identificazione digitali settoriali o sistemi che consentono di verificare solo i requisiti necessari per richiedere un servizio, ad es., l'età). In quest'ottica, il Gruppo suggerisce che il regolamento richiami più spesso la possibilità di utilizzare pseudonimi e riduca la quantità di dati personali che debbano essere resi noti per la verifica di una firma digitale; si auspica anche l'introduzione, nel regolamento, di disposizioni che impediscano che le informazioni personali necessarie per ottenere servizi fiduciari (in caso di autenticazione ad esempio) possano essere utilizzate per profilare gli interessati.

Progetti di ricerca e protezione dei dati

Hanno formato oggetto di valutazione da parte del Gruppo anche gli aspetti relativi alla protezione dei dati personali connessi ai trattamenti effettuati per la gestione di due progetti di ricerca finanziati dalla Commissione europea: il progetto INDECT, relativo all'impatto delle nuove tecnologie per il monitoraggio di comportamenti sospetti sulla rete e nell'ambiente urbano sulla vita privata dei soggetti residenti nell'Unione (doc. web n. 2983082), e il progetto Stork 2.0 (doc. web n. 2983042) che – come il precedente, già esaminato dal Gruppo Art. 29 nel 2011 – riguarda l'interoperabilità a livello europeo dei sistemi di identificazione elettronica.

Con l'occasione, il Gruppo ha concordato di curare un approfondimento sui requisiti richiesti dalla Commissione europea per il finanziamento dei progetti di ricerca in modo da verificare come siano presi in considerazione i profili relativi alla protezione dei dati e alla vita privata. In proposito, sono stati evidenziati i limiti e le difficoltà applicative derivanti dalle attuali condizioni contrattuali predisposte dalla Commissione europea per il finanziamento dei progetti di ricerca nell'ambito del settimo programma quadro. Tali clausole, nella parte in cui richiedono al coordinatore del progetto di presentare una "formale approvazione" da parte delle competenti autorità di protezione dei dati, non risultano coerenti con alcune legislazioni nazionali di attuazione della direttiva 95/46/CE (che, come ad esempio in Italia e Spagna, non prevedono tale tipo di approvazione) e hanno evidenziato l'opportunità di un approccio comune da parte delle autorità di protezione dei dati interessate. Alla luce di ciò, il Gruppo Art. 29 ha preso contatto con la DG Ricerca della Commissione europea che sta lavorando al nuovo programma quadro di investimenti nella ricerca e nell'innovazione per gli anni 2014-2020, *Horizon 2020*, per collaborare alla revisione delle clausole previste per i contratti di finanziamento e delle linee guida sulla *privacy* e sulla protezione dei dati (doc. web n. 2983072).

Law Enforcement

Rilevante è stata inoltre l'attività del Gruppo su proposte sviluppate da parte del *Borders, Travel and Law Enforcement subgroup* (BTLE). Il sottogruppo è nato dall'esigenza di trattare in seno al Gruppo Art. 29 le tematiche connesse al trattamento di dati nel settore di polizia e giustizia (*ex* III Pilastro), dopo l'eliminazione del WPPJ (*Working Party on Police and Justice*) nel corso della *Spring Conference* 2012 in ragione dell'unificazione dei pilastri dell'Unione successiva all'entrata in vigore del Trattato di Lisbona.

Direttiva III pilastro

Il Gruppo ha adottato il Parere n. 1/2013 del 26 febbraio 2013 (doc. web n. 2980389) riguardo alla proposta di direttiva sui trattamenti di dati personali nelle attività giudiziarie e di polizia, formulando specifiche osservazioni e chiedendo maggiori garanzie per quanto riguarda le categorie di interessati, l'esercizio del diritto di accesso, i co-titolari del trattamento ed i poteri delle autorità di protezione dati.

Futuro della supervisione

È stato altresì affrontato il tema della supervisione nel settore del *law enforcement*, in particolare sulla base del documento sul "Futuro della supervisione" sottoposto alla Conferenza di primavera tenutasi a Lisbona (cfr. par. 19.2). Aspetto centrale di tale discussione è stata l'analisi sui punti su cui può registrarsi una convergenza tra le autorità nazionali di protezione dei dati e il Garante europeo (EDPS). In particolare è stato valutato come assicurare coerenza e continuità di controllo per le attività che si svolgono nel settore della cooperazione giudiziaria e di polizia. La

prospettiva del lavoro *in itinere* è di pervenire ad una visione condivisa tra autorità nazionali ed EDPS per poi, in caso positivo, formulare delle proposte per adeguare il quadro normativo. Si è discusso circa l'opportunità di diminuire la pluralità di forme di supervisione oggi esistenti, prevedendo ove possibile un unico sistema di supervisione coordinata tra le autorità nazionali ed il Garante europeo, per tutti quei trattamenti di dati che prevedono la creazione di un *database* centralizzato a livello europeo o scambi analogamente strutturati.

PRISM

Alla luce delle recenti rivelazioni apparse sulla stampa ed ai documenti successivamente resi pubblici in merito al programma PRISM (*Planning Tool for Resource Integration, Synchronization, and Management*) ed altri programmi di raccolta dati a fini di *intelligence*, il Gruppo ha ampiamente dibattuto sulle conseguenze per i cittadini europei di tali attività in vista di una propria presa di posizione – attraverso la predisposizione di un parere in materia di sorveglianza delle comunicazioni elettroniche (previsto per il 2014) – che si soffermi in particolare sul rapporto tra la normativa europea in materia di protezione dati e i programmi di *intelligence* statunitensi. Al riguardo, è stata svolta un'analisi del quadro legale esistente a livello nazionale ed europeo in materia, prendendo in considerazione le basi normative su cui operano i sistemi di supervisione e controllo previsti dagli ordinamenti nazionali. Particolare attenzione è stata rivolta alle richieste della Commissione europea, che ha insistito sulla necessità di maggiore trasparenza nei programmi di *intelligence* e sulla possibilità di un effettivo controllo sulla loro legittimità.

In questa prospettiva è stato quindi redatto ed inviato un questionario alle diverse autorità di protezione dei dati per conoscere le modalità di supervisione sui trattamenti effettuati dai servizi segreti nazionali. È stato affidato al Garante, unitamente all'Autorità ceca, il compito di sviluppare il tema dei sistemi di sorveglianza all'interno dell'Europa e della supervisione dei servizi di sicurezza, al fine di elaborare proposte e raccomandazioni nel parere in preparazione.

In relazione ai menzionati programmi di *intelligence*, il Gruppo Art. 29 ha inoltre manifestato le proprie perplessità alla vicepresidente della Commissione europea Viviane Reding con due lettere, rispettivamente del 7 giugno 2013 (doc. web n. 3019822) e del 13 agosto 2013 (doc. web n. 3019832). In particolare le richieste di chiarimento contenute in tali lettere mirano a comprendere se il programma PRISM implichi il trattamento solamente di dati di cittadini e residenti degli Stati Uniti o se sia invece rivolto anche ai cittadini europei e se l'accesso a tali dati sia mirato o casuale. Il Gruppo ha inoltre comunicato alla vicepresidente Reding l'intenzione di analizzare il quadro legale esistente a livello nazionale ed europeo riguardo all'applicazione della normativa in materia di protezione dati nel contesto dei citati programmi di raccolta dati.

Parere sul concetto di necessità

Sempre in tema di *law enforcement*, il Gruppo ha cominciato a ragionare sulla predisposizione di un parere sul concetto di necessità, calendarizzato per il 2014. Tale parere mira a chiarire i concetti di necessità e proporzionalità – anche alla luce della giurisprudenza della Corte di Strasburgo in relazione all'art. 8 della Convenzione europea per i diritti dell'uomo – nelle misure esistenti predisposte dai legislatori (a più livelli, nazionale o europeo) per rispondere alle esigenze di giustizia e sicurezza.

