tezza, altre garanzie di natura contrattuale: clausole contrattuali *standard*, *Binding corporate rules*; altrimenti, osservanza di altri requisiti in deroga quali: consenso dell'interessato, interesse legittimo prevalente, ecc.). Da rilevare che nel capo V è stata introdotta dal Consiglio la possibilità di utilizzare codici di condotta vincolanti (per il titolare nel Paese terzo) al fine di consentire trasferimenti di dati nonché certificazioni rilasciate in base alle disposizioni del capo IV. In proposito, il Gruppo Art. 29 ha chiesto (in un proprio "*Statement*" del settembre 2014, WP 222, doc. web n. 3815204) maggiori garanzie rispetto all'utilizzo di codici di condotta (dubitando della loro effettiva vincolatività) ed al ruolo delle autorità di controllo in tale contesto.

Come si è detto, restano sul tappeto alcune questioni importanti e particolarmente controverse, sulle quali è comunque verosimile che sia possibile chiudere il negoziato entro il primo semestre del 2015, nel corso della Presidenza lettone. Si tratta di questioni sia orizzontali sia più specifiche e, quindi, relative a singole disposizioni. Fra le prime ricordiamo, innanzitutto, la necessità di delineare meglio i settori ai quali si applicherà la futura direttiva (polizia e giustizia) anziché il regolamento, disciplinando i rispettivi ambiti di competenza nella maniera più efficace e corretta possibile.

Lungamente dibattuta (e non risolta appieno) rimane anche la questione relativa agli atti delegati e di esecuzione, ossia al conferimento alla Commissione europea del potere di adottare, in maniera sistematica – e, a parere del Gruppo Art. 29, non sufficientemente giustificata – atti comunitari finalizzati a dare piena attuazione ad alcune disposizioni del regolamento; la rilevanza del tema emerge ulteriormente considerando l'impatto sui poteri di controllo dei Parlamenti nazionali alla luce del principio di sussidiarietà.

Fra le questioni più puntuali, ma di grande rilevanza, occorre menzionare quelle relative alla configurazione del "consenso" al trattamento, che secondo la proposta della Commissione deve essere (oltre che libero, informato, specifico) anche esplicito, mentre alcuni Stati membri preferirebbero mantenere la dicitura dell'attuale direttiva 95/46/CE (consenso "inequivocabile"). Sul diritto all'oblio, che è disciplinato dall'art. 17 della proposta di regolamento, i ministri hanno convenuto genericamente (durante il Consiglio GAI di ottobre 2014) di non appesantire il testo con disposizioni eccessivamente dettagliate, ma hanno sottolineato la necessità di garantire sempre il contemperamento dei diritti fondamentali in gioco (in particolare, libertà di espressione e tutela della vita privata); il dibattito è stato fortemente influenzato dalla menzionata sentenza della Corte di giustizia nel caso *Google Spain*, senza giungere però a conclusioni definite. Assai controverso anche il tema della profilazione (artt. 4 e 20 della proposta di regolamento), per la difficile individuazione di un approccio comune da adottare; si tratta di decidere se disciplinare le sole conseguenze della profilazione (come fa la direttiva 95/46/CE all'art. 15) oppure la profilazione in sé e per sé considerata, in particolare la raccolta di dati personali per tali finalità, basandosi eventualmente sull'apporto concettuale dell'analisi condotta in materia dal Consiglio d'Europa (cfr. *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*).

One stop shop

Infine, vi è il tema importante del cd. "sportello unico" (*One-Stop-Shop* - OSS) e, più in generale, dei meccanismi di collaborazione fra autorità di controllo (capi VI, VII, e VIII sulla tutela giurisdizionale). Le discussioni in sede di Consiglio GAI si sono concluse con un generale favore per il concetto di sportello unico, purché temperato con meccanismi volti ad assicurare un'effettiva "prossimità" territoriale degli interessati all'autorità competente a decidere su eventuali ricorsi. La Presidenza greca ha presentato un documento contenente alcune soluzioni volte ad introdurre i contrappesi necessari a bilanciare gli interessi in gioco e, in particolare, un ulteriore

criterio di competenza della "autorità capofila" del procedimento qualora il trattamento sia svolto a partire da un solo stabilimento di una multinazionale nell'UE ma interessi soggetti residenti in altri Stati membri. Per integrare i benefici offerti alle imprese dallo "sportello unico" con un'effettiva tutela amministrativa e giurisdizionale per i singoli interessati, si è proposto (da parte della Presidenza italiana) un meccanismo di co-decisione tra autorità locale e autorità capofila, con adozione da parte della autorità locale delle decisioni su contenziosi esclusivamente locali o di interesse solo locale (pur se in un contesto multinazionale). L'eventuale conflitto (in termini di competenza o di merito della decisione) tra due (o più) autorità verrebbe devoluto al Comitato europeo della protezione dati (EDPB), erede dell'attuale Gruppo Art. 29, al quale dovrebbe essere riconosciuto il potere di emettere decisioni vincolanti. Questa proposta ha ricevuto un sostanziale appoggio dalla maggioranza delle delegazioni; restano alcuni elementi da precisare, ma l'architettura complessiva è stata giudicata un buon compromesso fra i diversi interessi in gioco. Conviene ricordare che, in proposito, il Gruppo Art. 29 ha chiaramente indicato alcune precondizioni (*Statement* del 16 aprile 2014, doc. web n. 3815614): affermare il mantenimento della competenza territoriale delle DPA in ogni caso (anche in vista dei seguiti da dare a livello nazionale); prevedere che l'autorità capofila funga da contatto principale ma non da decisore unico; dare efficacia vincolante alle decisioni della autorità capofila nei confronti delle altre DPA coinvolte; precisare meglio la nozione di "stabilimento principale"; garantire agli interessati di poter sempre adire i giudici nazionali per impugnare le decisioni che li riguardino anche a seguito dell'intervento del meccanismo di OSS.

La proposta di direttiva

Gli incontri che si sono susseguiti in seno al Consiglio UE nel 2014 per discutere sulla proposta di direttiva hanno comportato diversi cambiamenti al testo rispetto a quello proposto inizialmente dalla Commissione. In linea generale va rilevato che, nel corso delle riunioni, molte perplessità sono state manifestate in ordine alla necessità di adottare tale nuovo strumento, essendosi diverse delegazioni espresse per il mantenimento dello *status quo* (consistente, come è noto, nella regolamentazione contenuta nella decisione quadro 977/2008) e, quindi, dei principi volti a disciplinare solo gli scambi di dati transfrontalieri (all'interno dell'Unione). È stata inoltre manifestata la necessità di definire meglio i confini rispetto alle norme che saranno contenute nel "regolamento generale" (con conseguente richiesta di inclusione nella direttiva degli aspetti legati al mantenimento dell'ordine e sicurezza pubblica) nonché di approfondire i problemi legati all'applicazione dei principi di protezioni dati all'attività giurisdizionale.

Sotto la Presidenza greca, diverse delegazioni si sono pronunciate per l'inserimento del consenso tra le basi legali dei trattamenti di dati e presentato richieste di modifica di aspetti chiave, quali il concetto di dato personale (solo i dati che portano all'identificabilità diretta), le nozioni di trattamento e di titolare/responsabile del trattamento, di profilazione: sono temi che restano pertanto tutti ancora aperti.

Nel corso della Presidenza italiana si sono tenute tre riunioni (il 29 settembre, il 27 ottobre e il 24 novembre) dedicate ad una rilettura di alcune parti dei titoli I, II e V della direttiva. Gli aspetti discussi sono stati quello del campo di applicazione (inserimento del concetto di mantenimento della sicurezza pubblica come ulteriore finalità separata da quella di prevenzione, accertamento, contrasto e repressione di reati) e quello della definizione delle autorità competenti (inserimento nella definizione anche di quei soggetti privati cui vengono delegati compiti istituzionali nelle materie coperte dalla direttiva). La Presidenza italiana ha anche proposto un nuovo testo per l'art. 8 che riguarda le condizioni di liceità per il trattamento di dati sensibili recependo le istanze di varie delegazioni che preferivano fosse mantenuto il

testo della Decisione quadro, non più basato sul binomio divieto come regola ed eccezioni ben specificate, quanto piuttosto sulla regolazione dell'uso, reso ammissibile in caso di stretta necessità.

