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

Nel periodo di riferimento si è confermato (*cfr. Relazione 2008*, p. 246) da un lato l'intensificarsi dei lavori del Gruppo di lavoro polizia e giustizia (*Wppj*) sotto la guida del presidente del Garante ed il crescente coordinamento con il Gruppo Art. 29 su tutti i temi con implicazioni più ampie della competenza di un singolo "pilastro" (in particolare dati dei passeggeri, dati delle transazioni finanziarie, dati delle comunicazioni elettroniche) e, dall'altro, il tentativo del Consiglio e della Commissione di proporre e legiferare secondo metodologie non corrispondenti al nuovo Trattato, entrato in vigore il 1° dicembre del 2009. Come già rilevato, questo ha comportato il riesame da parte del Parlamento europeo di tali iniziative, che in alcuni casi ne ha determinato la caducazione.

I Garanti europei, sia nel *Wppj* sia nel Gruppo Art. 29, intensificando la loro cooperazione, hanno definito le osservazioni in relazione al nuovo programma di lavoro quinquennale nel settore libertà, sicurezza e giustizia ed al futuro della *privacy* (*cd. "programma di Stoccolma"*) in rapporto soprattutto con il Parlamento europeo per sopperire seppur parzialmente alla mancanza di "momenti istituzionalizzati" di dialogo. Una corretta applicazione del Trattato di Lisbona dovrebbe comportare la creazione di tali momenti, indispensabili per monitorare l'effettività dell'affermarsi dei diritti alla protezione dei dati ed alla riservatezza come diritti fondamentali garantiti a chiunque si trovi sul territorio dell'Unione.

Di grande utilità ed interesse è stata la partecipazione ai lavori del gruppo di esperti creato dalla Commissione per seguire l'applicazione della direttiva sulla conservazione dei dati di traffico a fini di prevenzione e repressione dei reati (*cd. "direttiva data retention"*) anche tenendo conto della parallela azione di *enforcement* varata dal Gruppo Art. 29. Questa attività ha consentito di definire alcuni documenti di lavoro volti a chiarire alcuni aspetti della direttiva per renderne più facile una applicazione uniforme - quali, ad esempio, il ruolo dei fornitori di transito internet (*Internet transit provider*), le obbligazioni per il filtraggio dello *spam*, l'applicazione della direttiva alla messaggistica *web* (*web mail* e *web based messaging*), il concetto di telefonia internet - nonché di partecipare

pienamente al processo di valutazione della direttiva stessa, che la Commissione dovrà completare entro il 15 settembre 2010.

Va menzionato poi che nel "terzo pilastro", a parte l'attività del Gruppo polizia e giustizia, è continuata l'attività degli organismi di supervisione e controllo comuni istituiti da specifiche Convenzioni (in particolare le Autorità comuni di controllo Schengen, EUROPOL e Dogane) e che dal 1° gennaio 2010 EUROPOL opera con una nuova base giuridica; per quanto riguarda invece la cooperazione doganale, sono state adottate nuove basi giuridiche che prevedono l'istituzione di una supervisione coordinata sul modello SIS II per le attività del *cd.* "primo pilastro" ed il mantenimento dell'Acc Dogane per quelle del "terzo pilastro".

E' continuata anche l'attività di supervisione a livello europeo sul funzionamento del sistema EURODAC, coordinata dall'EDPS. Sotto il profilo giuridico, la Commissione ha presentato delle proposte di modifica che, in particolare, consentono l'accesso al sistema EURODAC anche alle autorità di contrasto nazionali ed all'EUROPOL; su tali aspetti le autorità di protezione dei dati personali, attraverso pareri e comunicati stampa, hanno espresso forti critiche.

Working Party on Police and Justice (Wppj)

L'attività del *Working Party on Police and Justice* è proseguita nel 2009 secondo le priorità individuate nel programma di lavoro 2008-2009 (*v. Relazione 2008*, pag. 254); nel corso dell'anno si sono tenuti quattro incontri plenari, mentre il lavoro dei sottogruppi costituiti per la trattazione dei singoli temi ha consentito di elaborare posizioni, documenti e lettere tese a manifestare il punto di vista e le richieste delle autorità europee in tutte le sedi istituzionali opportune. E' stato inoltre definito il programma di lavoro per il successivo biennio 2010-2011, fissando alcuni obiettivi a breve ed a medio termine anche alla luce dell'entrata in vigore del Trattato di Lisbona e dei contenuti del *"programma di Stoccolma"* (adottato dal Consiglio europeo del 10/11 dicembre 2009).

