Sottolinea inoltre l'importanza che la direttiva collochi la correttezza del trattamento tra i suoi princìpi chiave.

Quanto al principio di finalità, il documento richiama l'attenzione sulla necessità di garantire una idonea base legale per ogni ulteriore finalità del trattamento – non incompatibile – rispetto a quella originaria. Si chiede, inoltre, di inserire nuovamente nel testo dell'articolato la necessità di tener distinte le varie categorie di soggetti cui i dati si riferiscono (sospetti, non sospetti, vittime, testimoni, ecc.) e di ridefinire il trattamento dei dati sensibili (cui vanno aggiunti i dati biometrici) sulla base del principio del divieto come regola, prevedendo poi le eccezioni. Si chiede inoltre di specificare che la profilazione non può avvenire a partire dai dati sensibili. Quanto ai diritti dell'interessato il documento chiede il ripristino di diverse garanzie esistenti nel testo iniziale della Commissione, anche per quanto concerne il trattamento di dati di minori. Ulteriori osservazioni sono formulate riguardo ai poteri delle Autorità di protezione dati, la sicurezza del trattamento dei dati, gli obblighi del titolare, l'informazione in caso di *data breach*, il trasferimento di dati verso Paesi terzi.

Il Gruppo ha inoltre lavorato alla preparazione di una dichiarazione sulle conseguenze della sentenza della CGUE dell'8 aprile 2014 che ha annullato la direttiva sulla conservazione dei dati di traffico (direttiva *data retention*). La bozza di dichiarazione è stata predisposta dal Garante e dai colleghi della Repubblica ceca, soffermandosi soprattutto sulla necessità di un'applicazione uniforme delle legislazione di protezione dei dati, in particolare con riferimento ai tempi di conservazioni dei dari, e alle Linee guida su come garantire che l'accesso delle autorità di *law enforcement* sia selettivo e non massiccio ed indiscriminato. Il lavoro svolto è alla fine confluito in un questionario predisposto dal Garante volto ad ottenere informazioni sulla situazione negli Stati membri, al fine di acquisire elementi sui regimi di *data retention* esistenti nei vari Paesi e valutare quale sia stato l'impatto su di essi della sentenza della CGUE.

Sempre riguardo alla conservazione dei dati, si evidenzia che l'Alta Corte di giustizia del Regno Unito ha bocciato, il 17 luglio, la legge adottata, in via d'urgenza nel 2014 (*Data Retention and Investigatory Powers Act* – DRIPA). La Corte ha ritenuto che la stessa non forniva regole precise e chiare per assicurare che ai dati si potesse avere accesso, solo con l'autorizzazione di un giudice o di un'autorità indipendente, al fine di prevenire e accertare "*serious offences*" e per i soli casi strettamente necessari.

In tema di *cybercrime*, il Gruppo ha adottato ed inviato una lettera al Comitato per la Convenzione sul *cybercrime* (T-CY) del Consiglio d'Europa in occasione della Conferenza sul *cybercrime* (17-19 giugno, Strasburgo): la lettera, nel ricordare che in Europa trovano applicazione, per i trattamenti per finalità di *law enforcement* la direttiva 95/46 (anche se con le deroghe di cui all'art. 13 della stessa), la Convenzione 108/1981, la raccomandazione 87(15) e la decisione quadro 2008/977, richiama l'attenzione sulla necessità di rispettare sempre il principio di liceità del trattamento, di non considerare mai il consenso dell'interessato come idoneo presupposto per legittimare i trattamenti per finalità di *law enforcement* ed analizza i 18 scenari prospettati alla scorsa Conferenza sul *cybercrime*, fornendo, ove possibile, alcune specifiche indicazioni (doc. web nn. 4814829 e 4814840).

È inoltre proseguita l'attività su PNR, con la predisposizione di una lettera contenente i commenti del Gruppo Art. 29 sullo stato del negoziato relativo alla proposta di un PNR europeo e il rapporto presentato dal relatore al Parlamento europeo adottata il 19 marzo. Si è inoltre tenuto un seminario il 18 marzo organizzato dalla Commissione europea in cui si sono confrontati rappresentanti delle Autorità di protezione dati e dei governi che beneficiano dei finanziamenti per progetti PNR

nazionali. Il Gruppo ha anche incontrato gli esponenti delle compagnie aeree europee riuniti nell'AEA (SAS, *AirFrance, British Airways, Lufthansa, Austrian Airlines, Brussels Airlnes,* KLM, IATA) per rappresentare i timori delle compagnie riguardo alle richieste di dati PNR del governo messicano che, dal 1° aprile ha previsto importanti sanzioni ai vettori europei per mancato trasferimento di dati PNR.