Sul capo V della direttiva, dedicato ai trasferimenti transfrontalieri di dati, il testo presentato dalla Presidenza ha tenuto conto dell'Accordo parziale già raggiunto dal Consiglio sull'analogo capo del regolamento.

Il documento fatto circolare dalla Presidenza ha ribadito le condizioni per i trasferimenti: *in primis* l'esistenza di una decisione di adeguatezza adottata dalla Commissione europea (sentito il *Board* delle Autorità di protezione dei dati) che può essere generale (adottata secondo la procedura del Regolamento) ovvero specifica per il campo di applicazione della direttiva; in mancanza, la presenza di garanzie appropriate (clausole contrattuali o altri tipi di impegni); laddove le altre condizioni non siano presenti, la trasmissione può essere consentita in casi particolari. Il testo della Presidenza inoltre ha importato, sulla scorta dell'analogo accordo trovato sul Capo V del Regolamento, la definizione di organizzazioni internazionali.

Il testo è stato accolto favorevolmente per quanto concerne l'introduzione della definizione di organizzazioni internazionali, cui dopo una ulteriore riflessione si è deciso di aggiungere anche un riferimento ad Interpol.

Per quanto riguarda gli accordi bilaterali già in vigore che consentono gli scambi di informazioni con Paesi ed organismi terzi, sembra emergere una chiara volontà nel gruppo di mantenerne gli effetti, diversamente da quanto previsto dalla proposta di direttiva. Il Servizio giuridico del Consiglio ha fatto presente che comunque si applica il Trattato (che prevale).

La Presidenza italiana ha predisposto, al termine del suo periodo, un testo consolidato della direttiva che servirà da base per le successive discussioni sotto Presidenza lettone. In particolare il testo contiene una riformulazione dei capi esaminati sotto la Presidenza italiana (I, II e V) e alcune proposte atte a sciogliere le difficoltà delle delegazioni riguardo al campo di applicazione della direttiva ed alla definizione di autorità competenti.

23.2. *Le conferenze delle Autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati

La 36ª Conferenza internazionale si è tenuta a Mauritius dal 13 al 16 ottobre 2014. Le Autorità per la protezione dei dati e la *privacy* hanno esaminato, in particolare, le potenzialità e gli effetti dell'internet delle cose (*Internet of Things* - IoT). Quattro esperti, in rappresentanza del settore privato e del mondo universitario, hanno descritto alle autorità gli impatti positivi che l'internet delle cose può avere sul vissuto quotidiano, ma anche i rischi che esso comporta e i passi necessari per continuare a tutelare, anche in questo contesto, i dati personali e la vita privata.

Durante la sessione a porte chiuse, le autorità hanno adottato quattro risoluzioni ed una dichiarazione. La dichiarazione, che riguarda appunto il tema dell'*internet of things* (doc. web n. 3655156), tiene conto delle sfide che l'internet delle cose pone alle autorità di protezione dei dati e agli individui. La dichiarazione richiama tutti gli *stakeholders* a porre in essere un dibattito costruttivo sulle implicazioni delle IoT e dei *Big data* per aumentare la consapevolezza generale in ordine alle future scelte della società.

La risoluzione "*big data*" (doc. web n. 3655166) è stata fortemente voluta ed adottata al fine di sviluppare e utilizzare le tecnologie *big data* nel rispetto dei principi fondamentali di protezione dei dati, con particolare *focus* sul principio di *privacy by design*, e l'invito ad utilizzare dati anonimi per mitigare i rischi per la *privacy*. Ciò in linea con gli orientamenti espressi dal Gruppo di Berlino sul tema (v. *infra*).

La risoluzione "*Enforcement*" (doc. web n. 3655146) mira a concretizzare e rendere effettivo il quadro in cui favorire forme di coordinamento internazionali efficaci nell'attività di attuazione delle regole di protezione dati internazionalmente condivise svolta dalle autorità di controllo.

La risoluzione "*Privacy in digital age*" (doc. web n. 3655186) invita i membri della Conferenza, alla luce dello scandalo *Datagate* e del fenomeno della sorveglianza di massa, a garantire l'applicazione dei principi generali della protezione dei dati nel mondo digitale e il rispetto degli *standard* internazionali di Madrid (2009), del Patto internazionale diritti civili e politici e della Convenzione 108 del Consiglio d'Europa.

Va ricordata, infine, la risoluzione con la quale si sono accreditate le autorità per la protezione dei dati di Brema (Germania), Ghana e Senegal alla Conferenza internazionale nonché alcune organizzazioni (rispettivamente di Giappone, Bermuda, Messico, Singapore e Stati Uniti) che hanno ricevuto lo *status* di "osservatore" della Conferenza.

A margine della Conferenza si sono tenuti alcuni eventi a cui ha preso parte anche il Garante: un seminario in tema di *digital education* che si è concentrato sui criteri per garantire più efficaci politiche di sensibilizzazione sui temi *privacy* da parte delle DPA; il seminario sul Progetto PHAEDRA nel corso del quale sono stati illustrati i passi futuri per rafforzare la cooperazione internazionale nell'ambito della protezione dei dati; il seminario sull'*accountability*, organizzato dalla Nymity e la *Information Accountability Foundation*, nel corso del quale sono stati presentati i risultati dello Studio *Accountability Benchmarking* che mira ad evidenziare le modalità con cui varie organizzazioni a livello mondiale, stanno implementando il principio di *accountability*.

La Conferenza delle autorità europee (*Spring Conference*)

Come anticipato, la Conferenza di primavera dei Garanti europei, tenutasi a Strasburgo il 5 giugno 2014, si è concentrata sul tema della cooperazione europea ed internazionale nel settore della protezione dei dati e, con tre diverse sessioni, ha fatto il punto sullo stato attuale della cooperazione, sulle aspettative in merito ad essa e sulle soluzioni per il suo rafforzamento. Durante la Conferenza è stata adottata la risoluzione sulla modernizzazione della Convenzione 108 (doc. web n. 3845156) nella quale le autorità europee di protezione dati hanno messo in evidenza la necessità che tale processo di revisione, pur tenendo conto della opportunità di aprirsi a Paesi terzi, non porti in nessun modo alla riduzione dell'alto *standard* di protezione finora garantito dalla Convenzione 108.

È stata inoltre adottata la risoluzione per l'accreditamento dell'autorità di protezione dei dati della Georgia tra i membri della *Spring Conference*.

La Conferenza è stata l'occasione per ripercorrere le diverse forme di cooperazione finora attuate sia a livello europeo (*case handling*, sottogruppi del Gruppo Art. 29, ispezioni coordinate, BCR, ACC, ecc.), sia internazionale (Conferenza internazionale, GPEN, reti di autorità, cooperazione rafforzata nella nuova 108), nonché i diversi livelli di coordinamento che possono essere attuati: semplice condivisione di informazioni non riservate senza coordinamento (ad es., *case handling*), *sweep* con scambio di informazioni non riservate; scambio di informazioni riservate (ad es., GPEN); azioni coordinate e confidenziali (come nel caso dell'esame della *privacy policy* di Google). Sono stati inoltre considerati gli elementi da migliorare per una più efficace cooperazione, ed in particolare: una maggiore armonizzazione normativa, l'estensione della cooperazione anche a settori diversi dall'*enforcement*, l'approntamento di più specifiche procedure nazionali per la cooperazione, l'indicazione di diversi *contact points*, la formalizzazione delle richieste di informazione (anche per evitare la mancanza di risposte), regole più precise per la confidenzialità delle informazioni trattate, l'incremento di risorse economiche e tecnologiche per la cooperazione e l'approntamento di strutture permanenti (segretariato) per la cooperazione.

A conclusione della *Spring Conference*, è stato istituito un nuovo gruppo di lavoro – coordinato dal Consiglio d'Europa e dall'autorità di protezione dei dati francese (co-organizzatori dell'ultima *Spring*) – finalizzato all'individuazione degli strumenti europei per il rafforzamento della cooperazione in materia di protezione dei dati tra Paesi membri UE e non.