Più in particolare, dopo l'adozione della decisione quadro in materia di protezione dati nel "terzo pilastro" (2008/977/GAI), e in vista della possibile entrata in vigore del Trattato di Lisbona, il *Wppj* ha costituito un gruppo ristretto che, riunitosi a Roma presso la sede dell'Autorità nel mese di settembre, ha definito le questioni organizzative, strategiche e di

sostanza sulle quali più urgente appariva un intervento delle autorità di protezione dati europee. In tale ambito si è stabilito di contribuire alla consultazione pubblica della Commissione europea sul *"futuro della protezione dati"* in Europa integrando il documento in preparazione da parte del sottogruppo *"Future of Privacy"* del WP29 (*par.* 20.2.) per gli aspetti più direttamente connessi alle attività del "terzo pilastro" nell'ottica dell'approvazione del Trattato di Lisbona; il *Wppj* ha ribadito la necessità di individuare forme nuove e più organiche di collaborazione con il WP29 e gli altri soggetti che si occupano di protezione dati a livello sopranazionale (comprese le autorità comuni di controllo nel "terzo pilastro").

Il *Wppj* ha ritenuto, in particolare, indispensabile addivenire ad un unico quadro giuridico che consenta di applicare anche alle questioni di "terzo pilastro" i princìpi fissati dalla Direttiva n. 95/46/CE, in linea con l'abolizione della distinzione fra pilastri della politica comunitaria fissata nel Trattato di Lisbona; ciò non esclude, comunque, la possibilità di introdurre strumenti specifici per disciplinare meglio le peculiarità legate alla cooperazione giudiziaria e di polizia (cosa prevista, del resto, dallo stesso Trattato).

Fa parte di tale obiettivo il lavoro di monitoraggio proseguito nel 2009 rispetto all'attuazione della decisione quadro 2008/977, pur essendo venuta a mancare l'occasione di un confronto pubblico con la Commissione europea e le altre istituzioni al fine di raccogliere *input* e suggerimenti da parte delle istituzioni maggiormente coinvolte (confronto che avrebbe dovuto tenersi nel mese di novembre 2009). Vanno anche ricordati, in tale contesto, i richiami rivolti dal *Wppj* alle istituzioni europee rispetto al proliferare di forme di svuotamento dei princìpi di protezione dati: in particolare in relazione alla proposta di modifica presentata dalla Commissione nel mese di settembre 2009 con riguardo al regolamento che disciplina EURODAC, tesa a consentire alle forze dell'ordine l'accesso alla relativa banca dati (che comprende informazioni sui richiedenti asilo nei Paesi Ue, istituita per finalità amministrative). In un comunicato stampa pubblicato il giorno in cui tale proposta è stata resa pubblica (10 settembre 2009), il *Wppj* ha ribadito la propria contrarietà a tale modifica, che contravviene alle finalità primarie della banca dati EURODAC e costituisce un pericoloso precedente.

Il settore dei flussi transfrontalieri di dati personali ha rappresentato naturalmente un importante banco di prova anche nel 2009. Occorre menzionare in tale contesto gli sviluppi intercorsi con riguardo ai flussi di dati fra Europa ed Usa, in particolare l'attività dello *"Eu-US High-Level Contact Group on Information Sharing and Privacy and Personal Data Protection"*. Tale gruppo di lavoro aveva elaborato una relazione finale (pubblicata con *addendum* nel mese di novembre 2009) in cui venivano fissati alcuni princìpi "condivisi" fra Ue ed Usa per quanto riguarda la tutela dei dati personali scambiati a livello transatlantico per la lotta al terrorismo ed altre gravi forme di criminalità. Il *Wppj* in precedenza aveva sollecitato il coinvolgimento delle autorità europee di protezione dati nell'attività di tale gruppo, senza alcun esito (due lettere erano state inviate nel 2008 e nel 2009 alle competenti istituzioni europee), ed ha quindi fatto presente la propria posizione (attraverso la presidenza italiana) in occasione dell'incontro convocato dalla Commissione europea, nel mese di febbraio 2010, per raccogliere suggerimenti e indicazioni dalle autorità di protezione dati, al fine della negoziazione di un eventuale accordo bilaterale in materia. Il *Wppj* ha anche deciso di contribuire alla consultazione pubblica che la Commissione ha lanciato nel mese di gennaio 2010 su questo stesso *dossier*. Restano da chiarire numerosi aspetti di tale accordo, ad iniziare dalla sua portata e dallo specifico contenuto dei princìpi di protezione dati in esso contenuti; resta fondamentale la questione dei meccanismi atti a garantire la tutela dei cittadini europei che ritenessero violati i propri diritti dal trattamento dei dati effettuato negli Usa. Le autorità europee di protezione dati hanno in programma di adottare una mozione sul punto in occasione della *Spring Conference 2010*.

