicurezza. Nei successivi incontri volti a definire le valutazioni dell'Autorità in merito, sono state espresse perplessità in relazione ai dati ricevuti e non ancora attribuiti ad una specifica analisi, per quanto attiene al rispetto del principio di finalità. L'ACC dopo lunga discussione, ha informato con una lettera il direttore di EUROPOL che *prima facie* non ritiene tale modo di operare in contrasto con il quadro legale esistente e che non intende bloccare i lavori, anche se è indispensabile chiarire molti aspetti non secondari, per non abbassare il livello di garanzie e le possibilità di controllo oggi esistenti.

Sono state inoltre discusse le prime risultanze della 13ª ispezione annuale svoltasi nel marzo 2011 presso l'EUROPOL, e, in particolare, i punti critici emersi, in relazione sia alla perdurante mancata attuazione di alcune raccomandazioni formulate nelle precedenti ispezioni, sia alle risultanze dei controlli effettuati, che hanno riguardato sei file di analisi, incluso quello relativo al *TFTP*, il sistema di informazione EUROPOL (EIS), l'accesso di

EUROPOL al SIS, il sistema di messaggistica SIENA, il sistema di analisi EUROPOL (EAS), nonché i dati relativi ai dipendenti.

Al termine della discussione si è deciso, come prassi, di inviare copia della bozza di rapporto, senza le raccomandazioni, ad EUROPOL, che ha potuto formulare eventuali commenti poi valutati nel corso della successiva riunione, il 28 settembre, quando è stato adottato il rapporto di ispezione con le relative raccomandazioni.

Si è anche discusso della possibilità di verificare le condizioni e le modalità di accesso delle unità nazionali ed è stato suggerito di sviluppare una metodologia comune e di redigere una *checklist* affinché le Autorità di protezione dei dati possano svolgere in maniera efficace le loro attività di supervisione e controllo.

Il Comitato ricorsi di EUROPOL si è invece occupato di due ricorsi, ritenendo per il primo di dover ulteriormente consultare EUROPOL. Per il secondo, è stata invece adottata una bozza di decisione, che rileva come EUROPOL non abbia rispettato il disposto dell'art. 19 della Decisione EUROPOL, non avendo provato che nella specifica ipotesi l'accesso alle informazioni da parte del richiedente avrebbe rischiato di compromettere l'attività della stessa EUROPOL.

Il Sistema informativo Schengen (SIS): attività dell'ACC

In occasione della riunione dell'ACC Schengen nei giorni 1° e 2 marzo 2011, è stato approvato il testo del questionario da inviare alle autorità nazionali competenti, come prima parte dell'azione comune da svolgere per verificare la legittimità delle segnalazioni inserite nel SIS in base all'art. 95 (mandato di arresto europeo) della Convenzione Schengen. Sono stati inoltre definiti i tempi per lo svolgimento della stessa azione comune, in modo che il rapporto finale dell'ACC possa essere redatto con le raccomandazioni eventualmente necessarie. L'attività è cominciata nel giugno 2011 ed è tuttora in corso. Se ne prevede il completamento entro il primo trimestre del 2012.

Rispetto alle precedenti verifiche, l'attività da un lato è risultata più onerosa, in quanto è stato richiesto di ispezionare un campione di segnalazioni fissato in relazione al numero complessivo di segnalazioni inserite da ciascun Paese (per l'Italia circa 200), ma dall'altro lato è stata facilitata dal fatto che fosse prevista una sola fonte di inserimento, il *SIRENE* (*Supplementary Information Request at the National Entry*, la banca dati che raccoglie le informazioni aggiuntive utili a dare seguito alle segnalazioni inserite nel SIS).

Nel frattempo è stata richiesta anche una verifica del seguito dato alle raccomandazioni contenute nel rapporto relativo alle segnalazioni di cui all'art. 99 della suddetta Convenzione.

Si registrano altresì progressi per quanto riguarda la preparazione dell'ispezione al sistema centrale C-SIS a Strasburgo.

