inviare annunci modificando le impostazioni del *browser* o inserendo icone sul *desktop* dello *smartphone*. Tutti questi requisiti divengono ancora più pressanti per *app* rivolte (anche solo potenzialmente) ai minori per le quali vi sono obblighi più stringenti rispetto al consenso, all'informativa, ed alla scelta di modalità e linguaggi idonei a far comprendere ai soggetti minorenni la natura e gli scopi dei trattamenti previsti. Qui lo schema di parere fa appello alla creatività degli sviluppatori e distributori di *app*, che sono in grado di individuare gli approcci più idonei a tale scopo.

Parere sugli sviluppi nelle tecnologie biometriche

Attraverso il parere sugli sviluppi nelle tecnologie biometriche (Parere n. 3/2012 - WP 193 [doc. web n. 2375294]) è stato fornito un quadro aggiornato di linee-guida generali e di raccomandazioni sull'applicazione dei princìpi di protezione dei dati in ambito biometrico.

Il parere, rivolto alle autorità legislative europee e nazionali, all'industria dei sistemi biometrici e agli utenti di tali tecnologie, si sofferma sulle definizioni pertinenti del settore, sui princìpi fondamentali di protezione dei dati (finalità, proporzionalità, accuratezza, minimizzazione, sicurezza, criteri di legittimità del trattamento), sui nuovi sviluppi e tendenze in ambito biometrico e, anche attraverso specifici esempi, indica misure tecniche e organizzative per attenuare i rischi per la protezione dei dati e la vita privata dei cittadini europei.

Riconoscimento facciale

Con specifico riferimento al tema del riconoscimento facciale, un ulteriore approfondimento è stato condotto dal Gruppo Art. 29 (Parere n. 2/2012 - WP 192 [doc. web n. 2375284]) in relazione alle applicazioni *online* e di telefonia mobile. Il testo mette in luce i rischi di tali tecnologie, con particolare riguardo alla tipologia di dati trattati e alle finalità del trattamento e chiarisce che sono dati personali sia le immagini digitali, se contengono il volto visibile di una persona, sia i "modelli" (*templates*) ricavati dal trattamento delle immagini stesse. Il riconoscimento facciale può essere dunque effettuato solo nel rispetto dei princìpi fondamentali in materia di protezione dei dati, in particolare informando chiaramente gli utenti sui trattamenti previsti ed ottenendo il loro preventivo consenso in caso di "taggatura" delle immagini, sicché un utente non registrato o che non abbia dato il consenso non potrà essere "taggato" automaticamente in un *social network*. Per altro verso, sono possibili senza consenso alcune operazioni di trattamento fondate sull'interesse legittimo del titolare: ad es., un *social network* deve poter effettuare alcune operazioni

sull'immagine del volto per stabilire se una persona sia già "conosciuta" dal servizio ed abbia o meno acconsentito al "*tagging*" o ad ulteriori trattamenti. È indispensabile, infine, che siano adottate misure di sicurezza sia per la conservazione delle immagini che per il loro trasferimento in rete attraverso sistemi di cifratura.

I rapporti con Google

Va altresì segnalata una serie di iniziative che, a vari livelli, hanno riguardato i rapporti fra le autorità europee di protezione dati e Google Inc..

In primis, occorre menzionare la modifica apportata il 1° marzo 2012 da Google Inc. alla propria *privacy policy*, che prevede in via generalizzata la possibilità di incrociare e combinare dati relativi a più servizi offerti da Google. Il Gruppo Art. 29 ha deciso di valutare la conformità della nuova *privacy policy* con la normativa europea in materia di protezione dati, attraverso un'azione congiunta coordinata dall'Autorità francese per la protezione dei dati (CNIL). Google ha collaborato allo svolgimento di tali accertamenti rispondendo a due questionari inviati dalla CNIL rispettivamente il 19 marzo e il 22 maggio 2012, spiegando, fra l'altro, che molte delle prassi seguite in materia di *privacy* non si discostano da quelle di altre aziende statunitensi operanti su internet. Tuttavia, l'analisi delle risposte ai questionari ha evidenziato numerose problematiche con riguardo al mancato rispetto da parte della società americana di princìpi basilari della protezione dati. In primo luogo, gli accertamenti hanno dimostrato che Google non fornisce sufficienti informazioni agli utenti, in particolare rispetto alle finalità ed alle categorie di dati oggetto di trattamento. Ne consegue che l'utente non è in grado di stabilire quali categorie di dati siano trattate per il servizio di cui sta usufruendo, e per quali scopi tali dati siano trattati. In secondo luogo, gli accertamenti hanno confermato i rischi legati alla combinazione di dati tratti da servizi spesso molto diversi. La nuova *privacy policy* permette a Google di combinare sostanzialmente qualsiasi dato tratto da qualsiasi servizio per qualsivoglia finalità, ma in molti casi manca un'idonea base giuridica: talora manca il consenso inequivocabile dell'utente, oppure viene considerato erroneamente prevalente l'interesse legittimo di Google ad effettuare una raccolta massiva di informazioni, o non esiste alcun fondamento contrattuale per i trattamenti e gli incroci di dati effettuati. Resta da dimostrare, in molti casi, che i dati raccolti siano proporzionati agli scopi del trattamento:

Google non ha posto alcun limite ai possibili incroci di dati né ha fornito agli utenti strumenti che consentano loro di mantenere il controllo su tali operazioni di trattamento. Per tutti questi motivi, il 16 ottobre 2012 il Gruppo ha rivolto a Google in via ufficiale varie raccomandazioni per migliorare le informative, chiarire le modalità di incrocio dei dati e, più in generale, garantire l'osservanza delle norme e dei princìpi in materia di protezione dei dati con meccanismi semplificati di opposizione, raccolta del consenso espresso ai fini della combinazione di dati per determinate finalità, limitazione degli incroci di dati relativi ad utenti passivi. Il Gruppo ha concesso un periodo di quattro mesi a Google per le proprie valutazioni [doc. web nn. 2375141 e 2375151].

Bisogna ricordare in questa sede anche il contenzioso che oppone Google Inc. all'Autorità spagnola di protezione dati (APD), nel quale la Corte Suprema spagnola (*Audiencia Nacional*) ha formulato un rinvio pregiudiziale alla Corte di giustizia UE, al fine di stabilire se Google Inc. sia tenuta a rispondere alle richieste di cittadini spagnoli di cancellare i dati contenuti nelle stringhe di ricerca, e in che modo tale diritto all'oblio debba eventualmente essere esercitato. Secondo Google, che non riconosce l'applicabilità della normativa UE (e spagnola) così come sancita delle disposizioni di cui all'art. 4(1)c. della Direttiva n. 95/46/CE, la competenza esclusiva è delle autorità giudiziarie statunitensi. Il caso nasce da un ricorso presentato all'APD con riguardo alla pubblicazione di una notizia su un quotidiano, risalente a vari anni prima, che continuava ad apparire fra i risultati della ricerca effettuata digitando il nominativo della persona interessata. L'APD ha attribuito la responsabilità di agire per tutelare il diritto all'oblio a Google Inc. (tramite Google *Spain*) che invocando la propria natura di mero intermediario, ha negato la propria responsabilità per i contenuti raccolti in rete dal motore di ricerca. In una nota esplicativa dell'APD si evidenzia come la *Audiencia Nacional* sottolinei la necessità di un'interpretazione che prescinda dalla localizzazione dello strumento eventualmente utilizzato dal titolare *extra*-UE e, piuttosto, tenga conto dell'intera costellazione di elementi che formano il trattamento in oggetto, alla luce della natura di diritto fondamentale che ha assunto la protezione dei dati; secondo l'*Audiencia Nacional* dovrebbe prevalere il criterio del "*centro di gravità del conflitto*" tenendo conto di tutti gli interessi in gioco e delle norme implicate.

ICANN e registro *Whois*

Uno scambio di lettere fra il Gruppo Art. 29 e l'ICANN *(Internet Corporation for Assigned Names and Numbers,* con sede negli USA -ossia l'organismo di diritto privato- che assegna i nomi al dominio) ha permesso di evidenziare una serie di problematiche legate alla revisione di alcuni accordi ("*Registrar Accreditation Agreement, RAA*" e "*RAA Negotiations Summary Memo*") che disciplinano le modalità di registrazione e di accesso alle informazioni (dati identificativi di contatto per la gestione tecnica dei siti web) contenute nel registro denominato "*Whois*". Il Gruppo ha evidenziato le criticità relative alle forti pressioni di autorità giudiziarie e di polizia (USA e non solo) per accedere ai dati *Whois*, nonché alla possibile aggiunta, e verifica periodica, di informazioni ulteriori quali numero telefonico e indirizzo e-mail del registrante. Inoltre, il Gruppo ritiene sproporzionato l'allungamento dei tempi di conservazione dei dati contenuti in *Whois* (24 mesi) dopo la cessazione del contratto relativo ad un dominio web. Da parte sua, ICANN ha risposto che queste tematiche sono in corso di trattazione da parte della *Government Advisory Committee (GAC)* dell'ICANN stesso, di cui fa parte anche un rappresentate della Commissione europea, e che pertanto occorre assicurare il coordinamento con il rappresentante della Commissione al fine di segnalare in modo appropriato le criticità relative alla revisione del *RAA*. Inoltre, ICANN ha dichiarato che sarà aggiornato anche il meccanismo relativo ai casi in cui il *RAA* confligga con la normativa *privacy* (anche nazionale) del registrante, tramite la previsione di specifiche deroghe.

La nuova attività congiunta sui temi *Borders, Travel* e *Law Enforcement*

Nel 2012, il Gruppo Art. 29 ha dato il via all'attività del sottogruppo *Borders, Travel and Law Enforcement subgroup* (BTLE), sulle tematiche connesse al trattamento di dati nel settore di polizia e giustizia (*ex* III Pilastro), in seguito alla soppressione del WPPJ nel corso della *Spring Conference* 2012 e in ragione dell'unificazione dei pilastri dell'Unione dopo l'entrata in vigore del Trattato di Lisbona (v. *infra Spring Conference* 2012).