Sempre con riferimento ai flussi transatlantici di dati, il *Wppj* ha anche approvato il testo di una lettera destinata ai ministeri nazionali competenti e concernente la stipula di accordi bilaterali cosiddetti *"simil-Prüm"* fra alcuni Stati europei (fra cui l'Italia) e gli Stati Uniti ai fini dello scambio di informazioni per finalità giudiziarie e di polizia (in particolare dati Dna), per sollecitare attenzione sulla necessità di rispettare alcuni princìpi essenziali in materia di tutela dei dati personali. Peraltro, si sono manifestate alcune problematiche legate alla corretta attuazione a livello nazionale delle disposizioni contenute nelle

decisioni di recepimento del Trattato di Prüm, sulle quali il *Wppj* ha chiesto chiarimenti al Consiglio Ue ed ai ministeri competenti (con particolare riguardo alle prassi relative agli artt. 3 e 4, comma 1, della decisione di attuazione del Trattato di Prüm 2008/615/GAI). Un altro delicato *dossier* nel 2009 ha riguardato i sistemi di messaggistica *Swift* (dati relativi alle transazioni bancarie), in particolare il progetto di accordo fra Ue ed Usa in materia; il *Wppj* ha redatto una lettera congiunta con il WP29, indirizzata alla Commissione LIBE del Parlamento europeo nel mese di gennaio 2010, per manifestare le proprie perplessità e critiche rispetto a numerosi punti di tale accordo (ad iniziare dalle diverse definizioni di "terrorismo" in ambito Ue ed Usa e dai meccanismi di revisione dell'accordo stesso).

Per quanto riguarda le attività già programmate, il *Wppj* ha completato la ricognizione dello stato dell'arte relativo agli accordi bilaterali con Paesi extra-europei in materia di cooperazione giudiziaria e di polizia, grazie ai contributi forniti dalle delegazioni nazionali, ed ha elaborato il testo di una clausola addizionale da inserire in tali accordi per fissare i princìpi fondamentali in materia di protezione dati, in ciò seguendo l'indicazione fornita dalla *Spring Conference* di Edimburgo nel 2009. La clausola (poi approvata nel mese di marzo 2010) prevede una doppia formulazione, con un diverso livello di dettaglio, per tenere conto del diverso quadro di garanzie derivante dall'eventuale adesione del Paese terzo alla Convenzione 108/81 del Consiglio d'Europa; in quest'ultimo caso, infatti, il Paese terzo è tenuto quanto meno al rispetto dei princìpi fondamentali fissati in materia attraverso la Convenzione.

E' stata completata anche l'analisi riferita allo stato di attuazione della Convenzione del Consiglio d'Europa concernente la criminalità informatica, in questo caso attraverso l'elaborazione di alcune raccomandazioni che saranno veicolate dalle autorità di protezione dati ai ministeri competenti negli Stati membri che devono ancora recepire la Convenzione stessa; esse rispecchiano alcune delle problematiche emerse dall'analisi degli strumenti di recepimento nazionale attualmente in essere.

Va infine ricordato che, dopo l'approvazione da parte della *Spring Conference* di Edimburgo del "Catalogo" in materia di supervisione e co-operazione elaborato dal *Wppj*,

è iniziata nel 2009 un'attività di *"risk assessment"* basato sui criteri fissati in tale "Catalogo"; l'obiettivo è l'individuazione di alcuni settori meritevoli di accertamenti ulteriori (eventualmente attraverso ispezioni congiunte) al fine di elaborare una politica organica di supervisione per il 2010-2011 e garantire il rispetto armonizzato dei princìpi di protezione dati fissati nella Convenzione 108/81 e nella Direttiva n. 95/46/CE. La *Spring Conference* 2010 è stata chiamata ad approvare l'elenco di tali aree di intervento dando mandato al *Wppj* di proseguire i necessari approfondimenti.

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

A seguito della Decisione 2009/371/GAI del 6 aprile 2009 sull'integrazione di EUROPOL tra le strutture dell'Unione e sulla definizione del quadro generale di riferimento per lo svolgimento della sua attività e per le norme attuative della decisione medesima (entrata in vigore 1° gennaio 2010), che ha sostituito la Convenzione finora in vigore, gran parte dell'attività dell'anno è stata dedicata alla ridefinizione di tutte le norme collegate, in modo da adeguarle al nuovo quadro giuridico. Su molte di queste proposte l'Autorità comune di controllo è stata chiamata a rendere il suo parere. L'Acc ha anche adottato le necessarie modifiche al regolamento interno, nonché ridefinito il mandato dei suoi componenti e degli organi direttivi, nuovamente designati, procedendo poi alla rielezione/conferma di presidente e vicepresidente. È stato, inoltre, rinnovato il mandato per il gruppo ispezioni e confermato il coordinatore. L'ispezione annuale si è svolta come di regola nel mese di marzo ed il rapporto, che conferma l'importanza fondamentale delle stessa, è stato approvato.

Alcuni elementi emersi andranno approfonditi per valutarne la congruità con il quadro legale di EUROPOL, se del caso anche con azioni di verifica da svolgere a livello nazionale.

Mentre l'ispezione annuale consente infatti di monitorare attentamente la compliance di EUROPOL nei trattamenti di dati a quanto prescritto dalla Convenzione, sempre di più emergono scenari in cui l'acquisizione e la messa a disposizione di dati avvengono in un quadro meno chiaro.