Il Sistema informativo doganale (SID): *CIS Supervision Coordination Group* e ACC Dogane

Nella riunione del 1° e 2 marzo 2011, l'ACC Dogane ha organizzato un'ispezione al sistema centrale del Sistema informativo doganale (SID), da svolgersi con l'ausilio del Garante europeo della protezione dei dati (EDPS), a causa delle complicate basi giuridiche. L'ispezione ha avuto luogo il 12 e 13 ottobre 2011, il rapporto inviato in bozza all'Ufficio europeo per la lotta antifrode (OLAF) per commenti, è in via di adozione. L'attività ispettiva conferma che il sistema è poco usato (poco più di 200 file) e che tuttavia vi sono dati eccedenti quelli consentiti dalla base giuridica.

Nell'ambito della riunione dell'ACC Dogane è stato discusso un memo preparato dal segretariato, relativo all'impatto sulle competenze dell'ACC, della decisione quadro sulla protezione dei dati personali nell'*ex*-III Pilastro (Decisione quadro 2008/977/GAI).

Con i rappresentanti dell'EDPS, sono poi stati trattati i punti relativi all'organizzazione dell'ispezione del SID ed al manuale per l'utilizzo del FIDE (Archivio di identificazione dei fascicoli a fini doganali), tuttora in preparazione.

Quanto a quest'ultimo, si è previsto che i segretariati dell'ACC e dell'EDPS lavorino alla redazione di una *checklist*. È stata quindi preparata una bozza di parere congiunto che solleva, rispetto alla versione del manuale del 2009, questioni relative a: la possibilità di usare il FIDE come archivio nazionale, le modalità di accesso al SID per i pubblici ministeri, la possibilità di replicare l'archivio SID in quelli nazionali, i periodi di conservazione dei dati nel sistema.

Per quanto riguarda la riunione del CIS *Supervision Coordination Group* (Gruppo di coordinamento della supervisione del SID), il rappresentante dell'OLAF ha svolto un'interessante presentazione sul funzionamento del sistema FIDE e del relativo manuale, che però contiene un modello di tutela dei dati non soddisfacente. Inoltre, è stato rilevato che l'attuale base giuridica risulta troppo complicata, ed è allo studio un intervento normativo. Al riguardo, si registrano diverse ipotesi, che spaziano dal consolidamento del Regolamento

(CE) n. 515/97 del 13 marzo 1997 ed emendamento della Decisione 2009/917/GAI del 3 novembre 2009 (in particolare, la cancellazione dell'ACC Dogane e l'attribuzione delle competenze all'EDPS con poteri di coordinamento secondo il modello CIS) alla modificazione del solo regolamento, ovvero ancora al rinvio alla Direzione generale affari interni della Commissione europea della parte *ex*-III Pilastro del SID, che quindi non rientrerebbe più nelle competenze di OLAF.

È stato altresì discusso il programma di azione, da definire tendendo conto anche delle attività da svolgere in cooperazione con l'ACC Dogane.

18.4. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

Case Handling Workshop

Il 23° incontro del *"Case Handling Workshop"*, svoltosi a Varsavia il 4 e 5 ottobre 2011, è stato suddiviso in sessioni plenarie e sessioni parallele (la cui composizione ha tenuto conto delle dimensioni delle autorità) nelle quali sono stati discussi alcuni *case studies* relativi agli argomenti presentati in plenaria.

Il *workshop* in apertura è stato dedicato ai complessi temi della legge applicabile e della cooperazione tra le autorità in relazione ai casi transfrontalieri. Le differenze tra i poteri attribuiti a ciascuna autorità nell'ambito del proprio ordinamento e l'obbligatorietà o meno della risposta su casi singoli sono stati considerati tra i principali ostacoli di ordine "normativo" alla cooperazione. A ciò si aggiungono ostacoli di natura pratica, quali, ad esempio, la lingua da usare per la cooperazione e la fruibilità, per un'altra autorità, delle prove raccolte in lingua straniera.

Condivisa è stata l'esigenza di una struttura che possa occuparsi delle traduzioni attribuendo alle stesse un canone di ufficialità, che ne consenta l'utilizzo nei diversi Paesi europei, nonché di disporre di una lista aggiornata di punti di contatto all'interno delle singole autorità per facilitare la cooperazione.