In tale quadro il Gruppo Art. 29 ha seguito l'andamento della discussione al Parlamento europeo della proposta presentata dalla Commissione per l'introduzione di un sistema europeo di raccolta e trattamento dei dati dei passeggeri aerei (EU PNR - *Passenger Name Record*) ed ha espresso, insieme al Consiglio, Commissione e Parlamento, forti preoccupazioni in relazione al possibile accordo PNR con il Canada.

Si segnalano inoltre le lettere inviate dal Gruppo alla Commissaria Malmström il 12 giugno 2012 [doc. web nn. 2375181 e 2377470], per esprimere le proprie preoccupazioni in merito ai profili di protezione dati delle proposte della Commissione contenute nella comunicazione in materia di *smart borders* ("frontiere intelligenti", COM(2011) del 25 ottobre 2011) ed alla proposta di regolamento che istituisce un sistema europeo di sorveglianza delle frontiere (Eurosur: frontiere sud dell'Unione con i Paesi del bacino mediterraneo COM(2011) 873 del 12 dicembre 2011). Entrambi i sistemi hanno come finalità principale la lotta all'immigrazione clandestina ed il miglioramento del controllo delle frontiere dell'UE, anche con dispositivi elettronici.

Quanto, poi, agli specifici argomenti di *law enforcement* si menziona l'accordo del 28 giugno 2010 tra l'Unione europea e gli Stati Uniti sul trattamento e il trasferimento di dati di messaggistica finanziaria, per il controllo delle transazioni finanziarie dei terroristi *(Terrorist Finance Tracking Program).* La seconda revisione congiunta delle modalità di funzionamento dell'accordo si è svolta il 29 e 30 ottobre 2012 con la presenza, per le autorità di protezione dati, di rappresentanti delle Autorità dei Paesi Bassi e del Belgio. Gli Stati Uniti hanno rappresentato in quale modo le varie disposizioni dell'accordo siano rispettate. Non sono stati forniti ulteriori dettagli sui risultati della verifica congiunta, né sulle informazioni ricevute dagli Stati Uniti. Tuttavia, il delegato della DPA dei Paesi Bassi ha espresso le proprie perplessità sulle modalità di funzionamento dell'accordo: il *focus* negli USA è spostato "dai dati alle persone" e ciò desta non poche preoccupazioni -condivise dal Gruppo- in termini di controllo e profilazione degli individui.

In relazione poi, all'accesso alle cd. "informazioni classificate", è stato fatto circolare tra le delegazioni del Gruppo Art. 29 un questionario, al quale il Garante ha risposto illustrando, in particolare, gli obblighi di segretezza gravanti sul personale addetto all'Ufficio del Garante e sui suoi consulenti (v. art. 156, comma 8 del Codice).

Protezione dei dati in ambito finanziario

Nel 2012 il Gruppo Art. 29 ha continuato ad occuparsi del trattamento dei dati in ambito finanziario, con particolare riferimento all'attuazione della legislazione statunitense per il contrasto delle frodi fiscali (cd. "*off shore Foreign Account Tax Compliance Act*", FATCA); all'attuazione degli accordi di cooperazione internazionale "*Public Companies Accounting*

Oversight Bodies" (PCAOB) stipulati tra Stati Uniti e Stati membri dell'Unione europea; alla revisione della legislazione in materia di contrasto alle attività di riciclaggio e finanziamento del terrorismo.

Con riferimento alla legislazione statunitense FATCA -che introduce l'obbligo di rilevare specifici dati dei clienti cittadini statunitensi da parte di istituti finanziari ed assicurativi insediati nell'Unione europea, e di trasferire tali dati all'amministrazione fiscale degli Stati Uniti, per contrastare l'evasione fiscale da parte di "*US persons*"- è stato dato particolare rilievo al problema generale della sua applicabilità *extra*-territoriale nei Paesi membri dell'Unione europea.

La legittimità del criterio previsto per l'applicazione delle disposizioni in parola (titolarità di conti o polizze assicurative da parte di "*US persons*") non è risultata chiara, anche in quanto la legislazione è stata adottata "in via unilaterale", al di fuori dei *fora* internazionali (OCSE), e sembrerebbe non in linea con i vigenti accordi internazionali per la prevenzione della doppia imposizione fiscale.

Oltre alla mancanza di un'idonea base giuridica per il trattamento dei dati personali da parte dei titolari nell'Unione europea, il Gruppo ha considerato le criticità derivanti dall'applicazione di FATCA anche alle società di assicurazione.

Circa la sopravvenuta conclusione, da parte del Dipartimento del Tesoro degli Stati Uniti di un accordo (al quale aderiscono Italia, Spagna, Germania, Francia, Regno Unito), preliminare alla conclusione di accordi bilaterali ed aperto alla successiva adesione di altri Stati membri, è stata sottolineata la necessità di definire con precisione le misure di protezione dei dati personali, i diritti degli interessati, l'ambito dei soggetti obbligati, esentando le operazioni a basso rischio (come quelle svolte dalle società assicurative), ed evidenziata altresì, l'opportunità di assicurare la reciprocità degli obblighi di cooperazione tra Stati membri dell'Unione europea e Stati Uniti.