Ad esempio, si prospetta un coinvolgimento di EUROPOL per quanto riguarda i reati finanziari (sullo sfondo della prospettiva dell'accordo Eu-Usa sui dati *Swift*), il fenomeno

dell'immigrazione e l'attività di *Frontex*.

Altro aspetto di grande importanza attiene all'attribuzione di credenziali per l'accesso ai vari *database* creati per fini di cooperazione tra forze di polizia per operare il *crosschecking* dei dati.

Al fine di disporre, nelle ispezioni, di una metodologia uniforme e risultati comparabili, si è deciso di curare la predisposizione di un modulo uniforme per le risposte da fornire in relazione agli specifici, puntuali accertamenti da svolgere a livello nazionale sulla base delle segnalazioni inviate dal *team* ispettivo e necessarie al completamento dell'ispezione annuale. Le questioni relative al modo in cui l'autorità di protezione dati nazionale esercita il suo ruolo di controllo verranno esaminate in un secondo tempo.

Sono stati adottati due pareri sul livello di adeguatezza di Macedonia e Colombia concludendo che non ci sono ostacoli all'apertura di un negoziato con questi Paesi al fine di poter stipulare con gli stessi un accordo operativo che consenta anche lo scambio di dati personali.

Occorre tuttavia che l'Acc si esprima con un nuovo parere sulle specifiche ed effettive garanzie di tale scambio.

Sono altresì proseguite le discussioni sul trattamento di dati personali e su possibili punti di contrasto tra la (nuova) base giuridica dell'EUROPOL ed altri strumenti in vigore, fra i quali la decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e *intelligence* tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge (*"iniziativa svedese"*, GU L 386, del 29 dicembre 2006).

Revisione della funzione delle decisioni costitutive

L'Acc ha valutato la funzione delle decisioni costitutive degli archivi di lavoro per fini di analisi. L'Autorità ha discusso la struttura delle decisioni costitutive, il loro ruolo e scopo come pure la loro funzione, sia interna che esterna. Ha inoltre esaminato l'esigenza di operare una distinzione netta tra la nozione di "dati comuni" e quella di "dati sensibili", le modifiche all'attuale *iter* di analisi criminale e infine, ma non meno importante, l'opportunità di aumentare la funzione di trasparenza delle decisioni costitutive.

Sul punto, l'Acc ha deciso di avviare delle discussioni con l'EUROPOL volte a

sondare, chiarire e risolvere eventuali divergenze sulla funzione delle decisioni costitutive.

Ricezione di informazioni provenienti da fonti accessibili al pubblico, da persone private e parti private

L'Acc ha adottato un parere sul testo proposto da EUROPOL con cui in particolare si chiede di definire regole più dettagliate relative al contenuto e alla procedura di conclusione dei *memorandum* d'intesa previsti allo scopo dall'art. 26, *par.* 2, della suddetta decisione del Consiglio 2006/960/GAI. L'Acc ha anche richiamato l'esigenza di tenere conto di aspetti quali la chiarezza delle definizioni, la legittimità del trattamento dei dati trasmessi da parti private, l'attribuzione delle responsabilità e il diritto applicabile.

Check the web

Al fine di comprendere meglio la decisione costitutiva e le modalità di integrazione del progetto *"Check the web"* (controlla la rete) nel regime giuridico per gli archivi di lavoro nella convenzione EUROPOL, nonché nella decisione del Consiglio sull'EUROPOL, il gruppo di lavoro sulle decisioni costitutive ha visitato l'EUROPOL in data 15 settembre 2009. Una relazione sulle discussioni svoltesi durante la riunione e i relativi risultati è stata presentata all'Acc, unitamente a una proposta di modifica della decisione costitutiva relativa a questo archivio.

L'Acc è stata informata sui recenti sviluppi relativi al progetto SIENA, in particolare circa l'attuazione dei requisiti in materia di protezione dei dati nella prima fase di attuazione del nuovo sistema di messaggistica. La gran parte dei requisiti di protezione dei dati richiesti dall'Acc ha trovato piena attuazione. L'Acc continuerà a seguire da vicino lo sviluppo di SIENA.

Anche nel 2009 è stata organizzata una riunione con le autorità di protezione dei dati di Paesi terzi e degli organismi con cui l'EUROPOL ha stabilito accordi operativi. All'incontro erano presenti le autorità di protezione di Norvegia, Svizzera, Croazia ed i responsabili di protezione dati di EUROJUST ed INTERPOL. L'occasione ha offerto il modo di scambiare esperienze sugli aspetti della supervisione, anche se le informazioni fornite dirette a valutare il funzionamento dell'accordo in concreto sono risultate piuttosto scarse.

Attività del Comitato ricorsi

Il Comitato ricorsi ha definito un caso riguardante la richiesta dell'interessato di accesso e verifica dei propri dati.