In tema di TFTP (*Terrorist Finance Tracking Programme*), il Gruppo ha anche adottato (23 marzo) ed inviato una lettera alle istituzioni comunitarie per chiedere che le DPA siano coinvolte sulla rinegoziazione dell'Accordo TFTP (doc. web n. 4814901). La lettera tiene anche conto delle osservazioni formulate dal Garante per l'ACC Europol.

Inoltre, il Gruppo ha iniziato ad esaminare il tema delle intercettazioni dei cavi transatlantici e il Garante ha partecipato il 30 luglio alla prima riunione (tenutasi all'Aja) del gruppo ristretto di *drafting* (composto da rappresentanti di diversi sottogruppi del WP29) al fine di predisporre una bozza di indice per un parere in materia.

Cooperation

Nell'ottica di intensificare la cooperazione tra le Autorità di protezione dati, il Gruppo di lavoro ha cominciato a dedicare parte di attività ad incontri e *workshop* mirati ad anticipare parte del futuro lavoro derivante dai nuovi obblighi previsti dalla proposta di regolamento UE di protezione dati (assistenza reciproca, sportello unico, meccanismo di coerenza, ecc.). In particolare, si è tenuto a Budapest presso l'Autorità ungherese il 17 e 18 novembre un *workshop* avente ad oggetto la redazione di un unico e condiviso modulo di "ricorso" da utilizzare per i casi transfrontalieri in cui è necessaria una cooperazione ed assistenza tra le Autorità. È stata condivisa l'opportunità di redigere un unico modulo da utilizzare sia nel periodo transitorio che sotto il nuovo regolamento e di creare una piattaforma dedicata per lo scambio di informazioni fra le Autorità. È emerso il problema della lingua (e relativi costi) da utilizzare per la cooperazione (un accordo generale è stato espresso sulla lingua inglese) ed il problema della tempistica e delle diverse divergenze nazionali sui tempi per la decisione.

Come risultato del *workshop*, il Gruppo ha elaborato una prima bozza di modulo per la cooperazione su ricorso.

Protezione dei dati in ambito finanziario

È stata intensa l'attività del Gruppo riguardo alle tematiche di protezione dei dati in ambito finanziario, in particolare con la prosecuzione da parte del Garante, su mandato della Plenaria, del coordinamento del sottogruppo *Financial matters*.

Il Gruppo ha continuato ad occuparsi dello scambio automatizzato di dati a fini fiscali, un fenomeno in crescente espansione sia a livello internazionale (v. i *common reporting standard* dell'OCSE che si propongono quale modello globale per lo scambio di informazioni tra amministrazioni fiscali ai fini della lotta all'evasione internazionale), sia a livello europeo, in particolare con la 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 (v. Relazione 2014, p. 177).

Tale tema è stato oggetto della dichiarazione del Gruppo del 4 febbraio 2015 (WP230, doc. web n. 4810708), rivolta ai governi nazionali e alle istituzioni comunitarie competenti affinché gli accordi bilaterali e multilaterali che prevedono scambi automatizzati di dati a fini fiscali, nonché le relative normative nazionali, assicurino adeguate garanzie per la protezione dei dati senza portare a raccolte e scambi massivi, non proporzionati allo scopo perseguito.

Il Gruppo ha quindi predisposto e adottato un questionario sullo scambio automatizzato di dati a fini fiscali, rivolto alle aurorità nazionali competenti. Attraverso il questionario sono state raccolte informazioni sul livello di implementazione da parte dei diversi Stati membri degli obblighi, introdotti a livello europeo ed inter-