Il Gruppo ha, quindi, segnalato alla Commissione europea (lettera 21 giugno 2012 [doc. web n. 2375072]) come possibile, benché più problematica, base giuridica per il trattamento dei dati personali anche il contratto/*agreement* tra operatori finanziari e amministrazione tributaria USA. In particolare, rispetto al precedente "approccio unilaterale" statunitense è

stato considerato preferibile un sistema basato sul trasferimento dall'autorità fiscale nazionale competente all'omologa autorità statunitense dei soli dati personali rilevanti, sulla base di accordi bilaterali tra Stati Uniti e Stato membro dell'Unione europea (cd. "*model I agreement*"). Maggiori criticità sono state invece ravvisate nell'opzione che prevede il trasferimento diretto dei dati dagli operatori finanziari al Dipartimento del Tesoro degli Stati Uniti (cd. "*model II agreement*"). Il Gruppo si è comunque riservato la possibilità di esaminare tali accordi in seguito.

Quanto agli accordi di cooperazione internazionale PCAOB stipulati tra Stati Uniti e Stati membri dell'Unione europea, nel corso della plenaria di dicembre 2012 il Gruppo ha raccomandato alla Direzione Generale mercato interno della Commissione europea (v. lettera del 13 dicembre 2012 [doc. web n. 2375161]) il ricorso da parte delle competenti autorità degli Stati membri ad un "protocollo *standard*" (*agreement for the exchange of information*) predisposto dalla Commissione europea, accompagnato da un protocollo addizionale contenente misure idonee ad assicurare la protezione dei dati personali, aggiuntive rispetto a quelle prescritte nel precedente parere del Gruppo Art. 29 (parere 10/2007 - WP 143). È stato inoltre predisposto un questionario, successivamente trasmesso dalla Commissione europea alle autorità nazionali competenti, per ottenere informazioni in merito allo *status* degli accordi (*Memorandum of Understanding*, cd. "MoU") eventualmente stipulati o in corso di elaborazione da parte delle autorità di controllo europee (in Italia, la Consob) con il PCAOB, anche al fine di valutare la conformità di tali accordi alle misure proposte nel precedente parere del Gruppo Art. 29.

Trasferimento dati all'estero

Nel 2012 sono stati oggetto di particolare attenzione i trasferimenti effettuati dai gruppi multinazionali d'impresa (mediante il perfezionamento di norme vincolanti d'impresa cd. "*Binding corporate rules for controller*") e quelli effettuati nell'ambito di forme di esternalizzazione delle attività di trattamento dei dati (v. le clausole contrattuali tipo 87/2010/UE, da titolare a responsabile, approvate dalla Commissione europea).

In merito, è stata condivisa l'esigenza manifestata dal mondo dell'impresa di disporre di un sistema semplificato per i flussi transfrontalieri di dati gestiti da società multinazionali di servizi, in grado di ricomprendere anche il caso (non contemplato dalle clausole contrattuali

tipo 87/2010/UE), in cui il responsabile sia stabilito in uno Stato membro. A tal fine è stato elaborato un nuovo modello di norme vincolanti d'impresa definito *Bcr for processor*.

Lo strumento è concepito su un doppio livello: il cliente (titolare) sottoscrive un contratto generale di servizi (*Service Level Agreement* - SLA) con la società multinazionale (responsabile); il contratto impegna le parti al rispetto di una serie di clausole tra le quali sono ricomprese le *Bcr for processor* (allegate allo SLA). Tramite le *Bcr for processor*, la società multinazionale ha la possibilità di "sub-appaltare" le attività di trattamento (o alcune fasi di esso) alle proprie consociate o affiliate anche stabilite in Paesi terzi, senza necessità di ulteriori formalità (quali ad es., autorizzazioni *ad hoc*, *standard contractual clauses*).

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 in UE, rispetto dei princìpi della Direttiva n. 95/46/CE, impegno per il gruppo multinazionale di impresa a dotarsi di un sistema di *training*, a disporre di una struttura specializzata nella gestione delle segnalazioni degli interessati e a svolgere *audit* periodici sul rispetto dei princìpi di protezione dati da parte delle proprie affiliate. Il testo è stato adottato nel giugno 2012 (*Working Document* n. 02/2012 - WP 195 del 6 giugno 2012 [doc. web n. 2375532]).

Sempre in tema di trasferimento di dati all'estero, è stato adottato un parere che ritiene adeguato il livello di protezione dei dati personali nel Principato di Monaco (Parere 7/2012 - WP 198 [doc. web n. 2133808]) dopo aver attentamente valutato, in collaborazione con l'autorità locale (*Commission de Contrôle des Informations Nominatives* - CCIN) i criteri e i princìpi della normativa monegasca rispetto all'applicazione degli artt. 25 e 26 della direttiva europea.

Il Gruppo, con lettera del 3 marzo 2012 ha inoltre sollecitato la Commissione ad adottare le decisioni di esecuzione sull'adeguata protezione dei dati personali della Repubblica orientale dell'Uruguay e della Nuova Zelanda, rispettivamente sulla base dei pareri favorevoli del 12 ottobre 2010 (WP 177) e 4 aprile 2011 (WP 182), poi adottate il 21 agosto e il 19 dicembre 2012.