Il *workshop* si è anche occupato del trattamento di dati *online*, sui *social network* e attraverso il *cloud computing*. Si è convenuto sulla necessità di adottare un *privacy impact assessment* (valutazione dell'impatto-*privacy*) che consenta di valutare i rischi derivanti dall'uso di tali sistemi ed individuare meglio le forme di tutela utili; sulla designazione come

responsabile del trattamento del soggetto che offre il servizio di *cloud* e sulla esigenza di rispettare le disposizioni in materia di trasferimento dei dati all'estero nel caso in cui i dati vengano trattati presso *server* situati fuori dal territorio dell'Unione europea.

È stato discusso in tale ambito anche il caso della Municipalità di Odense, in Danimarca, che, nel febbraio 2010, ha chiesto all'autorità di protezione dati un parere circa l'utilizzo del sistema *"Google apps"* da parte degli insegnanti per l'archiviazione e il trattamento di dati (anche sensibili) relativi ad alunni e genitori. La necessità di rispettare le disposizioni in materia di trasferimento dei dati all'estero (visto che *Google Ireland Ltd.* ha rappresentato di raccogliere i dati su *server* collocati anche negli Stati Uniti) e di adottare più compiute istruzioni da impartire al responsabile del trattamento e maggiori misure di sicurezza (ad es., ottenendo maggiori dettagli in ordine sia alle modalità di distruzione dei dati in caso di risoluzione del contratto, sia ai sistemi di *"logging"* per verificare eventuali accessi illeciti) sono stati i principali aspetti su cui si è soffermata l'autorità.

La terza sessione dei lavori ha consentito, tanto nella fase plenaria, con le presentazioni da parte dell'EDPS e delle Autorità della Svizzera, della Francia e della Polonia, quanto nell'ambito dei sottogruppi, di confrontare le diverse modalità ispettive adottate dalle autorità di protezione dei dati. Interessante è stata reputata, compatibilmente con le potenzialità dell'organico, la possibilità di verificare, a distanza di tempo, l'adeguamento del titolare del trattamento alle misure indicate dalle autorità a seguito di una prima ispezione.

Nel sottogruppo, l'autorità del Regno Unito (*Information Commissioner's Office-ICO*) ha presentato il proprio sistema di audit, illustrando brevemente le linee-guida adottate in materia nel mese di maggio 2011 e citando quale esempio la relazione dell'audit consensuale effettuato con *Google Inc.*, dopo l'illecita raccolta di dati effettuata nell'ambito di *Google Street View*. A seguito dell'audit (la cui relazione –come le altre– è disponibile sul sito dell'*ICO*), l'Autorità ha evidenziato alcuni aspetti positivi delle politiche di *privacy* della società e individuato alcuni punti da potenziare, come l'informativa agli utenti dei differenti servizi.

La sessione dedicata al trattamento dei dati personali in ambito lavorativo (tema che continua a interessare tutte le autorità alla luce dei numerosi casi da affrontare), ha consentito di illustrare alcuni casi recenti in materia di trattamento di dati biometrici (soprattutto

impronte digitali) sui luoghi di lavoro. Unanime la valutazione sulla difficoltà di utilizzare il consenso quale presupposto di legittimità del trattamento dei dati in tale contesto, alla luce della dubbia libertà del lavoratore nel rifiutarlo.

IWGDPT: Il "Gruppo di Berlino" - *International Working Group on Data Protection in Telecommunication (IWGDPT)*

Nel 2011, come di consueto, il "Gruppo di Berlino" si è riunito due volte: la prima a Montreal (4 e 5 aprile); la seconda a Berlino (12 e 13 settembre).

Per quanto riguarda la riunione di Montreal, si segnala l'adozione del paper *"Event Data Recorders (EDR) on Vehicles - Privacy and data protection issues for governments and manufacturers"*. Questo documento prende in esame i "registratori di dati evento" (dispositivi installati su alcune autovetture per registrare informazioni in caso di incidenti e in grado di memorizzare il verificarsi di avarie al motore o improvvisi cambiamenti della velocità delle ruote), tenendo conto della possibilità che essi consentono la periodica trasmissione delle informazioni registrate sul veicolo ad un soggetto esterno. Poiché tale registrazione comporta il trattamento di dati personali relativi al guidatore o ai passeggeri (es. velocità sostenuta, utilizzo o meno di cinture di sicurezza) che potrebbero essere trattati per diverse finalità (gestione dei sinistri da parte delle compagnie di assicurazione, offerta di servizi di emergenza, attività di *marketing*, repressione dei reati), il Gruppo, nell'auspicare al più presto un intervento normativo, ha fornito alcune preliminari raccomandazioni in materia di trasparenza, consenso dell'interessato, modalità del trattamento e misure di sicurezza.