nazionale, di scambio-dati nell'ambito della lotta all'evasione fiscale. Le risposte pervenute hanno costituito una base informativa su cui è stato fondato il lavoro di elaborazione di specifiche Linee guida (WP234, doc. web n. 4810763) indirizzate ai governi affinché i princìpi di protezione dei dati siano tenuti in dovuta considerazione nei relativi accordi (bilaterali e multilaterali) che prevedano lo scambio di informazioni per il contrasto all'evasione fiscale. La redazione del testo delle *Guidelines* è stata curata dal Garante e dall'EDPS (*co-rapporteur*), anche alla luce del confronto avuto con esperti della Commissione europea (DG TAXUD) che, nel supportare il lavoro del Gruppo, hanno suggerito di dividere le Linee guida in raccomandazioni per Stati membri e raccomandazioni per Paesi terzi. Le Linee guida forniscono indicazioni circa le garanzie di protezione dei dati da applicare in tre diversi casi: (i) nello scambio di dati personali tra gli Stati membri dell'UE; (ii) nello scambio di dati personali tra uno Stato membro dell'UE e un Paese terzo che è stato oggetto di una decisione di adeguatezza della Commissione europea, e (iii) nello scambio di dati personali tra uno Stato membro UE e un Paese terzo che non è stato oggetto di una decisione di adeguarezza della Commissione europea. Vengono inoltre identificate diverse garanzie che dovrebbero essere sempre inserite nel contesto dello scambio automatico di dati per il contrasto all'evasione fiscale.

Sempre in tema di lotta all'evasione fiscale, il Gruppo ha avanzato un'esplicita richiesta in merito allo stato di ratifica dell'Accordo FATCA (*Foreign Account Tax Compliance Act,* la legislazione USA anti evasione fiscale *off shore*) nei vari Stati membri (cfr. par. 4.6). Il Garante ha raccolto e analizzato i contributi pervenuti dalle diverse delegazioni. Le informazioni raccolte mostrano che la maggior parte dei Paesi ha firmato (e poi recepito nella legislazione nazionale) l'Accordo tra il proprio governo e il governo degli USA al fine di migliorare la *compliance* fiscale e applicare la normativa FATCA. Solo in un caso, uno Stato membro ha firmato l'Accordo che però non è ancora in vigore. In altri casi, l'Accordo FATCA è stato firmato ed è entrato in vigore senza la necessità di una proceduta di ratifica in base alla loro legislazione nazionale. È opportuno sottolineare che alcuni Stati membri prevedono di firmare Accordi di attuazione del FATCA il più presto possibile. In base all'analisi delle risposte il Gruppo discuterà gli ulteriori passi da intraprendere (ad es., la possibile valutazione della qualità delle misure di recepimento – se presenti – in base al diritto nazionale dal punto di vista della protezione dei dati, nonché il coordinamento delle azioni di *enforcement* sulle norme di attuazione di FATCA).

Nel 2105, il Gruppo ha altresì portato avanti l'analisi delle normative cd. MIFID2 (pacchetto composto dalla direttiva 2014/65 relativa ai mercati degli strumenti finanziari e dal regolamento 600/2014, cd. MIFIR) e MAR (*Market Abuse Regulation*: regolamento 596/2014 relativo all'abuso di informazioni privilegiate e la manipolazione del mercato). Durante un incontro con esperti della Commissione europea (DG FISMA), per entrambi gli strumenti normativi sono emersi alcuni punti di criticità sui seguenti aspetti: a) 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; b) *whistleblowing*; 3) pubblicazione delle sanzioni e, con specifico riferimento a MAR: 4) prevenzione e rilevazione dell'abuso di mercato e 5) le cd. *insider lists*. Dalla discussione è emersa altresì la necessità che nell'effettiva implementazione dei princìpi *privacy*, di cui si è occupata ESMA (*European Securities Markets Authority*) attraverso la predisposizione di *Technical standard*, occorrerebbe un intervento del Gruppo Art. 29 per declinare tali princìpi in termini più concreti. In proposito si è anche tenuto un incontro con ESMA che ha confermato le predette criticità. Di conseguenza il Gruppo ha adottato ed inviato una lettera alla

Commissione (DG FISMA) per evidenziare nuovamente gli aspetti problematici degli *standard* tecnici che ESMA ha elaborato (doc. web n. 4814764).

Infine, il Gruppo ha replicato alla lettera con cui l'*International Organisation of Securities Commissions* (IOSCO) ha risposto alla lettera adottata dal Gruppo il 18 settembre 2014 con la quale il WP29 aveva rilevato l'assenza di salvaguardie, sul piano della protezione dei dati, nel "*Multilateral Memorandum of Understanding concerning consultation and the exchange of information*" (MMoU), aperto alla firma delle autorità di vigilanza, per una migliore cooperazione nel settore dei valori mobiliari e volto ad assicurare il rispetto delle discipline interne in tale settore (doc. web n. 4814818).