21.4. LA COOPERAZIONE DELLE AUTORITÀ NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Come riferito sopra, nel 2012 il Gruppo di lavoro Polizia e Giustizia (*Working Party on Police and Justice* - WPPJ) ha terminato i suoi lavori in seguito alla decisione presa dalla Conferenza europea delle autorità garanti svoltasi a Lussemburgo (v. *supra*). Le sue funzioni sono assorbite nelle competenze del Gruppo Art. 29, in particolare attraverso il sottogruppo BTLE, mentre sarà la Conferenza stessa, laddove necessario, a definire le modalità di intervento delle autorità europee su temi di più ampia rilevanza.

Si segnala inoltre l'entrata in vigore del VIS (Sistema informativo visti) che comporta una nuova attività di supervisione e controllo sulla legittimità dei trattamenti di dati da parte del Garante sia a livello nazionale, sia a livello europeo, attraverso il Gruppo di supervisione formato dalle autorità europee e dal Garante europeo, quale Autorità di controllo delle attività svolte da istituzioni ed organismi dell'Unione.

Si è riferito sopra anche della proposta di direttiva riguardo i trattamenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, che dovrebbe sostituire la Decisione quadro n. 2008/977, adottata prima dell'entrata in vigore del Trattato di Lisbona e che riguardava soltanto i princìpi necessari per consentire gli scambi di informazioni.

È comunque proseguita l'attività di supervisione e controllo svolta nelle Autorità comuni e nei Gruppi di supervisione già istituiti e menzionati nelle precedenti Relazioni.

Europol: l'attività dell'Autorità di controllo comune [Acc] e del comitato ricorsi

Nella riunione del 14 marzo 2012 è stato adottato il secondo rapporto d'ispezione sul trattamento da parte di Europol delle richieste di dati relativi a transazioni finanziarie europee, provenienti dal Tesoro americano in base all'Accordo UE-USA del 28 giugno 2010 per le esigenze del programma TFTP. Poiché gli atti relativi allo stesso accordo sono classificati come segreti, l'Acc ha deciso per ragioni di trasparenza di redigere la cd. "parte pubblica del rapporto" presentata con un breve comunicato stampa il 21 marzo 2012 [doc. web nn. 2375032 e 2375320]).

Per quanto riguarda il trattamento dati effettuato dalla Acc Europol (con riferimento agli archivi di analisi, al sistema di indice, al sistema di trasmissione dei dati), l'ispezione annuale presso la sede di Europol a L'Aja è stata svolta anche con la partecipazione di un esperto

tecnico del Garante. Alcune criticità riscontrate riguardano il sistema di trasmissione dati SIENA (che viene proposto come sistema generale di trasmissione per le comunicazioni tra Stati membri e per il quale Europol agisce come *service provider*) che necessiterebbe di una specifica base giuridica per definire adeguatamente ruoli, compiti e regole di accesso ai dati da parte dell'organizzazione. Il rapporto finale, adottato dall'Acc, contiene una serie di raccomandazioni in tal senso.

A completamento delle informazioni raccolte attraverso le ispezioni cd. "centrali" presso l'Europol, considerato il ruolo svolto dagli Stati attraverso le informazioni che inviano per l'analisi o per il sistema indice, l'Acc ha deliberato di verificare le condizioni di funzionamento degli uffici nazionali incaricati di scambiare informazioni con Europol. La verifica deve essere svolta in modo coordinato con una metodologia uniforme, predisposta dal segretariato ed approvata dall'Acc. Entro la prima metà del 2013 verrà pubblicato un rapporto con le risultanze delle verifiche e le raccomandazioni ritenute necessarie.

Nella riunione di dicembre 2012, l'Acc ha definito le tipologie di trattamenti che saranno oggetto dell'ispezione annuale, in programma nel marzo 2013; ha rinnovato il mandato al responsabile del *team* di ispezioni ed ai componenti (di cui fa parte un esperto tecnico del Garante) e deciso di includere nell'ordinaria ispezione annuale gli aspetti relativi al trattamento dati TFTP.

L'Acc ha, infine, adottato 2 pareri [doc. web nn. 2375221 e 2381001] sul livello di protezione dei dati in Serbia ed in Liechtenstein e un parere sull'accesso di Europol ad Eurodac [doc. web n. 2375211]; inoltre ha discusso aspetti relativi allo sviluppo del sistema di messaggistica SIENA ed adottato in principio il rapporto di attività relativo agli anni 2008-2012.

Il Comitato ricorsi non ha avuto riunioni nel 2012 e ciò perché la nuova risposta *standard* alle richieste di accesso, in caso di non esistenza di dati presso l'organizzazione, in linea con quanto suggerito più volte dall'Acc, sembrerebbe fornire elementi più chiari, sicché gli interessati non hanno presentato ricorsi all'Acc.