23.3. *La cooperazione tra Autorità garanti nell'UE: il Gruppo Art. 29*

L'attività delle Autorità garanti nell'UE riunite nel Gruppo Art. 29 è proseguita nel 2014 sulla base dei temi strategici generali fissati nel programma di lavoro relativo al biennio 2014-2015 adottato il 3 dicembre 2013 (doc. web n. 3815727). In particolare, il Gruppo si è impegnato, attraverso le sue riunioni plenarie (cinque nel corso dell'anno) e la costante attività dei suoi differenti sottogruppi, per assicurare un'applicazione coerente e corretta del quadro giuridico vigente e per preparare il futuro assetto giuridico, garantendo maggiore chiarezza ed efficacia nell'affrontare la globalizzazione e le sfide tecnologiche anche attraverso una più stretta cooperazione in materia di *enforcement*.

Con riferimento al nuovo quadro normativo, il Gruppo è intervenuto con proprie osservazioni, tra l'altro, in tema di "sportello unico", in materia di trasferimenti di dati in Paesi terzi – pronunciandosi a favore del mantenimento della previsione dello strumento Bcr *for processor* (strumento che risulta invece soppresso nel testo approvato in prima lettura dal Parlamento europeo) – e con riferimento all'introduzione di un approccio basato sul rischio (v., in proposito, il par. 23.1).

Il Gruppo Art. 29 e le sentenze della Corte di giustizia

Il Gruppo si è poi espresso con riferimento a due delle sentenze più rilevanti adottate in materia di protezione dei dati dalla Corte di giustizia: la citata sentenza del 14 maggio 2014, caso Google Spain (doc. web n. 3127044) e quella dell'8 aprile 2014 (C-293/12 e C-594/12), caso Digital Rights Ireland Ltd, in materia di *data retention* (doc. web n. 3845166).

In particolare, a seguito della sentenza della Corte di giustizia relativa al caso Google Spain – con cui la Corte ha riconosciuto la società statunitense come titolare del trattamento dei dati personali che appaiono nell'elenco dei risultati del suo motore di ricerca e l'applicabilità della disciplina europea (nel caso specifico spagnola) in materia di protezione dei dati, ritenendola stabilita sul territorio spagnolo alla luce delle attività, ivi svolte, di promozione e vendita degli spazi pubblicitari poi riprodotti nelle pagine dei risultati di ricerca – il Gruppo Art. 29 ha adottato un documento volto a fornire una sistematizzazione dei criteri, sia procedurali che sostanziali, per trattare le richieste di deindicizzazione dai motori di ricerca (WP 225, doc. web n. 3876849; sul punto cfr. anche par. 10.4). Le Linee guida, che riportano indicazioni ed esempi di carattere generale, potranno essere utilizzate dalle DPA per affrontare in modo quanto più omogeneo possibile i reclami/ricorsi in caso di mancata deindicizzazione, tenendo conto comunque delle peculiarità del caso di specie e sempre nell'ottica di contemperare diritto alla deindicizzazione e libertà di informazione. Il documento potrà formare oggetto di aggiornamento alla luce dell'esperienza acquisita dalle DPA.

Il Gruppo si è altresì espresso sulla sentenza dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12) con la quale la Corte di giustizia ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico ritenendo che dalla stessa derivi un'ingerenza di ampia portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, non limitata allo stretto necessario. In particolare, con la dichiarazione del 1° agosto 2014 (doc. web n. 3815184), il Gruppo, che

guarda con favore alle conclusioni della Corte, ha incoraggiato gli Stati membri e le istituzioni comunitarie a prendere atto della sentenza che fissa specifici criteri per le normative di *data retention* e ad agire in linea con tali criteri.

Concetti-chiave della direttiva 95/46/CE

Il Gruppo ha proseguito l'attività di approfondimento di disposizioni chiave della direttiva 95/46/CE, in particolare con l'adozione del parere 6/2014 (WP 217, doc. web n. 3815154) sulla nozione di "legittimo interesse", uno dei criteri di legittimità del trattamento previsti dall'art. 7 della direttiva 95/46/CE. In tale documento il Gruppo pone il legittimo interesse (del titolare o di terzi, purché non prevalgano i diritti e le libertà fondamentali dell'interessato) tra i requisiti che legittimano il trattamento al pari delle altre basi giuridiche di cui all'art. 7 (ad es., il consenso dell'interessato). La sua applicazione non deve dunque essere residuale, solo in caso di impossibilità di avvalersi degli altri criteri previsti dalla direttiva. Al contrario, esso può risultare il criterio di legittimità più congruo – purché siano rispettati i diritti fondamentali delle persone – per evitare di fondare il trattamento su requisiti che non forniscano sufficienti salvaguardie per l'interessato (si pensi al caso del trattamento di dati in ambito lavorativo fondato sul consenso del dipendente, difficilmente "libero", considerato lo squilibrio contrattuale tra datore di lavoro e dipendente stesso). Il legittimo interesse non deve tuttavia rappresentare la facile via d'uscita per il titolare che non abbia altra base su cui fondare il trattamento. Ed infatti il parere, dopo essersi soffermato sull'analisi testuale dell'art. 7, lett. *f*), mette in luce i diversi fattori che devono essere considerati. Ad esempio, le conseguenze del trattamento sulle persone devono essere valutate secondo un'ampia accezione (non limitandosi ai soli danni materiali che potrebbero incombere sull'interessato), devono riguardare la natura dei dati, la modalità del trattamento, le ragionevoli aspettative di *privacy* della persona coinvolta, lo *status* del titolare e dell'interessato stesso. Inoltre, perché il legittimo interesse del titolare possa dirsi prevalente e quindi costituire la base giuridica del trattamento, grande attenzione va prestata alle salvaguardie ulteriori (rispetto agli obblighi fissati dalla direttiva) poste in essere dal titolare stesso (ad es., garanzie di *accountability* e trasparenza, diritto di opposizione "incondizionato", garanzia di un'immediata cancellazione dei dati, misure di sicurezza particolarmente stringenti, utilizzo di tecniche di anonimizzazione ecc.) affinché i diritti degli interessati siano adeguatamente protetti.

Il parere, che fornisce raccomandazioni in merito al futuro quadro normativo UE, è stato sottoposto a consultazione pubblica al termine della quale il Gruppo ha adottato un documento riepilogativo fornendo un sintetico riscontro alle problematiche emerse in sede di consultazione ed alcuni chiarimenti, in particolare in materia di ricerca, *direct marketing* e giornalismo (doc. web n. 3815154).

Data breach notification

Molto intensa è stata l'attività del Gruppo Art. 29 con riferimento alle sfide per la protezione dei dati sollevate dalle nuove tecnologie. In particolare, il Gruppo ha affrontato il tema della cd. *data breach notification*, l'obbligo di notifica in caso di violazione della sicurezza dei dati, previsto allo stato dalla direttiva 2002/58/CE per i soli fornitori di servizi di comunicazione elettronica ma che potrebbe essere esteso ai diversi titolari del trattamento dal nuovo Regolamento sulla protezione dei dati.

Con il parere 3/2014 (WP 213, doc. web n. 3815121), il Gruppo fornisce indicazioni ai titolari del trattamento per una corretta notifica agli interessati in caso di *data breach*, e pur riferendosi all'esistente obbligo previsto per il settore delle comunicazioni elettroniche, riporta esempi per molteplici altri ambiti, introducendo "buone pratiche" per mettere al riparo gli interessati dai rischi delle falle nella sicurezza. A differenza della notifica all'autorità competente – che deve avvenire, secondo la direttiva 2002/58/CE, per tutte le violazioni dei dati – il parere esamina le violazioni dei dati personali per le quali è richiesta anche la notifica agli interes-

sati e considera ciò che i responsabili del trattamento avrebbero potuto fare nella messa in opera dei loro sistemi per prevenire la violazione dei dati personali o, quanto meno, per individuare le misure attuabili per esentare il titolare dall'obbligo di notifica agli interessati.