Accesso ai dati trattati nell'ambito dell'Accordo TFTP2 - programma di controllo delle transazioni finanziarie dei terroristi

In tema di diritti e trasferimento dei dati all'estero, il Gruppo Art. 29 ha poi adottato un modello per l'applicazione uniforme delle procedure relative all'esercizio del diritto di accesso ai dati personali trattati dal Dipartimento del Tesoro statunitense nell'ambito dell'Accordo TFTP2 (Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (doc. web n. 2613438).

L'Accordo TFTP prevede infatti il diritto di chiunque di accedere ai dati personali che lo riguardano trattati sulla base dell'accordo medesimo e di chiederne la rettifica, la cancellazione o il blocco qualora i medesimi siano inesatti o il trattamento sia in contrasto con l'accordo. Chiunque intenda esercitare tali diritti può presentare una richiesta alla propria autorità nazionale di controllo nell'Unione europea (per l'Italia, il Garante), che agirà da tramite con il Dipartimento del Tesoro statunitense, attraverso apposita modulistica pubblicata sul sito dell'Autorità (cfr. doc. web nn. 2613468, 2613478, 2613488, 2613498).

Border and Travel

Il Gruppo ha esaminato le proposte contenute nello *Smart border package* presentato dalla Commissione e composto di due Proposte di regolamento: la prima relativa all'istituzione di un sistema di ingressi/uscita per cittadini di Paesi terzi che attraversano le frontiere esterne degli Stati membri UE; la seconda all'istituzione di un programma per viaggiatori registrati. Il 6 giugno 2013 ha quindi adottato il Parere n. 5/2013 nel quale, in particolare, si stigmatizzano sia la creazione di un nuovo profilo criminale, quello dei migranti che si trattengono oltre la scadenza del titolo, sia la realizzazione di una ulteriore banca dati centrale oltre a VIS, SIS, Eurodac, nella quale confluirebbero, ai fini della lotta contro l'immigrazione irregolare, i dati personali di chi entra in Europa (doc. web n. 2572931).

Con riferimento al tema dello *screening* anticipato dei passeggeri, è proseguita l'analisi dell'attività dell'*International Air Transport Association* (IATA) e del nuovo modello (NDC) di profilazione degli acquirenti o potenziali acquirenti di biglietti aerei. Il modello NDC realizza un sistema d'individuazione del prezzo del volo basato sulla previa fornitura di una serie di informazioni, anche sensibili, della persona. Grazie al *Dynamic Airline Shopping engine Application Programme Interface* (DAS API) ed alla tecnologia dei messaggi XML, le compagnie aeree potranno fornire un servizio personalizzato agli utenti, basato sullo scambio di dati tra le agenzie di viaggio e gli utenti e le compagnie aeree stesse, ossia sul contenuto della richiesta inoltrata dai viaggiatori o dagli intermediari che agiscono per conto del consumatore finale alle compagnie aeree, tramite messaggio XML. Il menzionato sistema ha suscitato preoccupazioni considerato che il tipo di prodotto, il prezzo e i servizi accessori complementari, verrebbero offerti al cliente in base alle informazioni, tra cui dati personali, riferite a particolari necessità e preferenze, contenute nel predetto messaggio XML.

Protezione dei dati in ambito finanziario

È proseguito il lavoro di approfondimento sui profili di protezione dei dati nel settore finanziario. In particolare il Gruppo Art. 29 si è dedicato all'analisi delle nuove proposte in ambito europeo in materia di contrasto al riciclaggio e al finanziamento del terrorismo e all'impatto che tali disposizioni possono avere sulla protezione dei dati. La linea di tendenza a livello UE è parsa quella di un inasprimento della lotta al riciclaggio e al finanziamento del terrorismo senza però che siano tenuti in dovuta considerazione i diritti delle persone. In tale prospettiva e in linea con le posizioni già assunte dal Gruppo nel Parere n. 14/2011 (doc. web n. 2982816) e dall'EDPS con il Parere del 4 luglio 2013, il Gruppo ha predisposto due lettere, rispettivamente del 4 aprile 2013 (doc. web n. 2982756) e dell'8 novembre 2013 (doc. web n. 2982696), indirizzate al Presidente della Commissione LIBE del Parlamento europeo, con le quali ha manifestato forti preoccupazioni riguardo all'impatto che la proposta di direttiva sulla prevenzione del riciclaggio e la proposta di regolamento sui dati informativi che accompagnano i trasferimenti di fondi potrebbero avere sui diritti delle persone.

Un altro settore di indagine a cui il Gruppo si è dedicato nel corso dell'anno riguarda la profilazione dei clienti nell'ambito creditizio. Attraverso appositi questionari veicolati dalle autorità di protezione dei dati rivolti alle cd. centrali rischi che operano su territorio nazionale, il Gruppo ha svolto un lavoro di approfondimento volto a valutare il livello di adempimento dei principi *privacy* nel settore.

Trasferimento di dati all'estero

Il sistema previsto dagli artt. 25 e 26 della direttiva 95/46/CE per i trasferimenti dei dati verso Paesi terzi e, in particolare, gli strumenti quali il *Safe Harbour*, le clausole contrattuali *standard* e le regole vincolanti d'impresa (BCR) sono stati messi in discussione, nel corso del 2013, a seguito delle notizie relative ai programmi di sorveglianza di massa posti in essere dalle autorità statunitensi (e non solo) a fini di *intelligence* e di sicurezza nazionale e dal sempre maggior utilizzo da parte di soggetti pubblici e privati dei servizi di *cloud computing* (cfr., ad es., lo studio, pubblicato nel 2013 dalla Commissione libertà civili, giustizia e affari interni del Parlamento europeo, "*The US surveillance programmes and their impact on EU citizens' fundamental rights*" (doc. web n. 2983032).

In realtà, *Safe Harbour*, clausole contrattuali *standard* e regole vincolanti d'impresa (BCR) non contengono disposizioni specifiche a tutela degli interessati nel caso di accesso da parte di soggetti pubblici per finalità di sorveglianza (per di più di massa), poiché sono stati creati per governare i flussi transfrontalieri nell'ambito del settore privato e non possono pertanto costituire in alcun modo il fondamento giuridico di un trasferimento di dati per tali altre finalità.

Al riguardo, una riflessione sul tema è stata avviata, in seno al Gruppo, in occasione della decisione di predisporre, nell'ambito del sottogruppo BTLE, il parere relativo alla sorveglianza delle comunicazioni elettroniche a fini di *intelligence* e di sicurezza nazionale (cfr. *supra*) che affronterà, per una parte, anche l'aspetto relativo ai fondamenti normativi vigenti per trasferire dati personali verso gli USA e le condizioni che devono ricorrere alla luce, in particolare, della direttiva 95/46/CE e della Carta dei diritti fondamentali.

BCR e clausole contrattuali *for processor*

Con l'intento invece di rispondere alle sempre più pressanti esigenze di disciplinare i flussi di dati personali nell'ambito di forme di esternalizzazione delle attività di trattamento (quali, ad es., proprio i predetti servizi di *cloud computing*), il Gruppo ha adottato un documento esplicativo delle BCR *for processor* (doc. web n. 2572911) e ha avviato, nell'ambito del sottogruppo *International transfers*, un confronto volto alla predisposizione di un *set* di clausole contrattuali "*for processor*". Tali clausole potranno essere utilizzate – sulla scorta di quanto avviene, ad esempio, nell'ordinamento spagnolo – nei casi in cui un responsabile del trattamento stabilito sul territorio europeo intenda sub-appaltare attività di trattamento di dati personali a soggetti stabiliti in Paesi terzi. Allo stato, anche nel nostro ordinamento, siffatto trasferimento di dati può essere posto in essere dal responsabile del trattamento sulla base di un apposito mandato per la sottoscrizione di clausole contrattuali tipo di cui all'allegato della Decisione della Commissione europea del 5 febbraio 2010, n. 87/2010/UE, conferitogli dal titolare (cfr. Relazione 2012, p. 209 e doc. web n. 2191156).