Trasferimento dati all'estero

Il tema dell'accesso da parte di autorità pubbliche di Paesi terzi ai dati personali trasferiti all'estero attraverso gli strumenti previsti dagli artt. 25 e 26 della direttiva 95/46/CE e delle misure che devono essere adottate al fine di garantire il rispetto dei principi di necessità e proporzionalità anche nel caso in cui tali accessi siano effettuati sulla base delle deroghe previste per ragioni di giustizia o sicurezza pubblica è stato al centro dell'attività svolta, nel corso dell'anno, dal Gruppo attraverso il sottogruppo *International Transfers*.

Documento esplicativo sulle *Binding corporate rules for processor*

In particolare, l'argomento è stato affrontato nel documento esplicativo sulle *Binding corporate rules* per responsabili del trattamento (WP 204 rev. 01, doc. web n. 4810659) che ha modificato il precedente documento relativo alle *Bcr for processor* al fine di meglio chiarire i contenuti dell'obbligo di segnalazione alle DPA posto in capo ai *processor* (responsabili del trattamento) che ricevono una richiesta di *disclosure* da parte delle autorità di *law enforcement* o di pubblica sicurezza di un Paese terzo. Secondo le nuove indicazioni, le società dovranno comunicare alle DPA competenti tutte le informazioni disponibili in relazione alla richiesta ricevuta per consentire a queste ultime di valutare l'eventuale blocco o divieto di trasferimento ulteriore di dati; nel caso di divieti di comunicazione in ordine alla richiesta di *disclosure* ricevuta, le società dovranno cercare di adempiere all'obbligo, anche impugnando dinanzi alle corti competenti tali divieti. Nel caso in cui la preventiva informazione alle DPA risulti impossibile, le società dovranno fornire comunque, successivamente alla *disclosure*, informazioni sulle richieste ricevute (e, eventualmente, sulle ragioni per le quali non sia stato possibile informare prima la DPA).

Invalidità della decisione di adeguatezza del *Safe Harbour* e conseguenze

Lo stesso tema è stato discusso poi nel quadro di un'analisi avviata per verificare gli effetti della sentenza Schrems della CGUE – che ha invalidato la decisione 2000/250 con cui la Commissione europea aveva dichiarato adeguata la protezione offerta dal cd. "approdo sicuro" (v. *supra*) – non solo sulle decisioni di adeguatezza della legislazione di un Paese terzo, ma anche sugli altri strumenti di trasferimento dei dati all'estero previsti dall'art. 26 direttiva 95/46/CE (Clausole contrattuali *standard* adottate dalla Commissione europea, contratti *ad hoc*, *Binding corporate rules* e deroghe).

Al riguardo, il 16 ottobre, il Gruppo Art. 29 ha adottato uno *statement* (doc. web n. 4810342) con il quale ha anzitutto ribadito che, tenuto conto della sentenza, i dati personali non possono essere più trasferiti dall'UE agli USA sulla base del *Safe Harbour* e che pertanto, per porre in essere tali trasferimenti, si deve, allo stato, far riferimento alle deroghe previste dall'art. 26, par. 1 (da interpretare restrittivamente tenuto conto che si tratta appunto di "deroghe") e, soprattutto, agli strumenti di cui all'art. 26, par. 2 (clausole contrattuali *standard* e *ad hoc*, Bcr). Anche il ricorso a tali strumenti, tuttavia, dovrà essere attento: il titolare del trattamento deve infatti addurre comunque garanzie "adeguate" per i trasferimenti anche alla luce degli specifici elementi evidenziati dalla Corte (necessaria esistenza sia di rimedi giuridici che consentano all'interessaro di accedere a dati personali che lo riguardano, di ottenerne la rettifica o la soppressione, sia di misure volte ad evitare accessi da parte di soggetti pubblici che non siano necessari e proporzionati in una società democra-

tica). Le autorità di protezione dei dati sono tenute infatti ad esercitare i propri poteri di sospendere o vietare i trasferimenti nei casi in cui le salvaguardie addotte, di volta in volta, da ciascun titolare non siano considerate sufficienti. I poteri di controllo delle autorità saranno utilizzati ove possibile in modo coordinato, specie nel caso in cui istituzioni UE e Stati membri non individuino una soluzione politica che tenga conto della necessità di rispettare l'essenza del diritto fondamentale alla protezione dei dati anche in occasione dei trasferimenti di dati in Paesi terzi.