I temi affrontati nella riunione di Berlino hanno spaziato dall'analisi delle implicazioni per la *privacy* derivanti dall'adozione del protocollo internet IPv.6, alle raccomandazioni rivolte ai gestori ed utilizzatori di sistemi come *e-Call* (dispositivi per la sicurezza degli autoveicoli), al *cloud computing*, all'accordo commerciale Ue-Stati Uniti in materia di lotta alla contraffazione e tutela della proprietà intellettuale, anche *online* (*Anti-Counterfeiting Trade Agreement*), fino alle indicazioni fornite alle competenti autorità in materia di micropagamenti effettuati *online* (in particolare tramite smartphones).

A proposito dell'utilizzo del protocollo IPv6, è stato evidenziato che la migrazione dall'attuale protocollo (IPv4) non sarà rapida e che è prevedibile un lungo periodo di coesistenza tra i due protocolli. Pur non essendo possibile esprimere un parere definitivo sulle implicazioni *privacy* del protocollo, che presenta aspetti favorevoli per gli utenti, derivanti

dall'abbondanza di indirizzi (come la possibilità di molteplici allocazioni di indirizzi per singola sessione), e svantaggi non trascurabili, quali la possibilità di dedicare porzioni degli indirizzi a dati ad elevato potere identificativo (quali gli indirizzi MAC dei terminali e dati di localizzazione), il Gruppo ha auspicato un'applicazione quanto più possibile uniforme su scala globale del protocollo IPv6 e dei meccanismi di conversione IPv4-IPv6.

Relativamente al tema del *cloud computing*, il Gruppo ha individuato nella *"loss of control"* (perdita di controllo) da parte del titolare, il principale problema per l'introduzione su larga scala di questo nuovo servizio. Al fine di restituire al titolare un maggiore potere di controllo sul *provider*, il Gruppo ha auspicato l'introduzione, come strumento immediato di intervento, di meccanismi di *"location audit"* che consentano l'accertamento –da parte del titolare– sia della localizzazione dei *server* in cui sono conservati i dati, sia della *"applicable law"*, con particolare riferimento ai soggetti che possono avere accesso ai dati. Sull'argomento, i rappresentanti del Garante hanno illustrato l'avanzamento di nuove tecniche crittografiche (*Homomorphic Encryption*) in grado di consentire trattamenti direttamente su dati cifrati, senza che il *provider* sia a conoscenza dei dati trattati, che potrebbero innalzare il livello di fiducia sull'impiego dei servizi di *cloud computing*.

Il Gruppo ha inoltre raccomandato ai governi nazionali e alle autorità competenti di consentire l'effettuazione di micropagamenti elettronici in forma anonima, ovvero attraverso l'impiego di pseudonimi, onde evitare forme occulte di tracciamento legate ai beni o servizi acquistati tramite tali modalità di pagamento (spesso per somme minime o assai contenute); essenziale anche la previsione di adeguate informative per gli utenti, che illustrino i rischi associati a tali modalità.

Le riunioni hanno permesso di rappresentare novità o sviluppi nazionali di possibile interesse comune. In particolare, i rappresentanti del Garante hanno illustrato il provvedimento sull'invio di fax originati da apparecchi situati al di fuori del territorio nazionale [doc. *web* n. 1810207] ed i punti principali della campagna informativa sul tema *cloud computing* (documento annesso alla relazione annuale 2010), prima iniziativa di *"awareness raising"* rivolta alle imprese intrapresa da un'autorità di protezione dati. È stato illustrato anche il documento del Garante sul diritto all'oblio e sull'applicazione a tale scopo del protocollo