Tecniche di anonimizzazione

Il Gruppo ha ultimato l'approfondimento sulle tecniche di anonimizzazione con l'adozione del parere 5/2014 (WP 216, doc. web n. 3815144) il quale esamina l'efficacia e i limiti delle tecniche esistenti rispetto al quadro giuridico dell'UE in materia di protezione dei dati e fornisce raccomandazioni per il loro impiego, tenendo conto del rischio residuo di identificazione insito in ciascuna di esse. Il Gruppo riconosce il valore potenziale dell'anonimizzazione come strategia per consentire alle persone e alla società in senso lato di fruire dei vantaggi dei "dati aperti", attenuando al contempo i rischi per le persone interessate (nella consapevolezza di quanto sia difficile creare insiemi di dati effettivamente anonimi mantenendo al contempo tutte le informazioni necessarie per espletare l'attività richiesta).

Il parere sottolinea, inoltre, che l'anonimizzazione costituisce un trattamento ulteriore dei dati personali e, in quanto tale, deve soddisfare il requisito di compatibilità con le originarie finalità del trattamento, tenendo conto delle motivazioni giuridiche e delle circostanze del trattamento successivo. Una volta resi (effettivamente) anonimi, i dati non rientrano più nell'ambito di applicazione della legislazione in materia di protezione dei dati, tuttavia le persone interessate potrebbero comunque avere diritto a forme di tutela in base ad altre disposizioni (ad es., quelle che proteggono la riservatezza delle comunicazioni).

Il parere illustra poi le principali tecniche di anonimizzazione, ossia la "randomizzazione" e la "generalizzazione". In particolare, esamina l'aggiunta del rumore statistico, le permutazioni, la *privacy* differenziale, l'aggregazione, il k-anonimato, la l-diversità e la t-vicinanza. Ne illustra i principi, i punti di forza e di debolezza, nonché gli errori e gli insuccessi comuni connessi all'impiego di ciascuna tecnica.

Internet of things

Al centro dell'attività del Gruppo è stato anche il tema dell'internet delle cose (*Internet of things* - IoT). Con il parere 8/2014 (WP 223, doc. web n. 3815214), adottato proprio in vista della discussione che si sarebbe tenuta nella Conferenza internazionale (v. par. 23.2), il Gruppo si è soffermato sui principali rischi sottesi al sempre più ampio sviluppo dell'IoT (in particolare, in associazione a *wearable computing, quantified self* e domotica), fornendo prime indicazioni su come i principi di protezione dei dati possano trovare applicazione in tale ambito. Attraverso un'ampia esemplificazione, il parere auspica anzitutto che il maggior numero di garanzie siano introdotte già nella fase progettuale e che all'utilizzatore debba rimanere il controllo dei dati trattati dall'"oggetto" in ogni fase del trattamento, anche per il tramite del suo consenso informato, libero e specifico. Alcune raccomandazioni sono rivolte a tutti gli *stakeholder* interessati (produttori, sviluppatori di app, piattaforme *social*, etc.): applicazione dei principi di *privacy by design* e *privacy by default*, redazione del *Privacy Impact Assessment* (utilizzando le indicazioni già date dal Gruppo Art. 29 nel 2011 in materia di Rfid, WP 180), minimizzazione dei dati, utilizzo di informative cd. *user-friendly*, raccolta granulare del consenso, etc.

Device fingerprinting

Nel corso dell'anno è stato anche adottato il parere 9/2014 sul cd. *device fingerprinting* (WP 224, doc. web n. 3815224), ovvero sulle tecnologie che possono essere utilizzate, in alternativa ai *cookies*, per l'identificazione univoca ed il tracciamento degli utenti dei servizi internet. Il Gruppo, in linea con precedenti prese di posizione (parere 4/2010 sull'esenzione del consenso in materia di *cookies*), ritiene applicabile l'art. 5.3 della direttiva 2002/58/CE anche al *device fingerprinting*, rendendo pertanto necessaria la previa raccolta del consenso, salvo il caso in cui l'utilizzo di tale tecnologia sia necessario per la fornitura di un servizio. Il parere sottolinea inoltre

che le disposizioni in materia di protezione dei dati personali trovano comunque applicazione ogniqualvolta si realizzi un trattamento di dati personali (come nel caso in cui la combinazione di più elementi possa portare all'identificazione dell'utente – ad es., in occasione del trattamento di un indirizzo IP).

Big data

Il Gruppo con una dichiarazione adottata il 16 settembre 2014 (WP 221, doc. web n. 3815194), si è poi espresso sul tema dei *big data* e sul loro impatto sulla protezione dei dati. In questa sede, ha sottolineato come non vi sia motivo di credere che i principi europei di protezione dei dati, come sanciti nella direttiva 95/46/CE, possano essere messi in discussione dallo sviluppo di tale fenomeno. Ha tuttavia richiamato l'attenzione sulla necessità di declinare tali principi – e in particolare quello di finalità e quello di minimizzazione dei dati – in questo nuovo contesto al fine di favorirne un'applicazione adeguata. Il tema dei *big data* è stato altresì oggetto della lettera indirizzata all'amministrazione USA in relazione al cd. Rapporto Podesta "*Big Data*: *Seizing Opportunities, Preserving Values*" (doc. web n. 3815624).

Google privacy policy

Grazie all'attività di cooperazione tra diverse autorità nazionali, a settembre è stata concordata dal Gruppo una lettera (doc. web n. 3815664), poi inviata a Google, relativa al *set* delle misure che la società è tenuta a rispettare affinché la propria *privacy policy* possa essere ritenuta in linea con il quadro normativo europeo in materia di protezione dei dati personali. La lettera di accompagnamento spiega che Google potrà anche adottare misure diverse da quelle indicate ove le stesse raggiungano comunque gli obiettivi richiesti (doc. web n. 3815654).

Aerei a pilotaggio remoto (RPAS)

Anche a seguito di una specifica richiesta fatta pervenire dalla Commissione europea che l'8 aprile 2014 ha adottato la Comunicazione COM(2014) 207, "Una nuova era per il trasporto aereo - Aprire il mercato del trasporto aereo all'uso civile dei sistemi aerei a pilotaggio remoto in modo sicuro e sostenibile", il Gruppo ha iniziato i lavori per predisporre un parere in materia di utilizzo degli aerei a pilotaggio remoto (cd. droni) per scopi civili (ivi comprese le attività di *law enforcement*). Il documento, che dovrebbe essere adottato entro la prima metà del 2015, fa seguito alle risposte già fornite dal Gruppo ad un precedente questionario che la Commissione aveva inviato nel 2013 (v. Relazione 2013, p. 172) e fornirà una serie di indicazioni per consentire un utilizzo di tali mezzi rispettoso dei principi di protezione dei dati. Particolare attenzione dovrà essere prestata, in particolare, ai principi di minimizzazione, necessità e proporzionalità del trattamento (soprattutto mediante l'adozione di misure di *privacy by design* e *by default* da parte, ove possibile, dei costruttori ma, soprattutto, degli operatori), al rispetto del principio di finalità e di liceità (con l'individuazione, di volta in volta, della più idonea base giuridica per il trattamento) e alle modalità per rendere edotti gli interessati.

Borders, Travel e Law Enforcement

Alla luce dei recenti scandali in materia di sorveglianza di massa, di particolare rilievo è stata l'attività svolta dal Gruppo in relazione al lavoro del *Borders, Travel and Law Enforcement subgroup*.

Parere sull'applicazione dei principi di necessità e proporzionalità nel settore del *law enforcement*

A febbraio è stato adottato il parere 1/2014 sull'applicazione dei principi di necessità e proporzionalità nel settore del *law enforcement* (WP 211, doc. web n. 3815111) anche alla luce della giurisprudenza della Corte europea dei diritti dell'uomo che, in questi anni, si è venuta consolidando in relazione all'art. 8 della Convenzione europea dei diritti dell'uomo (che stabilisce il diritto al rispetto della vita privata e familiare). Anche se i concetti di necessità (e proporzionalità) si sono sviluppati in quella giurisprudenza al di là del contesto della protezione dei dati in senso stretto, il loro rapporto con quest'ultima disciplina va tenuto in considerazione, in quanto sia la Convenzione 108 (applicabile al settore del *law enforcement*) sia la direttiva 95/46/CE, nell'introdurre restrizioni ai diritti, fanno riferimento espresso o comunque sottendono il rispetto dei criteri indicati da tale articolo.