Per quanto concerne le BCR *for processor* (BCR-P), il documento esplicativo ribadisce che le stesse hanno lo scopo di consentire, nel rispetto delle garanzie previste dalla disciplina di protezione dei dati e senza la necessità di stipulare ogni volta specifici contratti, il trasferimento di dati personali da parte di una società di servizi/responsabile del trattamento situata sul territorio europeo ad una società del medesimo gruppo situata in un Paese terzo e illustra gli elementi essenziali che devono essere contenuti nel contratto generale di servizi (*Service Level Agreement* – SLA) sottoscritto con il cliente/titolare del trattamento e nel resto delle BCR che devono essere allegate al predetto contratto.

Con riferimento agli aspetti procedurali, il documento chiarisce che è la multinazionale interessata a dover presentare l'istanza per l'approvazione delle BCR-P secondo quanto previsto dalla procedura di approvazione da parte delle autorità di protezione dei dati stabilita dal documento di lavoro adottato il 14 aprile 2005 (doc. web n. 1296169) (cfr. Relazione 2005, p. 144), mentre l'autorizzazione nazionale dovrà essere richiesta da ciascun titolare del trattamento che ritenga di avvalersi, in qualità di responsabili del trattamento, di società multinazionali che intendano uti-

lizzare, per trasferimenti di dati verso Paesi terzi, BCR-P già approvate. In tale occasione, copia del contratto generale di servizi dovrà essere presentato alla competente autorità di protezione dei dati al fine di verificare la liceità del trattamento alla luce delle normative nazionali.

Sebbene lo strumento sia stato predisposto dal Gruppo solo a dicembre 2012, già nel 2013 sono state avviate nove procedure europee di approvazione di BCR-P e, tra esse, nel novembre 2013, una ha già concluso il suo *iter* di approvazione.

BCR *for controller*

Per quanto riguarda le BCR *for controller* (BCR-C), lo strumento è già ampiamente conosciuto e utilizzato dalle multinazionali (cfr. Relazioni precedenti), tanto che, nel corso del 2013, sono state avviate ventuno procedure europee di approvazione di BCR-C e sette, iniziate negli anni precedenti, sono state chiuse con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute (per le autorizzazioni nazionali si fa rinvio al par. 13). In tre occasioni il Garante ha operato in qualità di *co-reviewer* insieme all'autorità di protezione dei dati *leader* della procedura (per uno schema esplicativo delle procedure di approvazione, cfr. doc. web n. 2037871), fornendo specifiche indicazioni in ordine a modifiche da apportare nel testo delle BCR proposte dalle società al fine di renderle conformi al quadro normativo europeo.

Adeguatezza e *Referential* BCR/CBPR

Sempre in tema di trasferimento dei dati all'estero, il Gruppo, attraverso il sottogruppo *International transfers*, ha continuato a lavorare ad un documento ("*Referential*") che raccoglie gli elementi comuni tra il sistema BCR europeo e l'analogo sistema delle *Cross Border Privacy Rules*-CBPR adottato in ambito Apec (Cooperazione Economica Asiatico-Pacifica). Il documento, che dovrebbe essere adottato dall'Apec e dal Gruppo nel 2014, intende fornire indicazioni utili per le multinazionali che desiderino adottare regole vincolanti d'impresa che possano ottenere sia un'approvazione europea che una certificazione Apec.

Con riguardo all'attività volta a valutare l'adeguatezza della disciplina nazionale di Paesi terzi, sono inoltre all'attenzione del Gruppo la legge del Québec e la Comunicazione sul funzionamento del *Safe Harbour* (doc. web n. 2983002) con la quale, il 27 novembre 2013, la Commissione (soggetto competente, ai sensi dell'art. 25, comma 6, della direttiva 95/46/CE, a valutare periodicamente l'adeguatezza del regime già riconosciuta con la decisione n. 2000/520/CE), dopo aver illustrato alcuni aspetti critici del sistema, ha fornito tredici raccomandazioni per migliorarne il funzionamento. A quest'ultimo proposito, la Commissione ha chiesto di apportare miglioramenti al regime in tema di trasparenza, di tutela dei diritti degli interessati e di *enforcement* e ha rappresentato la necessità di una maggiore trasparenza da parte delle società iscritte al *Safe Harbour* in ordine ai casi in cui, per motivi di sicurezza nazionale, interesse pubblico o *law enforcement*, le stesse non rispettino i principi del *Safe Harbour*, ricordando che la deroga prevista per la sicurezza nazionale deve essere utilizzata in misura strettamente necessaria e proporzionata. Il riesame dell'intero sistema dovrebbe essere portato a termine dalla Commissione nel 2014 in modo da poter prendere in considerazione le misure di attuazione che le autorità statunitensi intenderanno dare alle raccomandazioni.

Trattamenti effettuati dall'Agenzia mondiale anti-*doping*

Il tema dell'adeguatezza della legge del Québec presenta un peculiare profilo di rilevanza in ragione della circostanza che in tale ordinamento l'Agenzia mondiale anti-*doping* (*World Anti-Doping Agency*-WADA) raccoglie e tratta, attraverso la banca dati ADAMS, i dati personali che gli atleti sono tenuti a comunicare sia direttamente, sia attraverso le federazioni sportive di appartenenza e le competenti organizzazioni nazionali per le finalità anti-*doping*. Nel marzo 2013, nell'ambito della consultazione avviata dall'Agenzia mondiale anti-*doping* in occasione della revisione del codice mondiale e degli *standard* che lo completano, il Gruppo è tornato sull'argomento con una lettera (cfr. doc. web nn. 2983092 e 2983102) con la quale, nel riprendere le conside-

razioni già svolte sul tema nel 2008 e nel 2009 – in occasione dell'adozione di pareri WP 156 (doc. web n. 1619614) e WP 162 (doc. web n. 1620339)–, ha riproposto le proprie perplessità in ordine ad alcuni aspetti della disciplina rimasti invariati rispetto al passato: la funzione del consenso quale presupposto legittimante il trattamento, i lunghi periodi di conservazione dei dati e di pubblicazione delle sanzioni, il rispetto del principio di proporzionalità nel trattamento dei dati relativi ai *whereabouts* (ovvero le informazioni volte a consentire la reperibilità degli atleti ai fini di controlli anti-*doping*), l'uso della banca dati ADAMS e l'assenza di un adeguato quadro giuridico per i flussi transfrontalieri dei dati.

Dal momento che con il nuovo Codice WADA e i relativi *standard*, adottati a novembre 2013, molti dei rilievi mossi dal Gruppo non sono stati recepiti, sono allo stato oggetto di discussione in seno al Gruppo medesimo le iniziative che le autorità di protezione dei dati dovranno porre in essere, anche sul piano nazionale, affinché i trattamenti effettuati dalle competenti organizzazioni nazionali anti-*doping*, ivi compresi i trasferimenti di dati verso la banca dati ADAMS, siano conformi alla disciplina di protezione dei dati.

Supervisione IMI

Con l'entrata in vigore, il 4 dicembre 2012, del Regolamento (UE) n. 1024/2012, è divenuto obbligatorio per la cooperazione amministrativa tra autorità competenti degli Stati membri nel settore del mercato interno l'utilizzo del sistema *Internal Market Information* (IMI). Si tratta di un'applicazione *software* (multilingue ed accessibile tramite internet) sviluppata dalla Commissione in collaborazione con gli Stati membri volta a favorire e accelerare lo scambio transfrontaliero di informazioni, anche personali, e la mutua assistenza previsti in diversi atti dell'Unione (direttiva sui servizi, direttiva sulle qualifiche professionali, direttiva sui diritti dei pazienti, regolamento sul trasporto transfrontaliero professionale di contante in euro, raccomandazione sulla rete per la soluzione dei problemi nel mercato interno-SOLVIT, nonché, sulla base di un progetto pilota, la direttiva sul distacco dei lavoratori).

Trattandosi di un sistema centralizzato, anche in questo caso la Commissione ha ritenuto necessario prevedere uno specifico organismo di supervisione. Il nuovo sistema di supervisione formato dalle autorità competenti a livello nazionale (le autorità di protezione dei dati) e dall'EDPS (cfr. art. 21 del regolamento medesimo) affida a quest'ultimo, come pure accade in altri sistemi, il segretariato del gruppo di supervisione.