Il Sistema Informativo Schengen: l'attività dell'Autorità di controllo comune [Acc] Schengen

Nel 2012 è proseguita la valutazione delle risposte pervenute al segretariato sull'attività di verifica svolta a livello nazionale dalle autorità di protezione dati, relativamente alla legittimità delle segnalazioni inserite nel Sistema Informativo Schengen (SIS), per quanto

necessario a fini del mandato di arresto europeo. L'Acc, in vista della discussione della bozza del rapporto conclusivo, ha chiesto al segretariato di prendere contatti con l'Acc Eurojust per eventuali valutazioni e contributi.

Quanto alle segnalazioni a fini di non ammissione, ai sensi dell'art. 96 della Convenzione Schengen, l'Acc ha deciso di segnalare alla Commissione europea il conflitto tra le norme della Convenzione medesima, che richiedono una attenta e documentata decisione, caso per caso, sull'inserimento della segnalazione nel SIS -oltre che negli archivi nazionali- ed il divieto di ingresso regolato dalla direttiva "rimpatri" (Direttiva n. 2008/115/CE) che introduce invece un automatismo nell'inserimento delle segnalazioni [doc. web n. 2375381].

L'Acc ha anche adottato pareri in merito alla proposta di introdurre una funzione *SEarCH* nel SIS, ritenuta non necessaria in quanto già sviluppata in altri gruppi di lavoro ed alla migrazione dall'attuale SIS 1+ al SIS II.

L'entrata in funzione del SIS II, le cui basi giuridiche sono state adottate fin dal 2006, in programma per la primavera del 2013, comporterà anche la decadenza dell'Acc essendo prevista una diversa forma di supervisione comune, simile a quella istituita per altri sistemi di informazioni europei come Eurodac e Vis. Poiché la transizione potrebbe avere una durata maggiore del preventivato, il parere dell'Acc richiama l'attenzione della Commissione -che gestirà il nuovo sistema con l'Agenzia- sulla necessità di evitare vuoti nella supervisione e controllo dei trattamenti durante la fase transitoria.

Il Sistema informativo doganale [Sid]: Cis Supervision Coordination Group e attività dell'Acc

L'attività dell'Acc Dogane è stata nel 2012 limitata ai temi correnti mentre si sta sviluppando quello del Cis *"Supervision Coordination Group"* (Gruppo di coordinamento della supervisione del Sid). Al riguardo la Commissione ha comunicato che si sta predisponendo una modifica degli strumenti normativi esistenti, che è stato redatto un primo rapporto sull'impatto dell'intervento, che dovrà, una volta approvato dal *board* della Commissione, essere presentato alla consultazione interservizi, entro il luglio del 2013. La proposta dovrebbe contenere norme sulla supervisione ben coordinate e senza ambiguità.

L'Acc Dogane aveva al riguardo stimolato l'azione della Commissione al fine di valutare la necessità del mantenimento di una Autorità comune di supervisione e controllo sulla

legittimità dei trattamenti dei dati nel Sid, data l'esiguità dei dati scambiati nel sistema e la netta preferenza delle amministrazioni doganali per i canali bilaterali di cooperazione.

Gruppo di supervisione Vis (Sistema informativo visti)

Il Gruppo di coordinamento e supervisione Vis è stato istituito dall'art. 43 del Regolamento (CE) n. 767/2008 per monitorare la liceità del trattamento dei dati personali sia da parte delle autorità di gestione nazionali, sia da parte dell'Autorità di gestione del Vis centrale, anche attraverso periodici *audit* di controllo. Il Gruppo ha tenuto la sua prima riunione, provvisoriamente diretta dal Garante europeo per la protezione dei dati P. Hustinx, il 21 novembre 2012.

Nel corso della riunione si è approvata una prima bozza di regolamento preparata dal segretariato in via provvisoria con riserva delle modifiche richieste da alcune delegazioni. Si è anche deciso di posporre la nomina del presidente alla prossima riunione e si è accolta la richiesta presentata dall'Irlanda di poter prender parte alla riunione in qualità di osservatore. Per la successiva riunione -prevista nella primavera del 2013- sarà autorizzata anche la presenza del rappresentante del Regno Unito (che, con l'Irlanda non è parte della cooperazione Schengen). Rappresentanti della Commissione hanno informato sullo sviluppo graduale del sistema, per regioni del mondo predefinite in base a decisioni della Commissione, che dovrebbe essere completato per la seconda metà del 2013, nonché sul trasferimento di competenze per la gestione operativa del VIS centrale (C-VIS) dalla Commissione all'Agenzia appositamente creata (*Large scale IT Agency*).

Il Gruppo Vis ha poi discusso con l'EDPS (Garante europeo per la protezione dei dati) dei risultati dell'*audit* eseguito sul sistema e sul seguito dato dalla Commissione alle raccomandazioni formulate. Sono state presentate esperienze di visite e verifiche svolte in alcuni consolati da parte delle Autorità di protezione dei dati della Svizzera e della Francia (basate anche sulla verifica degli obblighi previsti dalla Convenzione Schengen).