Le attività dell'Acc, inclusi i pareri adottati e le iniziative svolte, sono disponibili anche

in italiano sul sito dell'Acc all'indirizzo *http://europoljsb.consilium.europa.eu/documents.*

Schengen: l'attività dell'Autorità di controllo comune e la Valutazione Schengen dell'Italia

Per quanto concerne i lavori dell'Acc Schengen il perdurare dei ritardi per l'entrata in funzione del SIS II (*cfr. Relazione 2008*, p. 252) ha consentito all'Acc di continuare a svolgere i compiti di supervisione attribuiti con ulteriori iniziative, che concernono in particolare il controllo in tutti gli Stati Schengen delle modalità di inserimento delle segnalazioni di cui all'art. 95 (mandato di arresto europeo, arresto a fini di estradizione), con completamento degli accertamenti sinora svolti sulle diverse categorie di segnalazioni previste dalla Convenzione Schengen, e con un calendario per il *follow up* degli accertamenti già svolti.

È proseguita la valutazione dei risultati delle verifiche compiute con riguardo alle segnalazioni relative agli artt. 97 e 98 della Convenzione, con l'adozione dei relativi rapporti; sono stati anche esaminati gli aspetti relativi alla cooperazione tra le autorità di protezione dati (Apd), nel caso di richieste di accesso presentate in un Paese diverso da quello che ha inserito la segnalazione nel SIS. La Convenzione prevede infatti che il diritto di accesso e gli altri diritti connessi possano essere fatti valere dall'interessato in uno qualsiasi dei Paesi Schengen. Molte situazioni come, ad esempio, quella in cui la segnalazione sia stata inserita da un Paese diverso da quello cui la persona si è rivolta, ovvero decisioni amministrative o giudiziarie relative ad una segnalazione di altro Paese, richiedono una cooperazione tra le autorità competenti e le autorità di protezione dei dati.

Si è inoltre deciso di aggiornare la *"Guida per l'esercizio del diritto d'accesso"*, predisposta diversi anni addietro. Il protrarsi dell'attesa per l'entrata in vigore del SIS II - che comporta anche la soppressione dell'Acc e la sua sostituzione con un altro sistema di supervisione e prevede l'obbligo di svolgere in tutti i Paesi campagne informative sui diritti delle persone, affidando alla Commissione il compito di definirle ed organizzarle - e la considerazione che le nuove disposizioni non saranno comunque attuate prima di almeno altri due anni, mentre nuovi Paesi sono entrati a far parte del sistema Schengen, ha indotto l'Acc ad intervenire nuovamente per garantire agli interessati le informazioni necessarie per esercitare i diritti riconosciuti dalla Convenzione. L'attività di aggiornamento è stata

completata e la *"Guida per l'esercizio del diritto d'accesso"*, attualmente disponibile sul sito provvisorio dell'Acc Schengen, è raggiungibile attraverso un *link* posto sulla *home page* del sito del Garante, che contiene anche le informazioni necessarie per l'esercizio del diritto in Italia. Quanto alla campagna informativa, la Commissione già da tempo ha predisposto i modelli per la stampa di opuscoli e *poster* plurilingue, anche se le attività sono per il momento in una fase di stallo.

L'Acc ha continuato a seguire gli aspetti legati alla migrazione dei dati dal SIS al SIS II, e, in previsione dello scenario futuro della supervisione e controllo (che passerà dall'Acc all'EDPS, di concerto con le autorità di protezione dati), il Garante europeo per la protezione dei dati viene invitato a partecipare alle riunioni quando questi aspetti sono all'ordine del giorno.

In relazione all'azione comune lanciata per verificare in ciascuno dei Paesi partecipanti la regolarità delle segnalazioni inserite nel sistema, con riferimento all'art. 99 della Convenzione (sorveglianza discreta e controllo specifico) ed alle raccomandazioni formulate nel rapporto finale (che l'Autorità italiana ha ripreso nei provvedimenti conclusivi della parte nazionale dell'accertamento, uno dei quali riguarda le misure di sicurezza), è stato adottato un provvedimento che contiene le prescrizioni ritenute necessarie a conformare il trattamento alle disposizioni della Convenzione ed alle prescrizioni del Codice in materia di sicurezza (*cfr. par.* 7.3.)

Valutazione Schengen dell'Italia

L'Italia è stata sottoposta alla procedura di Valutazione Schengen, che riguarda anche il settore della protezione dati. Si tratta della seconda Valutazione, dopo la prima del settembre 2004. Il Gruppo di esperti in particolare ha avuto il mandato di verificare ruolo e poteri del Garante e l'esercizio da parte di questo della supervisione sui trattamenti di dati effettuati in base alla Convenzione.

Le visite presso il Garante e gli uffici del Ministero dell'interno si sono svolte nel gennaio del 2010 e gli esperti hanno espresso una valutazione globalmente positiva, pur raccomandando di migliorare alcune prassi ed intensificare le misure di sicurezza poste a tutela dei dati e dei sistemi, largamente in linea con le prescrizioni del Garante cui si è accennato sopra.