L'art. 21 prevede, infatti, che l'autorità o le autorità nazionali di controllo designate in ogni Stato membro e dotate dei poteri di cui all'art. 28 della direttiva 95/46/CE (per l'Italia il Garante) verifichino in modo indipendente la liceità del trattamento dei dati personali da parte dei partecipanti all'IMI del loro Stato membro, garantendo la tutela dei diritti degli interessati. Al controllo da parte delle autorità nazionali si somma quello del Garante europeo della protezione dei dati (EDPS). In particolare, l'EDPS controlla e provvede a garantire che le attività di trattamento dei dati personali della Commissione, nella veste di partecipante all'IMI, si svolgano in conformità al regolamento.

19.4. *La cooperazione delle Autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

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

Nel 2013, l'attività dell'ACC Europol, che a marzo ha eletto i nuovi organi (presidente la slovena Natasa Pirc, DP e *Information Commissioner* della Slovenia e vicepresidente Vanna Palumbo del Garante), si è incentrata sull'analisi dell'impatto della proposta presentata dalla Commissione europea di un regolamento che istituisce l'Agenzia dell'Unione europea per la cooperazione e la formazione delle autorità di contrasto (Europol) e abroga le decisioni nn. 2009/371/GAI e 2005/681/GAI del Consiglio.

La proposta, presentata formalmente dalla Commissione europea il 27 marzo 2013 (doc. web n. 2983062), prevede, da un lato, l'assorbimento da parte di Europol delle attività svolte dall'Accademia Europea di Polizia - CEPOL e, dall'altro, un ampliamento dei reati per i quali l'Europol è competente (nonché dei relativi poteri d'indagine), sviluppando anche le sue capacità di fornitore di servizi di comunicazione elettronica (SIENA) e di "*hub*" informativo per i Paesi membri.

Una scelta di fondamentale impatto per l'attività delle autorità di protezione dati è quella operata dalla Commissione riguardo la supervisione dei trattamenti di dati effettuati da Europol, attribuita al Garante europeo della protezione dei dati personali, come anche la competenza in materia di esercizio del diritto di accesso degli interessati e la decisione in merito ad eventuali ricorsi da questi presentati. Il modello di supervisione con al centro l'EDPS viene quindi progressivamente esteso dalla Commissione ad ogni nuovo strumento legislativo (anche le proposte concernenti Eurojust ed il procuratore europeo (EPPO) sono sulla stessa linea). I Garanti europei hanno discusso nella conferenza di primavera il tema, adottando una risoluzione abbastanza critica e preoccupata (v. par. 19.2) (doc. web n. 2980604).

L'Autorità di controllo comune Europol ha a sua volta adottato due pareri, il primo nel giugno ed il secondo nell'ottobre 2013, sulla proposta di regolamento. Con il primo parere (doc. web n. 2983184), anche sulla scorta della richiamata risoluzione dei Garanti europei, ha rilevato che l'ampliamento del ruolo e delle responsabilità di Europol avverrebbe a scapito della certezza giuridica necessaria a garantire la correttezza e controllabilità del suo operato, in particolare, nella misura in cui gli verrebbero attribuiti un compito di coordinamento nelle indagini e una competenza non più per "grave reato" ("*serious crime*") ma sulla base del più indeterminato criterio delle "forme di criminalità che ledono un interesse comune oggetto di una politica dell'Unione", nonché un ulteriore e non disciplinato ruolo di *provider* di servizi di comunicazione elettronica. Il parere si sofferma inoltre sull'effetto di tali cambiamenti sulle modalità di trattamento dei dati e quindi sulla struttura dei sistemi informatici finora creati (e, come noto, controllati con cadenza annuale dall'ACC attraverso il suo gruppo ispezioni) e sull'impatto degli stessi sulla supervisione dei trattamenti di dati personali effettuati.

Un secondo, più analitico parere è stato adottato il 9 ottobre 2013 (doc. web n. 2983132). Con lo stesso si evidenziano le lacune e le contraddizioni del testo proposto dalla Commissione rispetto alle finalità dichiarate e il conseguente rischio di una riduzione delle garanzie previste in materia di protezione dei dati rispetto a quelle della decisione n. 2009/371/GAI attualmente in vigore. Gran parte dei rilievi si fondano sull'esperienza acquisita dall'ACC nell'espletamento dei suoi compiti di controllo della legittimità dei trattamenti di dati effettuati da Europol, in particolare in occasione dell'ispezioni svolte in *loco*. Il parere è stato inviato al Consiglio, che ha in discussione il testo della proposta di regolamento, ed al Parlamento europeo.

L'ACC ha inoltre svolto, come di consueto, il controllo annuale sui trattamenti di dati effettuati da Europol e ha approvato il rapporto sull'attività ispettiva svolta. Il Garante ha partecipato con un proprio esperto all'ispezione svolta nel 2013 che ha incluso anche la verifica delle modalità con cui Europol effettua i trattamenti di dati in relazione ai compiti affidati dall'Accordo USA-UE sul TFTP (l'Accordo sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi).

Rispetto a tale tipologia di trattamento, l'ACC ha reso pubblica intanto, come era già avvenuto per l'anno precedente, una breve sintesi che illustra gli esiti della terza (ed ultima specifica) ispezione condotta nel novembre 2012 (doc. web n. 2983142) e ha accolto la richiesta dell'Ombudsman europeo di poter accedere alla parte secretata del rapporto sull'ispezione.

Per quanto riguarda l'attività dei sottogruppi, ci sono stati due incontri con i rappresentanti di Europol presso la sede dell'Aja per continuare l'analisi delle modalità di fornitura ed uso della rete per lo scambio di informazioni SIENA (che collega Europol alle autorità preposte ad attività di contrasto negli Stati membri e ad altri partner). Anche sulla scorta di tali incontri, l'ACC ha adottato, a dicembre, uno specifico parere sul tema. Altri pareri hanno riguardato due progetti di accordi operativi con Serbia e Albania (doc. web nn. 2983122 e 2983112) e le future attività di Europol (doc. web n. 2983162).

L'ACC ha adottato inoltre il rapporto sulle attività svolte nel quadriennio 2008-2012 (doc. web n. 2996478) e un rapporto sul funzionamento delle Unità nazionali Europol con particolare riguardo alla fase di introduzione dei dati nei sistemi Europol o di loro invio (doc. web n. 2983152). Quest'ultimo rapporto, traendo le conclusioni dalle risposte pervenute ad un questionario predisposto nel 2012, evidenzia la non completa armonizzazione del ruolo e delle responsabilità attribuiti, nei diversi Stati membri, alle Unità nazionali e formula alcune raccomandazioni al riguardo.

Il Sistema Informativo Schengen: l'attività dell'Autorità di controllo comune [ACC] Schengen e il nuovo Gruppo di coordinamento della supervisione SIS II

Dal 9 aprile 2013 è attivo il Sistema d'informazione Schengen di seconda generazione (SIS II). Dalla stessa data, pertanto, è cambiata la base giuridica per il trattamento dei dati personali effettuato nel sistema – non più disciplinato dalla Convenzione "Schengen" (integrata nel quadro istituzionale e giuridico dell'Unione europea nel 1999) ma dal Regolamento (CE) n. 1987/2006 di Parlamento europeo e Consiglio del 20 dicembre 2006 e dalla decisione n. 2007/533/GAI del Consiglio del 12 giugno 2007 che istituiscono e disciplinano il SIS II (doc. web nn. 2983012 e 2982882) – e l'Autorità comune di controllo Schengen ha concluso la propria attività di supervisione e controllo.