Si è inoltre discussa la bozza del programma di attività per il biennio 2013-2014 e si è convenuto di prevedere, nel rispetto del regolamento Vis (Regolamento CE n. 767/2008 del 9 luglio 2008), coordinate attività di verifica sia sul sistema centrale sia sulle parti nazionali del Vis (inclusa la verifica del modo in cui le forze dell'ordine hanno accesso ai dati secondo quanto previsto dalla Decisione n. 633 del 2008), garantendo però che le relative decisioni

siano prese nel rispetto delle priorità nazionali di ciascuna autorità. Questo anche con riferimento alla frequenza e alle modalità di riunione del Gruppo, che dovrà coordinarsi con il Gruppo Eurodac e con le altre forme di supervisione comune, per evitare sovrapposizioni di date e di concomitanti richieste di svolgere accertamenti nazionali.

Gruppo di supervisione Eurodac

Nel maggio 2012 il Gruppo di supervisione Eurodac, istituito per verificare la legittimità del trattamento dei dati nel sistema Eurodac (contenente le impronte digitali dei richiedenti asilo nei Paesi UE) ha conferito un secondo mandato di Presidente e Vicepresidente a P. Hustinx ed E.Wallin.

Il Gruppo ha discusso, tra l'altro, il progetto della Commissione relativo al regolamento Eurodac, che consentirebbe l'accesso ai dati contenuti in Eurodac alla forze di polizia. In merito, anche i rappresentanti dell'UNHCR (Alto Commissariato delle Nazioni Unite per i rifugiati), presenti alla riunione di maggio, hanno espresso le loro preoccupazioni rispetto alla proposta, che consente ricerche, a fini di polizia, anche a partire da frammenti di impronta ritrovati sulla scena del crimine. L'accesso ai dati sarà consentito a polizia, inquirenti e ad Europol solo qualora dall'interrogazione delle esistenti banche dati di polizia non emergano riscontri. Tale limitazione è stata peraltro ritenuta non sufficiente. La proposta, presentata il 30 maggio 2012 (COM(2012) 254 definitivo) è stata discussa in incontri trilaterali anche con il Parlamento ed il Consiglio.

Il Gruppo ha poi adottato il rapporto di attività per gli anni 2010 e 2011 [doc. web n. 2375052].

Sulla scorta di lavori pilota svolti da alcune delegazioni, il Gruppo ha messo a punto un piano di ispezione standardizzato, da utilizzare a livello nazionale per l'attività di supervisione e controllo attribuita dal regolamento Eurodac.

Nel 2012, il Gruppo di supervisione Eurodac ha anche svolto verifiche sul trattamento delle impronte digitali illeggibili e sulle eventuali conseguenze sulla procedura di asilo. Infatti, dal momento che il regolamento Eurodac prevede l'inserimento delle impronte nel sistema per verificare se corrispondono ad altre già contenute, il fatto che la persona non abbia impronte digitali "leggibili" dalle macchine usate (*live scan)* non può influire sull'accesso alla procedura di asilo poiché questo comporterebbe l'introduzione di un

ulteriore requisito -la presenza di impronte digitali leggibili- non previsto dal Regolamento "Dublino" di cui il Sistema Eurodac è servente. Il Gruppo ha inoltre cominciato una riflessione sul programma di lavoro per il biennio 2013-2014, nel corso della quale sono emerse preoccupazioni sul crescente carico di lavoro e quindi sull'opportunità di ridurre e rendere sinergiche le richieste di attività da svolgere a livello nazionale, come evidenziato anche in riferimento ai lavori del Gruppo VIS.

In ogni caso il programma di lavoro potrà essere definito solo una volta adottata la nuova base legale, dovendosi fissare tempi e forme per l'esercizio di una efficace supervisione a livello centrale sulla banca dati ed a livello nazionale sull'inserimento dei dati e l'uso del sistema da parte degli Stati.

21.5. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

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

La 51ª e 52ª riunione dell'*International Working Group on Data Protection in Telecommunications* (Gruppo di Berlino) si sono svolte il 23 e 24 aprile 2012 a Sopot (Polonia) e 10 e 11 settembre a Berlino.

Nel corso della prima riunione il Gruppo ha adottato un documento di lavoro (*Sopot Memorandum*) [doc. web n. 2375062], che contiene raccomandazioni generali volte a ridurre i rischi associati all'utilizzo del *cloud* ed a promuoverne uno sviluppo responsabile. In particolare il Gruppo raccomanda che: il *cloud computing* sia accompagnato da un livello di tutela di dati personali adeguato e non inferiore a quanto previsto negli altri ambiti; i titolari del trattamento valutino preliminarmente l'impatto di tali tecnologie sui diritti delle persone; i fornitori di servizi di *cloud* sviluppino pratiche in grado di garantire trasparenza, sicurezza e fiducia, in particolare fornendo informazioni su possibili violazioni dei dati (*data breach)* e favorendo la portabilità e il controllo dei dati da parte degli utenti; siano incentivate la ricerca, la certificazione da parte di soggetti terzi, la standardizzazione, e le tecniche di *privacy by design*; i legislatori valutino l'adeguatezza del quadro normativo esistente riguardo al trasferimento dei dati; le autorità di protezione dei dati continuino a fornire le necessarie informazioni ai titolari del trattamento, ai fornitori di *cloud* e ai legislatori sulla protezione dei dati in tale ambito.