Anche se la direttiva 95/46/CE non è applicabile in larga misura al settore dell'*ex* III pilastro, il parere sottolinea come i suoi principi sono stati estesi dai legislatori nazionali fino a coprire di regola tutti i trattamenti di dati, inclusi quelli del cd. *ex* III Pilastro, seppur con deroghe ed eccezioni. Nell'ottica del Gruppo Art. 29, anche attingendo alla giurisprudenza e all'esperienza dei membri del Gruppo, il parere ha lo scopo di indicare al legislatore e alle autorità di *law enforcement* gli elementi da tener presenti affinché le misure in materia di libertà, sicurezza e giustizia proposte per il futuro (sia in caso di introduzione di nuove misure o per modificare quelle esistenti) siano necessarie e proporzionate, invece di avere semplicemente un "valore aggiunto" o "essere utili": in particolare, sarà necessario tenere in considerazione la base giuridica, il problema specifico da risolvere (per esempio la sua gravità e il contesto sociale e culturale in cui è sorto), le motivazioni (cui sono strettamente legate le decisioni in materia di tempi di conservazione dei dati, di minimizzazione della raccolta e di qualità dei dati) e l'esistenza di elementi sufficienti a sostegno delle motivazioni che portano a scegliere quella misura.

Parere sulla sorveglianza delle comunicazioni elettroniche a fini di *intelligence* e sicurezza nazionale

Il 10 aprile 2014, il Gruppo ha adottato il parere 4/2014 sulla sorveglianza delle comunicazioni elettroniche a fini di *intelligence* e sicurezza nazionale (WP 215, doc. web n. 3815134) nel quale, alla luce dello scandalo *Datagate*, si sostiene che in nessun caso la lotta al terrorismo può giustificare forme di sorveglianza massiva e indiscriminata e si sollecitano maggiori controlli e trasparenza sulle attività dei servizi di *intelligence* unitamente all'introduzione di un quadro legale coerente ed una supervisione efficiente, anche attraverso: un effettivo coinvolgimento delle autorità di protezione dei dati; il rafforzamento degli obblighi – già gravanti sui Paesi dell'UE derivanti dalla Convenzione europea dei diritti dell'uomo e dal Trattato – di proteggere il diritto alla riservatezza ad alla tutela dei dati personali; la sollecita adozione del "pacchetto protezione dati" ed in particolare il mantenimento nella proposta di regolamento dell'art. 43a proposto dal Parlamento (obbligo di informare gli interessati ove sia stato riconosciuto ad autorità pubbliche l'accesso ai dati personali che li riguardano); l'adozione di un accordo internazionale che preveda forti garanzie per gli individui nel contesto delle attività di sorveglianza.

***Intelligence* e la sicurezza nazionale**

Al fine di sviluppare l'analisi giuridica di quanto già elaborato nel WP 215, il Gruppo ha inoltre adottato, a dicembre, un documento di lavoro sulla sorveglianza delle comunicazioni elettroniche per finalità di *intelligence* e la sicurezza nazionale (parere 18/2014, WP 228, doc. web n. 3815264). Esso contiene diverse raccomandazioni su come garantire il rispetto dei diritti fondamentali di riservatezza e protezione dei dati da parte dei servizi di *intelligence* e di sicurezza, su come migliorare la vigilanza di questi enti, pur nel rispetto della sicurezza nazionale, e ricorda a tutti i soggetti interessati la loro corresponsabilità nella progettazione e nell'applicazione di un quadro etico per la raccolta e l'uso dei dati personali nell'economia digitale. Il documento è stato presentato all'*European data governance forum* tenutosi a Parigi l'8 dicembre 2014.

Dichiarazione congiunta delle autorità di protezione dati europee in materia di sorveglianza

Sempre in tema di sorveglianza, si segnala inoltre la dichiarazione congiunta delle autorità di protezione dati europee riunite nel Gruppo Art. 29, adottata il 26 novembre (WP 227, doc. web n. 3815254). La dichiarazione (anch'essa presentata in occasione del predetto *European data governance forum* di Parigi), muovendo dalle problematiche emerse con il caso Snowden (senza limitarsi ad esse), richiama i principi fondamentali di protezione dei dati e l'importanza di un approccio preventivo fondato sulla *privacy by design* in grado di garantire un agevole esercizio dei diritti da parte degli interessati. Raccomanda inoltre una tempestiva adozione del regolamento e della Convenzione 108 modernizzata (mantenendo il più alto livello di protezione dei diritti), che gli accordi commerciali quali il TTIP e TISA non ero-

dano i principi di protezione dei dati, che una protezione rinforzata sia assicurata ai diritti dei minori, specie *online*, che la *digital education* diventi una priorità dei governi. La Dichiarazione condanna, infine, qualsiasi forma di sorveglianza massiva e indiscriminata e la conservazione non selettiva di dati.

PNR

In materia di raccolta anticipata dei dati dei passeggeri aerei (PNR), il Gruppo ha seguito inoltre lo sviluppo dei progetti nazionali che utilizzano il programma di finanziamento messo a disposizione dalla Commissione europea.

Protezione dei dati in ambito finanziario

È stata riavviata l'attività del Gruppo riguardo alle tematiche di protezione dei dati in ambito finanziario, in particolare con l'assunzione da parte del Garante del coordinamento del sottogruppo "*Financial matters*" a partire da giugno 2014, su mandato della plenaria.

L'attività del Gruppo si è concentrata sul tema dello scambio automatizzato di dati a fini fiscali, un fenomeno in crescente espansione a livello europeo e internazionale.

In particolare, anche sull'onda del consenso politico ottenuto dal FATCA (la legislazione USA anti evasione fiscale *offshore*), l'OCSE, su mandato del G20, ha adottato i cd. *common reporting standard* che si propongono quale modello globale per lo scambio di informazioni tra amministrazioni fiscali ai fini della lotta all'evasione. Il documento OCSE, oltre a prevedere criteri comuni per la raccolta (e l'invio alle amministrazioni competenti) di dati relativi ai clienti da parte degli istituti finanziari, riporta un modello di accordo che può essere utilizzato dalle amministrazioni fiscali nazionali per lo scambio di tali dati.

Il Gruppo, con la lettera indirizzata all'OCSE, al G20 e alle istituzioni comunitarie competenti, pur riconoscendo che la lotta all'evasione fiscale rappresenta un legittimo interesse pubblico, ha richiamato la necessità che tale finalità sia perseguita nel dovuto rispetto dei diritti fondamentali e non porti a raccolte e scambi massivi, non proporzionati allo scopo perseguito. La lettera fa riferimento alla sentenza della Corte di giustizia dell'8 aprile 2014 che ha invalidato la direttiva *data retention*, e sottolinea come i principi in essa contenuti abbiano portata generale e debbano essere considerati anche nel caso di scambi automatizzati di dati a fini fiscali. Richiama la necessità che gli accordi tra Stati derivanti dai CRS includano principi di protezione dei dati in maniera sostanziale e non si limitino ad un mero richiamo formale alla normativa. La lettera rinvia inoltre ad un allegato che contiene gli specifici elementi critici finora individuati nei CRS e i principi di protezione dei dati che dovrebbero essere considerati per garantire il rispetto della direttiva 95/46/CE. In particolare si segnala la necessità che gli scambi tra Stati abbiano una adeguata base giuridica, rispettino il principio di finalità (con una preliminare e chiara definizione dello scopo del trattamento ed evitando che, una volta acquisiti i dati, gli stessi siano poi impiegati per finalità incompatibili), prevedano criteri specifici di *data retention*, assicurino la trasparenza del trattamento con un'adeguata informativa agli interessati, garantiscano un agevole esercizio dei diritti, definiscano correttamente la titolarità del trattamento (e la presenza di eventuali responsabili) ed assicurino misure di sicurezza adeguate.