Il sistema SIS II, operativo dal 1995, ha lo scopo di aumentare la sicurezza e di facilitare la libera circolazione nello spazio Schengen, permettendo alle autorità nazionali doganali, di polizia e di controllo delle frontiere di scambiarsi agevolmente informazioni. Il Sistema contiene infatti segnalazioni sulle persone scomparse (soprattutto minori) e informazioni su determinati beni (quali banconote, automobili, furgoni, armi da fuoco e documenti di identità) che potrebbero essere stati rubati, sottratti o smarriti. È dotato di funzioni avanzate, come la possibilità di inserire dati biometrici (impronte digitali e fotografie), nuovi tipi di segnalazioni (aeromobili, natanti, *container* e mezzi di pagamento rubati) o la possibilità di collegare segnalazioni diverse (ad es., una segnalazione su una persona e su un veicolo). Il SIS II contiene copie dei mandati d'arresto europei collegati direttamente a segnalazioni per l'arresto a fini di consegna o di estradizione.

L'accesso al sistema è limitato alle autorità nazionali giudiziarie, doganali e di polizia e a quelle competenti per il controllo delle frontiere, i visti e i certificati di immatricolazione per veicoli. Come per il SIS I, chiunque ha il diritto di accedere ai dati che lo riguardano inseriti nel nuovo sistema può chiedere all'autorità nazionale competente di rettificare o cancellare i propri dati personali. Inoltre, chiunque può agire in giudizio per accedere alle informazioni, rettificarle, cancellarle o per ottenere un indennizzo nel caso di segnalazione che lo riguardi inserita illecitamente. È anche previsto che, almeno ogni 4 anni, si proceda ad una verifica della conformità dei trattamenti effettuati.

L'entrata in funzione del SIS II è stata accompagnata, come previsto dalle nuove basi giuridiche, da una campagna informativa in tutti i Paesi secondo modelli *standard* plurilingue, predisposti dalla Commissione che dovrebbero essere distribuiti sia nei punti di frontiera sia sul territorio.

In questo quadro di cambiamento, l'ACC Schengen – di cui sono stati fatti circolare i rapporti di attività (2008 - aprile 2013, doc. web n. 2982892) – ha tenuto la sua

ultima riunione nella pienezza dei poteri nel marzo 2013, adottando il rapporto relativo ai lavori di verifica sull'inserimento nel sistema delle segnalazioni *ex* art. 95 della Convenzione (mandato di arresto europeo) e lasciando al Gruppo di coordinamento della supervisione SIS II – cui ha passato il testimone – il compito di portare a termine le attività avviate in relazione all'esercizio del diritto di accesso e ai criteri per l'introduzione nel sistema delle segnalazioni relative a veicoli rubati.

Il Gruppo di coordinamento – che si è riunito, per la prima volta, nel giugno 2013, adottando il regolamento interno ed eleggendo, quale presidente, Clara Guerra, dell'Autorità di protezione dei dati portoghese, e, come vicepresidente, David Cauchi, del Garante maltese – è stato informato, da rappresentanti della DG Affari interni della Commissione europea e dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA), su modi e forme del passaggio dal SIS I al SIS II, avvenuto senza problemi dal punto di visto informatico ed operativo. Il menzionato Gruppo ha poi costituito un sottogruppo tecnico incaricato, tra l'altro, di seguire gli sviluppi di un'indagine avviata su un grave caso di *data breach* al SIRENE danese, avvenuto a seguito di un attacco di *hacker* e reso noto nel giugno 2013. Proprio alla luce di tale evento, gli Stati Schengen sono stati chiamati, attraverso la compilazione di un questionario, a svolgere un *self-assessment* dei sistemi nazionali e della sicurezza della trasmissione dei dati, anche tenendo conto di eventuali forme di *outsourcing*/subcontratto nella gestione operativa degli stessi.

Il Sistema informativo doganale (SID): ACC Dogane e Gruppo di coordinamento della supervisione SID

L'ACC Dogane e il Gruppo di coordinamento della supervisione del Sistema informativo doganale (SID) si riuniscono normalmente insieme in quanto condividono la supervisione sullo stesso *database* in cui sono trattati dati di cooperazione doganale relativi agli *ex* primo e terzo pilastro.

L'ACC Dogane ha proseguito la sua attività adottando il rapporto di attività fino a dicembre 2013, il nuovo programma di lavoro e una lettera sull'accesso al SID attraverso un singolo punto di contatto. È stata inoltre messa a punto una *brochure* informativa, dal titolo "Guida alle vostre responsabilità", rivolta alle autorità doganali ed alle altre autorità che hanno accesso al SID, che fornisce indicazioni per i casi in cui i dati inseriti nel sistema doganale comune SID non siano accurati o leciti (art. 13 della decisione SID 2009/917 ed art. 8 (2) della decisione quadro protezione dati 2008/977).

Il Gruppo di coordinamento della supervisione SID ha confermato per un secondo ed ultimo mandato Presidente e Vicepresidente. Sono in corso attività relative alla verifica della lista delle autorità che possono avere accesso al SID (comunicate da ciascuno Stato membro alla Commissione europea) e verrà esaminata, al fine di predisporre un parere, la proposta di modifica del Regolamento presentata a novembre 2013 dalla Commissione europea e l'ulteriore proposta di modifica della supervisione del sistema (doc. web n. 2983022).

Il Sistema Informativo Visti (VIS): Gruppo di coordinamento della supervisione VIS

Il Gruppo di coordinamento della supervisione VIS, che ha approvato il regolamento interno ed ha proceduto alla elezione del Presidente (Peter Hustinx, EDPS) e del Vicepresidente (Vanna Palumbo, del Garante), ha conferito lo *status* di osservatori, su loro richiesta, ad Irlanda e Regno Unito, Paesi non partecipanti alla cooperazione Schengen ed alle misure dell'Unione adottate sulla base di questa (in sostanza, la quasi totalità delle attività in materia di asilo ed immigrazione, controllo delle frontiere *etc.*).

È stato discusso e adottato il programma di attività per il biennio 2013-2014, anche con riferimento all'attività di supervisione. Tale attività riguarderà non solo la parte centrale del sistema, posta sotto la responsabilità operativa dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA), ma anche le parti nazionali del VIS; oggetto di verifica sarà anche il modo in cui le forze dell'or-

dine hanno accesso ai dati secondo quanto previsto dalla decisione 2008/633/GAI. Sul tema dello sviluppo di possibili *standard* per effettuare le ispezioni, sia a livello nazionale sia congiuntamente, ad esempio nei Paesi in cui gli uffici diplomatici di uno Stato membro emettono visti anche per altri Stati UE, il Gruppo sta valutando se e quali *standard* internazionali possono essere applicati, cercando di mantenere la sinergia con il lavoro già fatto dal Gruppo Eurodac (che potrà essere adattato alle specificità delle verifiche sul VIS). Il Gruppo ha poi esaminato le implicazioni per la protezione dei dati del sistema, in particolare per quanto riguarda i responsabili del trattamento (*sub contractors*). Al riguardo è stato deciso di istituire un piccolo sottogruppo che approfondirà il tema, anche basandosi sulle ispezioni nelle sedi di tali soggetti già effettuate da alcune DPA.

Quanto alle attività del prossimo biennio, l'attenzione del Gruppo si focalizzerà oltre che sugli aspetti sopra indicati, sui soggetti che possono accedere al sistema, sulle modalità di esercizio del diritto di accesso, rettifica, *etc.*, nonché sulle modalità di accesso delle LEAs al sistema.

Gruppo di supervisione Eurodac

L'attenzione del Gruppo è stata in massima parte rivolta ad un'analisi degli sviluppi derivanti dall'adozione, il 26 giugno 2013, della proposta di rifusione (cd. *recast*) del regolamento Eurodac (regolamento (UE) n. 603/2013, doc. web n. 2983052) che, tra l'altro, renderà possibile l'accesso ai dati contenuti nella banca dati Eurodac da parte delle forze di polizia, con conseguenti modifiche all'architettura del sistema (quali la possibilità di consultare il *database*, ai fini di polizia, anche a partire da frammenti di impronta ritrovati sulla scena del crimine).