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

L'Acc ha concentrato gran parte dei suoi lavori sulla proposta di decisione volta a sostituire l'attuale base legale con uno strumento dell'Unione. Dopo un primo parere nel mese di marzo, il testo è stato modificato accogliendo le osservazioni formulate dall'Acc. Successivamente, però, il servizio giuridico del Consiglio ha chiesto di modificare il testo, che conservava alle autorità nazionali di protezione dei dati riunite in una autorità comune di controllo la supervisione sulla liceità dei trattamenti dei dati svolti nel SID (Sistema informativo doganale), in modo da introdurre una forma di supervisione centrata sul Garante europeo, del tipo di quella oggi realizzata in EURODAC.

Al riguardo, una lettera a firma del Presidente dell'Acc, dando atto del favore con cui la gran parte delle osservazioni formulate nel parere sono state accolte dal gruppo del Consiglio che discute la proposta di decisione, ha ribadito l'importanza di mantenere la forma "comune" del controllo, offrendo di articolare sul punto, laddove opportuno nel corso dei lavori. Successivamente si è giunti all'adozione di un secondo parere, limitato agli aspetti della supervisione.

Il testo finale del provvedimento prevede la forma collegiale di supervisione, ma l'art. 25 nella sua forma definitiva è scritto in modo non del tutto chiaro. La decisione è stata finalmente adottata (Decisione 2009/917/GAI del Consiglio del 30 novembre 2009) ed entrerà in vigore il 27 maggio 2011.

Inoltre l'Acc, sulla scorta dei positivi risultati della sperimentazione intrapresa (*cfr. Relazione 2008*, p. 251) ha esteso l'attività di verifica a tutti i Paesi che applicano la Convenzione, utilizzando un questionario per l'autovalutazione. Le domande si basano su *standard* internazionali e riguardano principalmente misure di sicurezza fisiche e logiche esistenti e formazione del personale.

Supervision EURODAC

La supervisione sul sistema EURODAC, attribuita come coordinamento al Garante europeo (Gepd), è proseguita con conclusione della seconda ispezione comune, basata in particolare sulla verifica delle modalità attraverso le quali viene resa l'informativa all'interessato (richiedente asilo) e sui sistemi usati per accertare il requisito dell'età (solo ultra quattordicenni) ai fini dell' acquisizione delle impronte digitali per l'inserimento nella base di dati europea.

Nella riunione di giugno è stato adottato il rapporto relativo a tale supervisione coordinata. Il documento presenta i risultati dell'attività di verifica svolta e propone alcune raccomandazioni sulle proposte di modifica delle disposizioni europee che regolano il funzionamento di EURODAC e la cooperazione ai fini dell'esame della domanda di asilo (Regolamento Dublino), raccomandazioni che sono anche destinate ad essere utilizzate a livello nazionale.

La versione finale del documento, solo in inglese, è stata resa disponibile per una diffusione sia in ambito Unione sia nazionale. Un sommario del rapporto redatto è disponibile nelle diverse lingue.

Al riguardo è da rilevare che la "eguale" partecipazione delle autorità di protezione dei dati richiederebbe un adeguato regime linguistico e la traduzione nelle diverse lingue almeno dei principali documenti - in particolare di quelli provenienti dal gruppo di lavoro di EURODAC - per la circolazione all'interno dei diversi Paesi. Attualmente la lingua di lavoro è solo l'inglese, anche per la redazione dei documenti, differentemente da quanto avviene per i lavori delle Autorità comuni di controllo. Il Garante europeo al riguardo fa riferimento al costo da sostenere, ma tale stato di cose potrebbe incidere sulla funzionalità del meccanismo di supervisione, da assicurare su base collegiale.

Altro tema approfondito nel periodo considerato ha riguardato il funzionamento della rete di comunicazione utilizzata nell'ambito della procedura di asilo (*DubliNet*): sulla base del lavoro svolto in modo coordinato nei vari Paesi è stato redatto un rapporto che presenta lo stato dei fatti e formula alcune raccomandazioni.

Il rapporto suggerisce la necessità di utilizzare *DubliNet* in modo sistematico per gli scambi di informazioni e le comunicazioni che avvengono tra gli uffici "Dublino", di dettare regole complementari a livello nazionale sull'uso del sistema (manuali d'uso, guida alle migliori prassi). Raccomanda infine, rivolgendosi in particolare alla Commissione, di dettare regole chiare ed armonizzate per quanto concerne la cancellazione dei dati una volta che la finalità dello scambio sia stata ottenuta. Anche questo documento, una volta formalmente adottato, sarà distribuito alle delegazioni e diffuso tra le autorità ed istituzioni competenti.

E' in corso l'attività per la redazione del rapporto di attività per gli anni 2008-2009 e per la definizione del programma di attività per il biennio 2010-2011.