Il Gruppo ha continuato a seguire l'argomento dello scambio automatizzato di dati a fini fiscali anche in ragione dell'avvenuta adozione (9 dicembre 2014) della direttiva 2014/107 (recante modifica della direttiva 2011/16/UE per quanto riguarda lo scambio automatico obbligatorio di informazioni nel settore fiscale) che ha sostanzialmente recepito il modello OCSE dei CRS in ambito europeo, e in vista della predisposizione, da parte del Gruppo stesso, di future linee guida per i governi nazionali per una corretta implementazione dei principi di protezione dei dati.

Sempre sotto il coordinamento italiano, il Gruppo Art. 29 ha inoltre avviato un lavoro sul "*Multilateral Memorandum of Understanding*" (MMoU), predisposto dalla *International Organisation of Securities Commissions* (IOSCO), aperto alla firma

delle autorità di vigilanza nazionali, per una migliore cooperazione nel settore dei valori mobiliari e volto ad assicurare il rispetto delle discipline interne in tale settore. Con la lettera del 18 settembre 2014 il Gruppo si è rivolto a IOSCO, affinché in tale accordo siano tenuti in dovuta considerazione i profili di protezione dei dati (doc. web n. 3815644).

È stata altresì avviata una riflessione sull'impatto sulla protezione dei dati derivante sia dal pacchetto composto dalla direttiva 2014/65 relativa ai mercati degli strumenti finanziari (la cd. MIFID2), e dal regolamento 600/2014 (in particolare in relazione al rafforzamento previsto da tali strumenti normativi degli obblighi di registrazione di telefonate e comunicazioni elettroniche da parte delle società di investimento per consentire alle autorità competenti di svolgere i loro compiti di supervisione per un corretto andamento del mercato), sia dal regolamento 596/2014 in tema di abusi di mercato (cd. MAR).

Sia su MIFID2 che su MAR, sono stati predisposti *standard* tecnici (sottoposti a consultazione pubblica) da parte della *European Securities Markets Authority* (ESMA) con la quale il Gruppo ha aperto un dialogo al fine di orientare tali *standard* ad una corretta implementazione degli obblighi di protezione dei dati previsti dalla direttiva 95/46/CE.

Trasferimento dati all'estero

Facilitare il trasferimento dei dati all'estero salvaguardando, al contempo, il necessario rispetto del diritto alla protezione dei dati è stato, anche nel 2014, l'obiettivo che il Gruppo ha cercato di perseguire attraverso l'attività del sottogruppo *international transfers*.

***Referential* Bcr/CBPR e adeguatezza**

In quest'ottica, guardando in particolare al mondo delle multinazionali, è stato adottato a febbraio un documento di consultazione (*referential*) che individua i requisiti comuni alle norme vincolanti di impresa (Bcr) – autorizzate dalle autorità di protezione dei dati europee per i trasferimenti di dati personali effettuati, nell'ambito di un gruppo societario, al di fuori dell'Unione – e al sistema delle norme transfrontaliere in materia di *privacy* (CBPR) della Cooperazione economica Asia-Pacifico (APEC). Il documento potrà essere utilizzato, quale strumento comparativo dei due sistemi, dalle multinazionali che intendano presentare sia una domanda di approvazione di Bcr presso le DPA europee sia una richiesta di certificazione di CBPR da parte di un agente responsabile dell'APEC, al fine di ottenere una doppia certificazione (parere 2/2014, WP 212, doc. web n. 3815101).

In tema di adeguatezza delle discipline nazionali di Paesi terzi (adeguatezza in virtù della quale i trasferimenti di dati dall'UE possono avvenire senza alcun tipo di autorizzazione) e tutela dei diritti degli interessati, il Gruppo si è pronunciato con particolare chiarezza sia nel parere relativo alla (non) adeguatezza del Québec (WP 219 Opinion 7/2014, doc. web n. 3815174) che in una lettera inviata alla Commissione europea in relazione al processo di valutazione del regime attuale del *Safe Harbour* ancora in corso.

Con riferimento alla legislazione del Québec, il Gruppo ha ritenuto che la stessa, per poter essere dichiarata adeguata, necessita dell'introduzione di ulteriori misure, anche normative, volte a chiarire l'ambito di applicazione territoriale della legge nazionale, a garantire adeguata tutela ai dati sensibili (categoria non chiaramente definita dall'attuale legislazione) e individuare strumenti vincolanti per il trasferimento di dati all'estero (rilievo quest'ultimo importante tenuto conto che in Québec è stabilita l'Agenzia mondiale *anti-doping* - WADA che raccoglie e tratta i dati che gli atleti sono tenuti a comunicare per le finalità *anti-doping*, attraverso la banca dati ADAMS; cfr. al riguardo par. 4.1).

Ancor più rigorosa la lettera inviata dal Gruppo alla Commissione europea concernente il funzionamento del *Safe Harbour* (cfr. Relazione 2013, p. 181 e doc. web

n. 2983002) nella quale si sollevano dubbi in ordine all'adeguatezza del sistema come attualmente configurato e si profila la possibilità che l'accordo sia sospeso ove il processo di revisione condotto dalla Commissione con le autorità USA non porti ad un risultato positivo. La lettera fornisce diversi suggerimenti per migliorare il sistema allo stato in vigore. Si suggerisce una maggiore trasparenza in ordine ai soggetti che possono far parte del sistema, alle regole per le società che agiscono in qualità di responsabili del trattamento e una maggiore tutela dei diritti degli interessati residenti in EU (si chiede, in particolare, che agli stessi possa essere riconosciuto il diritto di adire una corte europea come pure che siano loro riconosciuti gli stessi diritti dei cittadini statunitensi). Si auspica inoltre l'introduzione di una nozione di "trattamento" analoga a quella prevista dalla direttiva, che includa anche la mera raccolta dei dati e l'inserimento di un chiaro riferimento al rispetto dei principi di necessità e proporzionalità anche nel caso in cui operi la deroga prevista per la sicurezza nazionale e sia consentita, quindi, una *disclosure* dei dati alle autorità pubbliche statunitensi (doc. web n. 3820223).

Clausole contrattuali tipo

Il Gruppo è intervenuto anche in materia di clausole contrattuali, adottando, a marzo, un documento di lavoro sul modello di clausole contrattuali *ad hoc* per i trasferimenti da un EU *processor* a non-EU *subprocessor* (WP 214, *Working document* 1/2014, doc. web n. 3815346) che potrà essere utilizzato nei casi in cui un responsabile del trattamento stabilito sul territorio europeo (EU-*processor*) intenda "subappaltare" attività che comportino il trattamento di dati a soggetti stabiliti in Paesi terzi (non EU-*subprocessor*). Le clausole, pur non essendo clausole contrattuali *standard* adottate dalla Commissione europea (come quelle previste per il trasferimento di dati da titolare a titolare e da titolare a responsabile), intendono costituire un modello cui le società possono ispirarsi nel caso di trasferimenti fra responsabili del trattamento non coperti da altri strumenti quali, ad esempio, le Bcr *for processor*. Il documento è stato aperto ad una procedura di consultazione i cui esiti dovrebbero essere resi noti nel corso del 2015.

Sempre in materia di clausole contrattuali *standard*, il Gruppo ha adottato, a novembre, un documento di lavoro (WP 226, doc. web n. 3815244) che istituisce una procedura di cooperazione per emettere pareri comuni nei casi in cui una società, con più stabilimenti in diversi Stati membri, decida di utilizzare il medesimo strumento contrattuale per i trasferimenti di dati posti in essere dalle proprie filiali stabilite in UE e si trovi, pertanto, nella condizione di doversi rivolgere alle diverse DPA competenti al fine di ottenere una valutazione circa la conformità o meno delle proprie clausole ad uno dei *set* di clausole contrattuali tipo adottati dalla Commissione (si tratta spesso di società che rendono servizi di *cloud*, come nel caso delle clausole già sottoposte da Microsoft e Amazon).

Bcr *for controller* e Bcr *for processor*

Ormai consolidata è invece la procedura per l'adozione, a livello europeo, delle regole vincolanti d'impresa (Bcr), strumento sempre più diffuso per il trasferimento dei dati effettuato tra società appartenenti ad un medesimo gruppo che operino in qualità di titolare del trattamento (Bcr *for controller*, Bcr-C) o in qualità di responsabili del trattamento (Bcr *for processor*, Bcr-P).