Tenendo conto della sensibilità del trattamento dei dati di richiedenti asilo, l'accesso agli stessi sarà consentito a polizia ed inquirenti e ad Europol solo qualora dall'interrogazione delle banche dati di polizia nazionali o del VIS non emergano già riscontri: garanzie, queste, non ritenute tuttavia sufficienti dai Garanti che hanno eccepito, oltre alla mancata dimostrazione della necessità e proporzionalità della misura, la finalità "incompatibile" dell'utilizzo dei dati previsto dal regolamento rispetto alla finalità della loro raccolta.

Alla luce di ciò, il Gruppo EURODAC ha deciso di focalizzare anche le prossime attività sulla valutazione del nuovo regolamento, con lo scopo di influenzare la definizione dell'architettura del sistema, in particolare introducendo delle funzionalità che consentano di registrare separatamente gli accessi delle forze di polizia da quelli delle autorità competenti per le procedure di asilo. Ciò considerato anche che dalla data di adozione del testo a quella dell'entrata in funzione del sistema nella nuova forma intercorreranno due anni (il regolamento entrerà in vigore infatti il 20 luglio 2015).

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

A maggio 2013, alla luce delle risposte fornite dalle competenti autorità nazionali ad un questionario volto a verificare le modalità utilizzate per la raccolta delle impronte digitali dei richiedenti asilo e le conseguenze in caso di impronte illeggibili (cfr. anche Relazione 2012, p. 294), il Gruppo ha approvato il rapporto sull'ispezione coordinata sulle impronte illeggibili con cui si raccomanda l'adozione di procedure uniformi nei diversi Stati membri e l'introduzione da parte del legislatore europeo di una specifica disposizione che preveda espressamente che il semplice possesso di impronte illeggibili non determini effetti negativi sulla procedura di riconoscimento dello *status* di rifugiato (doc. web n. 2985748).

19.5. *La partecipazione ad altri comitati e gruppi di lavoro*

IWGDPT: il Gruppo di Berlino - *International Working Group on Data Protection in Telecommunication*

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication*, cd. Gruppo di Berlino, che nel corso del 2013 si è riunito come d'uso due volte (a Praga in primavera ed a Berlino a fine estate).

In qualità di relatore, l'Autorità ha lavorato all'adozione del documento sulla pubblicazione di dati personali sul web, adottato nella riunione di Praga, che, affrontando il tema da un punto di vista tecnologico, ha individuato metodologie e soluzioni per realizzare un efficace esercizio del diritto all'oblio. Il documento ha fornito inoltre precise raccomandazioni per ciascuno degli attori coinvolti (*webmaster*, motori di ricerca) e buone pratiche tecnologiche, evidenziando che il raggiungimento di un'effettiva tutela dei diritti degli interessati richiede un approccio multilaterale fondato sull'azione coordinata dei vari *stakeholder* (doc. web n. 2982786).

Nel documento di lavoro sul *web tracking* adottato nella stessa riunione ed essenzialmente indirizzato ai fornitori di siti web, sviluppatori di *software* e di tecnologie che consentono il tracciamento degli utenti della rete, il Gruppo ha fornito specifiche raccomandazioni volte a garantire trasparenza e controllo da parte degli interessati. In particolare, occorre valorizzare e attuare anche nel contesto del *tracking*, il rispetto della finalità del trattamento evitando che pratiche di condivisione dei dati rendano possibile il loro utilizzo in un contesto diverso da quello della raccolta e all'insaputa dell'interessato (doc. web n. 2982776).

La riunione di Berlino ha invece portato all'adozione di due ulteriori documenti, rispettivamente sulla segretezza delle telecomunicazioni e sulla sorveglianza aerea.

Il primo, in risposta ai recenti fatti legati alla sorveglianza delle comunicazioni svolta su scala mondiale dalle autorità di *law enforcement* e dai servizi segreti di alcuni Paesi, esorta i governi a: riconoscere la segretezza delle comunicazioni come una parte essenziale del diritto alla vita privata e a rafforzarla anche attraverso il suo riconoscimento, tra i diritti fondamentali, in una convenzione internazionale; predisporre *standard* internazionali volti a limitare l'accesso, da parte delle autorità pubbliche, ai dati personali conservati dai fornitori di servizi internet; incoraggiare l'impiego di forme sicure di comunicazione tra i cittadini e assicurare un controllo indipendente ed effettivo riguardo alle attività di sorveglianza svolte dalle autorità di polizia e di *intelligence* o, per loro conto, da soggetti privati (doc. web n. 2982796).

Nel documento di lavoro sulla sorveglianza aerea, il Gruppo ha inteso sottolineare che la particolare intrusività e invisibilità dell'impiego di nuovi dispositivi quali i droni, unita al fatto che essi portano a una sorveglianza indiscriminata e potenzialmente continua sulle persone, rende ineludibile l'implementazione di misure specifiche: prima di tutto garantire che l'impiego della sorveglianza aerea sia limitata a specifiche finalità, ad esempio la ricerca di persone scomparse; far sì che l'impiego di immagini raccolte attraverso i droni dalle autorità pubbliche sia soggetto a mandato giudiziario; assicurare la massima pubblicità di tali impieghi; limitare la sorveglianza ad aree il più possibile circoscritte; garantire controlli stringenti sull'utilizzo delle informazioni raccolte e sull'accesso a tali dati. Misure volte, cioè, ad assicurare un giusto bilanciamento tra gli interessi pubblici perseguiti e la legittima aspettativa di *privacy* delle persone (doc. web n. 2982806).

Nel corso dell'anno il Gruppo ha altresì deciso di affrontare il tema del cd. *wearable computing*, ossia dei dispositivi che possono essere indossati e che possono dare luogo a forme di sorveglianza indiscriminata e nascosta, e di avviare un'attività ricognitiva sul cd. *bring your own device* (BYOD), uno schema di cooperazione tra individui che mettono in condivisione i propri terminali e applicazioni all'interno di una rete (in diversi contesti: all'interno di pubblica amministrazione, di una sala

conferenza, di un esercizio commerciale, *etc.*). Da esso possono infatti nascere problemi di sicurezza dei dati ad esempio legati all'uso promiscuo dei terminali negli ambiti domestico e lavorativo o alla condivisione degli stessi da più persone, nonché forme di sorveglianza suscettibili di ricadere nell'ambito di applicazione della disciplina sulla protezione dei dati personali.

Data retention - Expert Group

Con decisione C(2013)2144 del 18 aprile 2013, la Commissione europea ha deciso di istituire un nuovo gruppo di esperti – *Data Retention Expert Group* – che, in continuità con il lavoro svolto dal precedente gruppo il cui mandato è terminato nel 2012, ha ricevuto l'incarico di approfondire gli aspetti legati alla direttiva 2006/24/CE (cd. *data retention*, ovvero conservazione dei dati) ed in particolare di predisporre *best practice* sulla conservazione dei dati relativi alle comunicazioni elettroniche a fini investigativi e per la persecuzione di gravi reati. Il Gruppo è formato da rappresentanti delle società fornitrici di servizi di comunicazione elettronica, da rappresentanti delle forze dell'ordine e di polizia nonché da rappresentanti delle Autorità di protezione dei dati. Il Garante partecipa all'attività del *Data Retention Expert Group*. Il Gruppo, sui cui lavori hanno avuto peso le conclusioni presentate dall'avvocato generale della Corte di Giustizia dell'Unione europea il 12 dicembre 2013 riguardo alla direttiva *data retention* (Causa C-293/12), nonché la prospettiva di una imminente decisione della stessa Corte di Giustizia in merito (poi intervenuta, come si è detto al par. 10.2), sta comunque continuando l'attività di predisposizione di un manuale sulle buone prassi in materia di conservazione dei dati che dovrebbe venire alla luce nel corso del 2014.

Consiglio d'Europa

Anche il 2013 è stato caratterizzato dal lavoro di revisione della Convenzione n. 108/1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

Parallelamente al pacchetto di riforma in discussione al livello UE, anche il Consiglio d'Europa (CoE) ha infatti ritenuto necessario rivedere tale Convenzione alla luce delle tante novità emerse negli ultimi decenni, sia con riferimento allo sviluppo tecnologico che alla crescente globalizzazione.