20.4. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

Case Handling Workshop

I due incontri semestrali previsti nell'ambito dei *Case Handling Workshop* si sono tenuti rispettivamente il 12-13 marzo a Praga ed il 22-23 ottobre a Limassol (Cipro).

Come di consueto, sono stati affrontati alcuni temi già discussi in precedenti riunioni del gruppo e, in particolare, in occasione del precedente *workshop* a Bratislava (*mass media* e *privacy*; videosorveglianza; trattamento di dati dei lavoratori compreso il tema del *whistleblowing*) nonché problematiche più generali, legate all'esercizio del diritto di accesso da parte degli interessati. Il *workshop* di Cipro, in particolare, è stato organizzato tenendo conto delle indicazioni della *Spring Conference* 2009, con la presentazione di *case studies* da discutere in sessioni parallele su alcuni argomenti dalla stessa indicati (oltre a quelli sopra ricordati, i trattamenti di dati personali effettuati attraverso la rete internet ed i trattamenti effettuati nel settore bancario e presso i sistemi di informazione creditizia).

Quanto al rapporto tra protezione dei dati e *mass media*, occorre rilevare che nella maggior parte dei Paesi europei il trattamento effettuato per finalità giornalistiche non rientra nella competenza delle autorità di protezione dati, essendo rimesso (visto il carattere costituzionale del diritto alla manifestazione del pensiero) all'autorità giudiziaria.

La sessione di Praga ha consentito all'Autorità finlandese di presentare il caso oggetto della sentenza della Corte di giustizia delle Comunità europee del 16 dicembre 2008 (*Satakunnan Markkinapörssi and Satamedia*), relativo all'inoltro via *Sms* - e a pagamento - dei dati reddituali raccolti da una società e dapprima pubblicati dalla stessa su un "quotidiano" regionale; l'Autorità ha richiamato l'attenzione sulla mancata specificazione da parte della Corte del concetto di *"trattamento effettuato per finalità giornalistiche"* che ha lasciato, nella sostanza, alla Suprema Corte amministrativa finlandese il compito di decidere se il predetto trattamento rientri o meno in tali finalità. L'autorità italiana ha sollevato il problema della pubblicazione *online* degli archivi storici di testate giornalistiche ma, forse per i motivi sopra riportati, nessuna esperienza simile alla nostra è stata segnalata.

Un tema sempre di attualità, anche guardando ai precedenti incontri, è quello della videosorveglianza. In occasione dell'incontro di Praga, il rappresentante dell'autorità federale tedesca ha rilevato come, a suo avviso, il tema possa essere oggetto di una futura revisione della Direttiva n. 95/46/CE che non lo affronta in modo specifico: la Germania ha una legge federale che disciplina il trattamento di dati effettuato per mezzo di strumento di videosorveglianza nelle aree accessibili al pubblico, ma non nel privato (nell'ambito del quale la questione è stata affrontata soprattutto attraverso la giurisprudenza e un'applicazione delle disposizioni generali in materia di protezione dei dati). In questo contesto, il periodo di conservazione delle immagini rappresenta da sempre una delle problematiche più spinose; durante l'incontro di Cipro se ne è discusso a partire dalla presentazione effettuata dall'autorità svizzera federale, relativa all'approccio complessivo alla videosorveglianza adottato nella confederazione elvetica. Dati per assodati alcuni princìpi fondamentali in materia di protezione dati (minimizzazione, proporzionalità, finalità), e sottolineata l'esigenza di un'opera di sensibilizzazione da parte delle autorità di protezione dati, l'autorità svizzera ha prospettato l'esigenza di un approccio basato sull'uso di misure tecnologiche (*blanking* selettivo delle immagini, *motion detection*, posizionamento) al fine di garantire il rispetto di tali princìpi; tuttavia, esistono innegabili divergenze rispetto alla congruità del periodo di conservazione delle immagini (un mese, una settimana), talora legate all'esistenza di specifica legislazione nazionale. Per quanto riguarda l'impiego della videosorveglianza in ambiti privati, la relazione della delegazione lituana durante l'incontro di Cipro ha offerto l'occasione per discutere del concetto di *"uso personale"*, trattando di un caso in cui l'installazione di una videocamera in un cortile interno ad un palazzo è stata ritenuta dall'autorità giudiziaria (chiamata a pronunciarsi sulla decisione impugnata dell'Apd) sottratta all'applicazione della normativa in materia di protezione dati (nonostante la visibilità di parte della proprietà di un altro inquilino dello stabile). Linee-guida in materia di videosorveglianza sono state elaborate dall'autorità olandese (con riferimento all'utilizzo da parte delle forze di polizia del proprio paese di un sistema di riconoscimento automatico delle targhe che, nato originariamente solo per le sanzioni relative al superamento dei limiti di velocità, è attualmente utilizzato anche per la repressione di

reati) e dall'autorità spagnola (riferite solo al settore privato, essendovi norme apposite per l'utilizzo di dispositivi di videosorveglianza nel settore pubblico). L'EDPS ha ricordato il proprio documento in materia, oggetto di consultazione pubblica a fine 2009, volto soprattutto a consentire al titolare del trattamento di valutare l'effettiva necessità di porre in essere e poi mantenere tali sistemi, attraverso una *"analisi prima dell'installazione"* (per verificare gli scopi, il fondamento normativo, l'opportunità/necessità dell'installazione, il rapporto costi/benefici) e un *"self audit"* costante su tali tipologie di trattamento. E' stata anche formulata la proposta di introdurre un "logo" armonizzato a livello Ue per segnalare la presenza di videocamere.