Nel 2014 sono state avviate 9 procedure per Bcr-C e 2 per Bcr-P e sono state concluse, con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute, 13 Bcr-C e 6 Bcr-P; l'Autorità è intervenuta in qualità *co-reviewer* in 5 procedure (per le autorizzazioni nazionali si fa rinvio al par. 18) fornendo specifiche indicazioni in ordine a modifiche da apportare nel testo delle Bcr (una delle quali *for processor*) proposte dalle società al fine di renderle conformi al quadro normativo europeo.

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

Europol: l'attività dell'Autorità di controllo comune (ACC)

L'attività dell'ACC Europol, che a giugno ha eletto i nuovi organi (presidente Vanna Palumbo del Garante e vicepresidente l'olandese Wilbert Tomesen), si è incentrata da un lato, come nel 2013, sull'analisi della proposta di 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 (presentata dalla Commissione europea nel 2013, doc. web n. 2983062) e, dall'altro, sull'attività ispettiva svolta in relazione ai trattamenti di dati effettuati da Europol.

Con riguardo alle discussioni sul nuovo quadro normativo (rispetto al quale il Parlamento europeo ha adottato il proprio parere in prima lettura con emendamenti il 25 febbraio 2014) e alle modifiche proposte dal Consiglio (nell'ambito dell'approccio generale raggiunto dal Consiglio Giustizia ed Affari Interni di giugno), l'ACC ha verificato che sono stati accolti alcuni dei punti sollevati nei pareri dalla stessa resi nel 2013 (vedi Relazione 2013, p. 183), in particolare, per quanto riguarda la predisposizione di una base legale per il trattamento di dati nel sistema di messaggistica SIENA e la sua gestione e per la cooperazione diretta con le unità di analisi finanziaria (FIU) costituite in attuazione delle direttive antiriciclaggio. Passi indietro sembrano invece essere stati fatti rispetto al testo iniziale in materia di diritto di accesso degli interessati. Per quanto concerne la supervisione, una modifica importante riguarda il possibile coinvolgimento delle Autorità nazionali nel *board* accanto all'EDPS (modifica che potrà diventare definitiva però solo laddove la stessa risulti coerente con le scelte che matureranno nelle discussioni per aggiornare la base legale di Eurojust e creare l'EPPO). Alla luce di ciò, l'ACC ha adottato un terzo parere (doc. web n. 3815594) che, soffermandosi su tre aspetti principali (il trattamento dei dati sensibili e di diverse categorie di interessati, il diritto di accesso e la cooperazione tra le autorità nazionali e l'EDPS), ha concluso col ritenere il nuovo quadro normativo prospettato più fragile di quello attuale.

Per quanto concerne l'attività ispettiva, nel 2014, oltre alla tradizionale ispezione annuale di Europol svoltasi a marzo (cui ha partecipato, come negli anni scorsi, anche l'Autorità e rispetto alla quale è stato adottato a ottobre il consueto rapporto), l'ACC ha svolto, nel mese di settembre, una specifica attività volta ad accertare se le informazioni e i dati personali condivisi con Europol siano stati legittimamente acquisiti dalle autorità nazionali. L'ispezione – effettuata al fine di rispondere ad una specifica richiesta contenuta nel rapporto che la Commissione LIBE del Parlamento europeo ha adottato il 21 febbraio 2014 sui programmi di sorveglianza di massa (doc. web n. 3815717) – ha avuto ad oggetto oltre centocinquanta casi. Nella maggior parte di essi, gli elementi raccolti hanno consentito di escludere che i dati fossero stati acquisiti in violazione di legge; in alcuni casi, invece, tale verifica non ha potuto aver luogo o perché le informazioni trasmesse dalle autorità segnalanti non sono state sufficienti oppure perché coperte da un livello di classificazione che non ne consentiva la comunicazione. Alla luce di ciò, il rapporto adottato dall'ACC il 9 dicembre (doc. web n. 3815604) ha ribadito la necessità che le autorità nazionali forniscano ad Europol tutte le informazioni necessarie per consentire allo stesso di valutare la liceità delle informazioni trattate.

L'ACC ha deciso di approfondire, anche grazie all'esperienza maturata da Europol, il tema del traffico di esseri umani per definire orientamenti e raccomandazioni su come assicurare il rispetto dei principi di protezione dei dati e di tutela delle vittime nell'attività di analisi svolta da Europol e dagli Stati membri, garan-

tendo che nella fornitura di dati personali lo *status* di vittima o "potenziale" vittima sia adeguatamente evidenziato.

I sottogruppi dell'ACC hanno anch'essi continuato il loro lavoro. Il *New Project Group*, in particolare, ha approfondito alcuni nuovi progetti di Europol, riguardanti la strategia di sviluppo del sistema di messaggistica SIENA, un nuovo sistema di analisi, di archiviazione delle informazioni, il progetto per la creazione di una lista condivisa dei maggiori ricercati da parte degli Stati membri (*most wanted*).

L'ACC, al fine di instaurare/mantenere rapporti con le corrispondenti autorità dei Paesi terzi con cui Europol ha accordi operativi (che prevedono anche lo scambio di dati personali), ha incontrato, nel mese di giugno, le DPA di Svizzera, Liechtenstein, Macedonia-Fyrom e Monaco.

Il Comitato ricorsi ha ricevuto un nuovo caso da esaminare, sempre relativo ad una richiesta di riesame della risposta fornita da Europol ad una richiesta di accesso. Il Comitato, secondo quanto previsto dal regolamento interno, non avendo ricevuto le informazioni aggiuntive richieste al ricorrente, ha concluso l'analisi rigettando il ricorso.

Il Sistema Informativo Schengen: l'attività del Gruppo di coordinamento della supervisione SISII

Il Gruppo di coordinamento della supervisione SIS II, dopo il grave caso di *data breach* al SIRENE danese reso noto nel giugno 2013 (cfr. Relazione 2013, p. 185), ha proseguito la propria attività di approfondimento circa gli aspetti legati alla sicurezza del sistema, inoltrando alle autorità nazionali un questionario volto a favorire un *self-assessment* dei sistemi nazionali e della sicurezza in tema di trasmissione dei dati. Sebbene le risposte ricevute siano apparse abbastanza lacunose e disomogenee, un passo in avanti potrebbe comunque essere fatto attraverso l'entrata a regime del *Security officer network* (SON) lanciato dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA) proprio per il *report* di incidenti e per definire *standard* anche in relazione all'*outsourcing* di attività rilevanti nella gestione del SIS.

All'esito dei lavori avviati lo scorso anno, il Gruppo ha inoltre adottato la guida per l'esercizio dei diritti di accesso degli interessati ai dati che li riguardano contenuti nel SIS II che le autorità nazionali di protezione dei dati dovranno rendere disponibile anche nella lingua nazionale di riferimento.

Il Gruppo si è poi occupato dei criteri per l'introduzione nel sistema delle segnalazioni concernenti i veicoli rubati e delle ricerche sistematiche nel SIS sui clienti degli alberghi. La discussione in corso è spinta da alcuni Paesi che premono perché, con riferimento al tema dei veicoli rubati, l'interpretazione della relativa norma contenuta nella decisione SIS II sia tale da poter obbligare la cancellazione dal SIS delle segnalazioni nel momento in cui l'oggetto segnalato sia stato ritrovato o la condotta richiesta si sia perfezionata.

In tema di verifiche sistematiche del SIS sui clienti degli alberghi, il Gruppo ha ritenuto che, non avendo il nuovo quadro legale inciso sul contenuto della previgente normativa, restasse del tutto confermato il parere espresso nel 2011 dall'ACC Schengen che riteneva tale verifica non rispettosa del principio di finalità.

Gruppo di supervisione Eurodac

Nel corso delle riunioni tenutesi nel 2014, il Gruppo di supervisione del sistema Eurodac, partendo dall'approvazione del regolamento interno e della relazione di attività del biennio 2012-2013, ha analizzato gli aspetti su cui prioritariamente intervenire prima dell'entrata in vigore della nuova base giuridica (il 20 luglio 2015) derivante dall'adozione, il 26 giugno 2013, della proposta di rifusione (cd. *recast*) del regolamento Eurodac (regolamento (UE) n. 603/2013: cfr. Relazione 2013, p. 186, doc. web n. 2983052).