La discussione in seno al CoE si è peraltro svolta con l'intento di assicurare un quadro di principi coerenti con il progetto di revisione degli strumenti di protezione dei dati in discussione a livello UE.

Come anticipato, il T-PD, Comitato della Convenzione a cui il Garante partecipa da anni, anche nella sua composizione ristretta (T-PD Bureau), aveva concluso nel 2012 il lavoro tecnico relativo alla modernizzazione della 108, con l'adozione, in occasione della sua 29ma plenaria, di un documento finale contenente le proposte di revisione della Convenzione (cfr. Relazione 2012, p. 298, doc. web n. 2375191).

Con l'adozione del menzionato documento da parte del T-PD, che ha comunque proseguito la sua riflessione sulla revisione della Convenzione n. 108, impegnandosi nella redazione del *Memorandum* esplicativo che accompagnerà il progetto, si è aperta la fase "politica" della modernizzazione di tale settore alla quale l'Autorità ha continuato a partecipare.

Il Comitato dei Ministri del Consiglio d'Europa il 10 luglio 2013 ha infatti deciso l'istituzione di un Comitato *ad hoc* (CAHDATA) composto dai rappresentanti degli Stati membri del Consiglio d'Europa, di altre Parti che hanno aderito alla Convenzione, e da Stati che non fanno parte del CoE, con il compito di finalizzare il processo di revisione e negoziare formalmente un Protocollo emendativo alla Convenzione n. 108.

Il Segretario generale del Garante è stato designato rappresentante per l'Italia all'interno del CAHDATA e ha dunque preso parte alla prima riunione del Comitato che si è tenuta a Strasburgo il 12-14 novembre 2013.

In tale incontro, durante il quale sono stati eletti il rappresentante irlandese e la rappresentante svizzera, rispettivamente alla Presidenza e alla Vicepresidenza del

Comitato, è emerso un generale plauso per il lavoro svolto dal T-PD le cui proposte di modifica alla Convenzione hanno costituito la base di discussione del CAHDATA. È altresì emersa la necessità di riflettere sul giusto equilibrio che la nuova Convenzione dovrà garantire tra l'esigenza di mantenere un'impostazione coerente con il quadro comunitario e quella di preservare la vocazione universale della 108, fondata su principi di carattere generale.

Il CAHDATA ha dunque effettuato una prima lettura "esplorativa" del testo proposto dal T-PD che, come illustrato nella Relazione 2012, pur mantenendo il carattere trasversale della Convenzione (applicabile sia al settore privato sia a quello pubblico) tecnologicamente neutro e fondato su principi di carattere generale, ha innovato su diversi punti salienti della stessa.

Parallelamente alla discussione sulla Convenzione n. 108, il T-PD ha proseguito il suo lavoro sul processo di revisione delle raccomandazioni del CoE, in particolare della Raccomandazione (89)2 sulla protezione dei dati in ambito lavorativo e della Raccomandazione (87)15 sull'utilizzo dei dati a carattere personale nel settore della polizia. È stata inoltre avviata una riflessione sulla opportunità di rivedere anche la Raccomandazione (97)5 sui dati sanitari, alla luce delle innumerevoli novità tecnologiche nel settore medico, in particolare con riferimento al Fse, alla telemedicina, all'impiego di RFID e di applicativi ("*app*").

Il T-PD ha inoltre portato avanti la riflessione sulla protezione dei dati biometrici dalla quale è emersa l'opportunità di proseguire il lavoro già svolto, ampliando il *Progress Report* del 2005 in modo da dar conto del mutato contesto tecnologico degli ultimi anni, ed in particolare tenendo conto delle tecniche biometriche di seconda generazione che consentono classificazioni automatizzate di individui anche all'insaputa degli stessi interessati.

L'Autorità ha continuato a partecipare ai lavori del WPISP (*Working Party on Information Security and Privacy*) dell'Ocse. Nel 2013 il Garante, già membro del Gruppo e del *Bureau* del WPISP, è stato riconfermato nel *Bureau* del Gruppo anche per il 2014. **OCSE**

Attività centrale del lavoro del WPISP è stata la revisione delle linee guida *privacy* dell'Ocse del 1980 (*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*) che ha portato all'adozione del documento finale da parte del Consiglio Ocse, avvenuta l'11 luglio 2013 (doc. web n. 2629667). Si è giunti così all'approvazione delle *Revised Privacy Guidelines* attraverso una vivace e contrastata discussione durata diversi mesi, alla quale il Garante ha attivamente contribuito affinché il nuovo testo mantenesse un adeguato livello di tutela dei diritti delle persone anche alla luce del quadro europeo di protezione dei dati.

Al centro delle linee guida aggiornate emergono, tra gli altri, due temi. Il primo è un *focus* sulla realizzazione pratica della protezione della *privacy*, attraverso un approccio fondato sulla gestione del rischio. Il secondo riguarda la necessità di affrontare la dimensione globale della protezione dei dati personali attraverso una migliore interoperabilità.

L'attività del WPISP degli ultimi mesi del 2013 si è concentrata sull'esigenza di implementare le linee guida *privacy*, anche attraverso: la diffusione e promozione del testo; lo sviluppo di programmi di *privacy management* (che rientrano nel quadro degli obblighi di *accountability* che ricadono sui titolari del trattamento); l'attuazione della cd. *data security breach notification*; l'elaborazione di strategie nazionali di interoperabilità globale in materia di protezione dei dati personali.

Quanto al tema della *cybersecurity*, il WPISP ha proseguito i lavori del Gruppo di esperti (costituito nel 2012) sulla Revisione delle linee guida sicurezza Ocse del 2002 (*Guidelines for the security of Information Systems and Networks).* Il lavoro è confluito

in un Rapporto in cui è stata evidenziata la necessità di coinvolgere altri esperti per portare avanti la più amplia consultazione possibile per una revisione complessa che deve dare un messaggio importante su un nuovo approccio "in positivo" sulla sicurezza intesa come mezzo per la crescita economica e la prosperità e non solo come "sicurezza da" in termini di difesa da attacchi esterni. A tal fine, è stata condivisa la necessità di trasparenza e di controllo da parte degli utenti. Quanto più gli utenti sono messi in condizione di comprendere (attraverso delle linee guida chiare ed *user-friendly*) e controllare la sicurezza della rete, tanto più la sicurezza sarà positiva e diventerà fattore di crescita globale.

Un altro settore al quale il WPISP nel corso del 2013 ha dedicato attenzione è quello relativo al valore economico dei dati e al ruolo degli stessi nel promuovere la crescita economica e il benessere globale, con particolare riferimento ai cambiamenti tecnologici e organizzativi rappresentati dai *big data* e alle relative analisi di impatto economico. Sono stati affrontati dal WPISP gli argomenti di *privacy* emergenti nella cosiddetta *data driven economy*. La nozione di *trust*, intesa come fiducia nella tecnica e nell'etica dei titolari del trattamento dei dati, è stata molto dibattuta nel corso dell'anno e sempre più associata al benessere economico e alla prosperità. Per la maggior parte delle delegazioni del Gruppo la nozione di *trust* sta diventando un cappello sotto il quale far rientrare tutto ciò che può considerarsi in altri termini *accountability* e affidabilità nella gestione dei dati personali. In ogni caso, il lavoro sulla "*security in a data driven economy*" resta un lavoro *in itinere* che per ora si limita ad introdurre solo delle riflessioni preliminari.

Infine, si segnala che nel dicembre 2013 è stato modificato il nominativo del Gruppo per la necessità condivisa di aggiornare – in relazione ai cambiamenti tecnologici in atto – la forma e il mandato del WPISP (costituito nel lontano 1995). Il cambiamento comporta il passaggio dell'acronimo da WPISP in *WPSP in the Digital economy*. A livello sostanziale, il mandato del lavoro del Gruppo sarà più contenuto e concentrato nello sviluppo di "principi" di *policies* (e non più *policies* in senso largo), linee guida e *best practices* con particolare riferimento alle aeree in cui vi è un crescente bisogno di cooperazione transfrontaliera.