Un altro ambito significativo ha riguardato il trattamento dei dati personali sul luogo di lavoro. Al riguardo, il tema del *whistleblowing* (meccanismi dedicati per la segnalazione interna, in forma protetta, di irregolarità, soprattutto finanziarie) è stato affrontato a Praga attraverso il caso presentato dall'EDPS e relativo all'ufficio dell'OLAF (l'organismo comunitario per la lotta alle frodi); a giudizio dell'EDPS, esso troverebbe il suo unico fondamento normativo nel regolamento sul personale dell'OLAF, nel rispetto di una serie di princìpi: qualità dei dati, tempi di conservazione non eccedenti le finalità del trattamento (allo stato, le informazioni raccolte sono conservate per venti anni), diritto di accesso e di rettificazione da parte dell'interessato, informativa (con possibilità di differirla fino all'esito degli accertamenti). L'autorità portoghese ha invece descritto le linee-guida adottate in materia di accertamenti sul luogo di lavoro relativi all'uso di sostanze alcoliche o droghe da parte dei dipendenti; principio fondamentale è quello secondo cui i dati possono essere raccolti dal solo medico del lavoro e solo in caso di lavori che comportano particolari rischi per la sicurezza, anche di terzi, mentre il datore di lavoro può solo conoscere se il lavoratore sia idoneo o meno all'attività da svolgere. Va segnalato che durante l'incontro di Cipro l'autorità inglese ha presentato un caso che ha suscitato ampia eco nella stampa anglosassone, relativo ad una banca dati (in effetti una *black list*) dei lavoratori edili creata all'insaputa degli interessati; ciò ha costituito l'occasione per un confronto delle autorità sui mezzi a propria disposizione per bloccare e "sanzionare" un trattamento illecito di dati.

Sul rapporto fra protezione dei dati ed internet, la discussione nei due *workshop* ha toccato da un lato le attività di sensibilizzazione messe in atto da alcune autorità (l'autorità spagnola ha presentato la propria campagna di sensibilizzazione nelle scuole sull'uso di internet da parte dei minori) e, d'altro canto, il tema della responsabilità per la pubblicazione di dati personali su internet. Su quest'ultimo punto, l'autorità svedese ha descritto un caso relativo a forum di discussione e siti di *rating* (*ad es.*, di professori universitari), sollevando le questioni dell'eventuale responsabilità in capo al *service provider* per contenuti non propri, e del rischio di costringere gli ISP ad operare quali "censori" di libere forme di manifestazione del pensiero; un orientamento prevalente fra le autorità partecipanti riconoscerebbe la responsabilità in capo al *provider* che, pur a conoscenza di un contenuto chiaramente "illecito", non lo rimuova. Da ricordare anche i casi concernenti *Google StreetView*, sollevati dall'autorità ceca e da quella federale tedesca, sull'applicabilità e sull'opportunità della disciplina nazionale in materia di protezione dei dati (e, in tale contesto, sull'opportunità di richiedere, *ad es.*, una notificazione del trattamento); secondo l'autorità federale tedesca, la raccolta dei dati grezzi utilizzati per il servizio è effettuata sul territorio nazionale, gli stessi sono elaborati all'interno del veicolo che li raccoglie e solo successivamente trasferiti in un paese terzo, e dunque la normativa nazionale troverebbe applicazione.

Infine, durante l'incontro di Cipro sono state affrontate le tematiche relative, più in generale, all'esercizio del diritto di accesso ai dati. La discussione si è soffermata sull'interpretazione dell'art. 12, *par.* 1, lett. *a*), della Direttiva n. 95/46/CE che fa riferimento al diritto per l'interessato di ottenere informazioni su *"destinatari o categorie di destinatari cui sono comunicati i dati"*.

La nostra Autorità, partendo da due casi di studio e richiamando la recente sentenza del 7 maggio 2009 (caso *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*) - con cui la Corte di giustizia, nell'interpretare tale articolo, ha stabilito che gli Stati membri sono tenuti a prevedere il diritto di accesso alle informazioni sui destinatari o sulle categorie di destinatari dei dati nonché sul contenuto delle informazioni comunicate non solo per il presente, ma anche per il passato - ha fatto circolare un questionario