Il Gruppo ha deciso di impegnarsi, da un lato, a verificare la congruità ed esattezza degli elenchi delle autorità nazionali che possono accedere al sistema e la qualità delle impronte e, dall'altro, in previsione dell'entrata in vigore del nuovo quadro

giuridico, a verificare il funzionamento del sistema sia a livello di unità centrale (trasferita da Lussemburgo a Strasburgo e gestita dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala, EU-LISA) che a livello nazionale. La verifica dovrà approfondire, in particolare, le nuove funzionalità e le modifiche introdotte nel sistema per consentire l'accesso da parte delle autorità di *law enforcement* come ora previsto dal Regolamento (cfr. al riguardo Relazione 2013, p. 186), la cancellazione anticipata dei dati, i ruoli e le responsabilità dei diversi soggetti abilitati ad accedere ed inserire dati nel sistema, la trasmissione di dati a Paesi terzi, il cd. *blocking/marking* dei dati, le misure di sicurezza e l'esercizio dei diritti dell'interessato.

L'attività di verifica si svolgerà probabilmente in sinergia con gli altri due gruppi di supervisione (VIS, SIS II) gestiti da EU-LISA, tenuto conto della struttura informatica comune ai tre sistemi, realizzata sulla base del principio di interoperabilità delle piattaforme.

Il Sistema Informativo Visti [VIS]: Gruppo di coordinamento della supervisione

La qualità delle impronte raccolte è tra i temi trattati dal Gruppo di coordinamento della supervisione VIS considerata l'assenza di *best practices*, in particolare per la raccolta delle impronte biometriche (impronte digitali), spesso effettuata, attraverso contratti di *outsourcing*, da fornitori di servizi stabiliti in Paesi terzi. A tal proposito, sulla scorta di un approfondimento circa gli aspetti legali e le condizioni contenute nell'art. 43 del Regolamento (CE) n. 810/2009 del 13 luglio 2009 che istituisce il codice comunitario dei visti, il Gruppo ha predisposto una nota in cui evidenzia gli aspetti di protezione dati rilevanti, soffermandosi anche sull'eventuale possibilità per le autorità di protezione dei dati di effettuare controlli sull'operato di tali società all'estero. La nota si aggiunge ad una richiesta formulata alle DPA nazionali volta a prevedere controlli nei consolati per verificare *in loco* sia le modalità di raccolta delle informazioni (dal punto di vista delle misure di sicurezza adottate e delle regole che le società esterne devono rispettare con riferimento alla raccolta, al trattamento e alla restituzione dei dati) sia l'osservanza degli obblighi in materia di protezione dei dati; ciò, in particolare, per quanto riguarda l'informativa resa ai richiedenti il visto in relazione al possibile esercizio dei diritti di accesso, rettifica, etc. (soprattutto in caso di diniego del visto in presenza di una segnalazione Schengen). Un altro aspetto delicato su cui il Gruppo si è soffermato, ha riguardato alcuni casi di non allineamento VIS e SIS e quindi l'uso di informazioni SIS non aggiornate, con conseguenti effetti sull'accettazione/rifiuto del visto.

Sono stati inoltre definiti tre questionari (rispettivamente relativi a: lista delle autorità che possono accedere al VIS; accesso al VIS da parte delle autorità di *law enforcement* in base alla decisione 2008/633/GAI; esercizio dei diritti degli interessati) che consentiranno alle DPA di valutare eventuali carenze rispetto a quanto previsto dalle norme di riferimento; sulla base degli esiti di tali questionari, il Gruppo potrà decidere di intervenire adottando specifiche raccomandazioni laddove necessario.

Sono infine proseguiti i lavori per la definizione di una sorta di documento di metodologia comune per lo svolgimento delle ispezioni o *audit*.

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 SID si sono riunite *back to back* condividendo la supervisione sullo stesso *database*, dove sono contenuti dati relativi ad operazioni che possono anche coinvolgere fattispecie criminali. Il *database* peraltro risulta poco popolato e scarsamente utilizzato. Proprio per rimarcare il desiderio di procedere in parallelo nell'attività di supervisione che sostanzialmente riguarda gli stessi *file*, il Gruppo di supervisione ha eletto come vice *chair*, il *chair* dell'ACC Dogane.

Circa le attività, l'ACC Dogane ha fatto progressi per la definizione di un questionario, da inviare ad OLAF ed alle stesse DPA, come *follow up* dell'ispezione svoltasi nel 2011.

Per quanto concerne il Gruppo di supervisione, è stato discusso il programma di lavoro per il 2014-2015, che, una volta adottato, sarà comunicato all'esterno, in particolare a Commissione, Consiglio, Parlamento europeo.

Il Gruppo ha deciso, sulla scorta di quanto già fatto dalle altre autorità di supervisione, di lavorare su una guida per l'esercizio del diritto di accesso al sistema.

23.5. *La partecipazione ad altri comitati e gruppi di lavoro internazionali*

Consiglio d'Europa: CAHDATA

Anche il 2014 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, volto ad adeguarne i principi al mutato scenario tecnologico e ad assicurare un alto livello di tutela del diritto alla protezione dei dati. In particolare, si sono svolte la seconda e la terza (ed ultima) riunione (rispettivamente il 28-30 aprile e il 1-3 dicembre) del sopra menzionato CAHDATA (vedi par. 23).

Nell'ultima riunione del suo mandato, il CAHDATA, il cui rappresentante per l'Italia è il segretario generale del Garante Giuseppe Busia, ha adottato il testo finale della Convenzione modernizzata (doc. web n. 3815674). Tuttavia, seppur conclusosi con l'approvazione del testo, il processo di modernizzazione è stato fortemente influenzato dal parallelo lavoro di riforma del quadro di regole in materia di protezione dei dati in atto in ambito UE. La Commissione europea, che ha partecipato ai lavori del CAHDATA sulla base di un mandato del Consiglio UE a negoziare per conto degli Stati UE nelle materie di competenze comunitaria, non avendo (come si è anticipato) ancora sciolto alcuni nodi in sede di discussione del nuovo regolamento UE sulla protezione dei dati, pur dando un generale supporto al testo del CAHDATA, ha mantenuto riserva su alcuni principi (v. *infra*). Sul testo adottato dal CAHDATA, accanto ad alcune riserve di delegazioni nazionali, permangono quelle della Commissione che potranno venir meno solo una volta raggiunto un accordo tra gli Stati nell'elaborazione del Regolamento UE.

Il CAHDATA ha comunque dato mandato al segretariato del Consiglio d'Europa di predisporre il protocollo emendativo della Convenzione 108 che rifletterà il testo concordato in riunione e di allineare il *memorandum* esplicativo, nel frattempo predisposto dal Comitato T-PD, a quanto deciso in riunione. Il testo della nuova Convenzione 108 – che darà conto in nota delle riserve – sarà trasmesso al Comitato dei ministri del Consiglio d'Europa nel corso del 2015, passo comunque necessario per la finalizzazione della nuova Convenzione in sede di CoE.

T-PD

Sempre nell'ambito del Consiglio d'Europa è proseguita l'attività del T-PD, Comitato consultivo della Convenzione 108/1981 a cui il Garante partecipa da anni, anche nella sua composizione ristretta (T-PD *bureau*) e con l'incarico, ottenuto nel 2014, della vice-Presidenza.

Il T-PD, che nel 2012 aveva concluso il lavoro tecnico relativo alla modernizzazione della Convenzione 108, con l'adozione del un documento finale contenente le proposte di revisione (poi impiegato dal CAHDATA come base di discussione), ha proseguito il suo lavoro di approfondimento e supporto per la modernizzazione della 108, in particolare con la predisposizione del *memorandum* esplicativo che accompagnerà la nuova Convenzione.

È giunto invece a conclusione il lavoro del T-PD sul processo di revisione della raccomandazione 89(2) sulla protezione dei dati in ambito lavorativo. Nella plenaria di giugno il T-PD ha infatti adottato la nuova bozza di raccomandazione volta a sostituire il testo del 1989, adottata infine dal Comitato dei ministri il 1° aprile