Accountability Project

Nel 2013 si è concluso il lavoro dell'*accountability project*, iniziato nel 2009 e illustrato nelle precedenti relazioni annuali.

La quinta ed ultima fase del progetto, che ha visto riunirsi gli esperti due volte, rispettivamente in Europa (Varsavia) e in Canada (Toronto), si è incentrata sulla ricerca di un consenso sugli aspetti di rischio per i diritti e le libertà fondamentali delle persone in caso di trattamento illecito di dati personali da parte di titolari del trattamento non *accountable*. I partecipanti hanno condiviso e discusso un possibile elenco di rischi frutto del confronto avutosi nel corso delle riunioni della fase IV del progetto e dei vari contributi fatti pervenire dagli esperti.

Anche a causa della difficoltà di trovare, sia a livello internazionale che europeo, definizioni *ad hoc* e parametri condivisi sui rischi e i danni tangibili ed intangibili (ad es., alla reputazione o alla dignità) per i singoli individui derivanti dal trattamento dei dati da parte delle organizzazioni, è stato ritenuto necessario un approccio basato sulla valutazione dei rischi caso per caso. Gli esperti hanno analizzato il rapporto *accountability*/rischi, in particolare enfatizzando la necessità di un forte canale di comunicazione tra titolare e interessato (per incrementare il livello di consapevolezza sui trattamenti e di riduzione dei rischi, nonché la fiducia tra le parti coinvolte), di adeguate misure di sicurezza, di trasparenza sulle finalità del trattamento, di *policy* chiare e condivise. Tutti questi elementi devono essere finalizzati al raggiungimento di un più elevato livello di responsabilità "misurabile" (anche da parte dell'interessato). È emersa, inoltre, la necessità di avviare un dibattito sul tema della fiducia/*trust* come bene pub-

blico da tutelare con adeguati strumenti tecnico-normativi. L'*accountability* è uno degli strumenti che si prestano a questo scopo e dovrà essere implementata ad ogni livello (realtà economiche, pubbliche amministrazioni, Stati). Infine, è stato affrontato il tema della cd. scalabilità, ossia della necessità di disporre di strumenti in grado di gestire le varie fasi quantitative di "misurazione" dei parametri necessari al raggiungimento degli obiettivi di *accountability*. Occorre infatti evidenziare che l'*accountability*, considerata come una forma di responsabilità misurabile, richiederà a realtà economiche o amministrazioni (anche di piccole o piccolissime dimensioni) di trattare grandi quantitativi di dati relativi a interessati, anche in contesti sovranazionali. L'industria, dal canto suo, dovrà fornire strumenti efficaci e "usabili" per consentire queste operazioni anche a titolari non particolarmente forniti di competenze specialistiche, o sofisticati strumenti tecnologici.

Cooperazione internazionale GPEN, IECWG, *PHAEDRA project*

Nell'ambito della Conferenza internazionale (cfr. par. 19.2), si è deciso di rafforzare l'attività del *Global Privacy Enforcement Network - GPEN*, la Rete Internazionale lanciata nel 2010, per promuovere una migliore cooperazione transfrontaliera in tema di *enforcement*, costituendo il Gruppo di coordinamento delle attività internazionali di *enforcement* (IECWG), volto a mettere in atto le raccomandazioni formulate durante l'evento internazionale di coordinamento *enforcement* svoltosi a Montreal nel 2012. Si sono tenute diverse *conference call* del IECWG durante le quali si è discusso, tra l'altro, del lavoro da svolgere per la redazione di un documento illustrativo di uno schema multilaterale di *enforcement* da adottarsi nel corso della 36ª Conferenza internazionale delle autorità di protezione dati. Tale documento dovrà fondarsi sullo schema di coordinamento delle attività internazionali di *enforcement* presentato alla 34ª Conferenza, nonché sull'attività del GPEN, e dovrà prendere in considerazione la condivisione delle informazioni connesse all'attività di *enforcement* nonché la gestione di tali informazioni da parte dei rispettivi destinatari. Il documento in corso di elaborazione non intende sostituirsi alle condizioni ed ai meccanismi già in essere a livello nazionale e regionale per quanto riguarda la condivisione di informazioni, né interferire con analoghi meccanismi operanti all'interno di altre reti. In ogni caso, è stata condivisa l'esigenza di elaborare un quadro multilaterale non legalmente vincolante.

Sempre al fine di migliorare le attività internazionali di *enforcement*, è stata decisa la messa a punto di una piattaforma informativa che offra uno "spazio sicuro" (GPEN *alert system*), dove le autorità responsabili dell'*enforcement* in materia di *privacy* possano condividere informazioni confidenziali e facilitare la promozione e conduzione di azioni coordinate di *enforcement*.

Infine, è proseguita anche l'attività del *PHAEDRA project*, progetto europeo (sostenuto anche dal Garante) volto a sostenere una migliore cooperazione e coordinamento tra i Commissari *privacy* e le autorità di protezione dei dati di tutto il mondo. Si tratta di un progetto biennale, promosso dal Consorzio costituito dalla Vrije Universiteit Brussel, Trilateral Research & Consulting, Università Jaume I di Madrid e l'Autorità polacca per la protezione dei dati personali. Il progetto mira – attraverso la cooperazione – a rendere più efficiente ed efficace l'uso delle risorse (sempre più limitate in questi ultimi anni) di cui dispongono le autorità di protezione dati e della *privacy* (v. par. 19.2).

Incontri con delegazioni estere e organizzazioni internazionali

L'Autorità ha proseguito la sua attività di partecipazione a programmi di partenariato europeo negli ambiti di competenza, in particolare nell'ambito dei programmi Taiex e Twinning e Icoiss della Commissione europea, offrendo la propria esperienza e competenza per facilitare l'avvicinamento delle normative dei paesi coinvolti al quadro comunitario in materia di protezione dei dati.

Nell'ambito di un quadro di collaborazione avviato con l'Autorità di protezione dati macedone risalente al 2008, anno in cui è stata firmata una dichiarazione di

mutua cooperazione, nel mese di aprile, il Garante ha ospitato delegati dell'Autorità macedone in visita-studio dedicata, in particolare, alla materia ispettiva. Inoltre, un delegato dell'Autorità ha partecipato al seminario sulla videosorveglianza nelle scuole, articolato in tre *workshop* che si sono svolti a Skopje nel mese di aprile.

Riguardo alla collaborazione con la Croazia, il Garante ha inviato propri esperti in occasione di alcuni *workshop* organizzati, nell'ambito del *Twinning* coordinato dall'Autorità spagnola di protezione dei dati, sui compiti e le responsabilità del *data protection officer* (7-8 e 27-28 febbraio) e di un seminario in materia di protezione dei dati personali e internet, tenutosi a giugno.

Nell'ambito del programma Icoiss finanziato dall'Unione europea, il Garante nel mese di settembre ha ricevuto una delegazione di alti dirigenti del Ministero dell'interno della Turchia, interessati al sistema della pubblica sicurezza a livello centrale e periferico.

Nell'ambito di un progetto di collaborazione accademica, inoltre, l'Università di Washington, con una delegazione composta da studenti e professori, ha avuto un incontro ufficiale con il Garante, in particolare sui temi del processo legislativo e sanzionatorio in Italia e negli USA e i profili di protezione dei dati legati a internet.

Il 10 settembre nella sede dell'Autorità, il relatore speciale delle Nazioni Unite per la promozione e la tutela della libertà di espressione, signor Frank La Rue è stato ricevuto dal Presidente del Garante. Nel corso dell'incontro, in vista del rapporto che l'inviato dell'Onu dovrà stilare e dell'incontro formale tenutosi il 13 novembre presso il Ministero degli esteri sui temi legati alla libertà di espressione nella rete con le diverse autorità competenti, sono state in particolare trattate le questioni del rapporto tra *privacy* e libertà di informazione, nonché le preoccupazioni per la proliferazione delle nuove forme di sorveglianza di massa, attraverso internet e i sistemi di telecomunicazioni, venute alla luce dopo il caso *Datagate*.