Il documento approvato contiene altresì diverse indicazioni concernenti le *best practices,* che dovrebbero essere adottate dai titolari del trattamento e dai fornitori di servizi di *cloud.*

Nel 2012 il Gruppo si è occupato anche del diritto all'oblio (*right to be forgotten*) in internet, affrontato da due prospettive. La prima riguarda il "diritto a non essere trovato", attraverso strumenti tecnici che consentano di limitare la reperibilità sul web di informazioni relative all'interessato. La seconda, di carattere prettamente giuridico, riguarda il "diritto a essere dimenticato", ossia l'insieme delle condizioni e dei contesti pubblici (ad es., diffusione attraverso mezzi di informazione, casi giudiziari) e privati (ad es., ambienti di lavoro, contesti sanitari) in cui l'interessato può legittimamente chiedere a un titolare di non trattare i propri dati personali.

Il Gruppo ha deciso di affrontare i due aspetti separatamente e di concentrarsi in prima battuta su un documento di lavoro, di cui l'Autorità è *rapporteur,* relativo agli strumenti tecnici che consentono all'utente -pur nel rispetto della libertà di espressione- di esercitare il proprio diritto a non essere rintracciato nella "rete", in particolare attraverso l'uso del protocollo *robots.txt* da parte dei gestori dei siti web, che permette di limitare l'indicizzazione -operata dai motori di ricerca- delle informazioni presenti in internet.

Il Gruppo si è occupato inoltre del tema del web *tracking*, ossia delle tecnologie per il tracciamento, a fini di pubblicità comportamentale, delle attività degli utenti svolte sui siti internet. La questione, oggetto di un parere in via di elaborazione, afferisce al sempre più frequente ricorso da parte degli utenti a servizi web di calendario e gestione di rubriche. Tali servizi, in passato resi da applicazioni che trattavano dati memorizzati sui terminali, oggi, per via della maggiore disponibilità di banda, memoria e potenza di calcolo disponibili in rete, vengono per lo più realizzati in modalità *cloud*, consentendo agli utenti una maggiore integrazione con altre applicazioni di natura gestionale o semplicemente di socializzazione.

Tra i maggiori rischi in questo campo per la protezione dei dati si evidenziano il potenziale trasferimento di dati di traffico al fornitore dell'applicazione e il ricorso a tecnologie di trattamento digitale delle immagini in grado di riconoscere volti e più in generale di ricostruire il contesto di riferimento dell'interessato (e segnatamente abitazione, luogo di lavoro, amicizie). Nelle proposte formulate si sottolinea l'esigenza di distinguere la fase di

raccolta dei dati (*collecting*) dal loro successivo uso (*tracking*), per regolare il trattamento in maniera più flessibile. Attenzione è stata anche prestata all'opportunità di richiedere "*test* di necessità e proporzionalità" da realizzare prima del lancio commerciale di una nuova applicazione, in modo da prevedere la possibilità di alternative "*privacy friendly*", rispetto ad ogni specifico trattamento.

Nel corso delle riunioni è stato anche affrontato il tema del trattamento dei dati nell'ambito di Google *analytics*, il servizio che consente di monitorare le attività svolte sul proprio sito web dagli utenti (cd. "*audience measurement*"). Sono stati in particolare considerati i profili critici relativi alla mancanza di una idonea informativa e all'assenza di procedure tecniche per l'anonimizzazione degli indirizzi *Ip* raccolti dai titolari e trasferiti al motore di ricerca.

Data retention-expert Group

Nel 2012 il Gruppo di lavoro si è riunito tre volte per continuare ad esaminare aspetti legati all'interpretazione di alcuni termini della Direttiva n. 2006/24/CE (cd. "direttiva *data retention*") nonché alla possibile revisione della medesima. Il Gruppo infatti assiste la Commissione nel verificare l'applicazione della suddetta Direttiva ed è composto da rappresentanti provenienti dall'industria TLC, dalle *Law enforcement agencies* degli Stati membri, nonché dai rappresentanti delle Autorità di protezione dati degli Stati membri e dall'EDPS.

La Commissione, sulla base dei lavori del Gruppo dello scorso anno, ha individuato una forte disomogeneità di applicazione della normativa negli Stati membri, dando mandato al Gruppo di redigere le linee-guida volte all'armonizzazione, che verranno verosimilmente pubblicate nei primi mesi del 2013. La Commissione ha anche chiesto indicazioni alle varie parti per poter sviluppare un progetto che da un lato definisca meglio la composizione del gruppo, mantenendo la tripartizione -dimostratasi utile-Governi/*Law Enforcement Authorities agencies - LEAs* (che include Europol), industria ed autorità di protezione dei dati, e dall'altro precisi mandato e modalità di azione del Gruppo, anche in vista della nuova proposta di direttiva che la Commissione potrebbe presentare nel 2013. Al riguardo la Commissaria Malmström, partecipando alla sessione plenaria del Parlamento europeo per rispondere ad alcune interrogazioni sul tema, nel confermare che i tempi di revisione della direttiva saranno