Alla luce della sentenza, la Commissione europea e gli Stati Uniti, già da tempo impegnati sul tema dei trasferimenti dei dati nell'ambito del processo di revisione del *Safe Harbour* avviato nel 2013 (cfr. Relazione 2013, p. 181), hanno proseguito le negoziazioni al fine di definire un nuovo quadro di riferimento per la protezione dei flussi transatlantici dei dati personali che tenga conto dei rilievi mossi dalla Corte di giustizia e superi tutti i dubbi in ordine all'adeguatezza del precedente sistema (cfr. anche Relazione 2014, p. 178): nel febbraio 2016 la Commissione ha così reso disponibile la documentazione relativa ad un nuovo sistema denominato "EU-US *Privacy Shield*" (comprendente una bozza di decisione di adeguatezza e le lettere di impegni degli organismi statunitensi competenti) che, ove considerato adeguato dalla Commissione medesima ai sensi dell'art. 25 della direttiva 95/46/CE, potrà consentire il libero trasferimento di dati personali verso le società statunitensi che vi aderiranno.

Soggetti pubblici e trasferimenti di dati personali

Sempre in tema di trasferimenti di dati verso Paesi terzi, il Gruppo ha lavorato sul tema dei trasferimenti di dati personali tra istituzioni e soggetti pubblici per finalità di cooperazione amministrativa. In materia, si ravvisa la necessità che i principi di protezione dei dati siano tenuti in considerazione nella predisposizione degli accordi per il trasferimento di dati tra soggetti pubblici UE e non-UE quando il Paese di destinazione non assicura una protezione adeguata, anche attraverso specifiche clausole che riguardino, in particolare, la liceità del trattamento, la proporzionalità e la qualità dei dati, il principio di finalità, la conservazione dei dati, le misure di sicurezza, i trasferimenti ulteriori di dati, la clausola di supervisione.

Bcr for controller* e *Bcr for processor

Con riguardo ai trasferimenti di dati verso Paesi terzi, continua l'attività di cooperazione del Garante nel quadro della procedura per l'adozione, a livello europeo, delle regole vincolanti d'impresa (Bcr) che possono essere utilizzate 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 2015 sono state avviate 13 procedure per Bcr-C e 3 per Bcr-P e sono state concluse, con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute, 10 Bcr-C e 2 Bcr-P (per le autorizzazioni nazionali v. cap. 17).

L'Autorità ha partecipato in qualità *co-reviewer* in 5 procedure 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.

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

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

Come per il 2014, l'ACC Europol – che si è riunita quattro volte nel corso dell'anno – ha concentrato la propria attenzione sul processo legislativo relativo 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 nel 2013 dalla

Commissione europea, doc. web n. 2983062) e sulla necessità di garantire, attraverso la propria attività ispettiva ed i propri sottogruppi, che i trattamenti di dati personali siano effettuati da Europol nel rispetto della disciplina di protezione dei dati.

Con riferimento al nuovo quadro normativo, la cui definizione risulta imminente alla luce dell'accordo che sembra essere stato raggiunto alla fine dell'anno dalle tre istituzioni europee nell'ambito del trilogo, l'ACC (nelle persone della presidente Vanna Palumbo e vicepresidente Wilbert Tomesen) ha incontrato, il 22 giugno, il relatore della proposta di regolamento al Parlamento europeo per discutere alcuni aspetti sostanziali del nuovo quadro giuridico e, in particolare, il tema della supervisione. In proposito è stata ribadita la necessità, già evidenziata nei pareri espressi dall'ACC sulla proposta di regolamento (doc. web nn. 2983184, 2983132 e 3815594), di mantenere un ruolo effettivo alla cooperazione tra le Autorità nazionali di protezione dati, attesa la complessità del sistema e la rilevanza dell'attività di Europol per le attività giudiziarie e di polizia nazionali. Tale cooperazione dovrebbe, in effetti, essere garantita dal nuovo regolamento che attribuisce la supervisione all'EDPS coadiuvato da un Gruppo di coordinamento composto da rappresentanti delle DPA nazionali.

Alla luce dell'entrata in vigore del nuovo testo – attesa per la primavera del 2017 – l'ACC ha iniziato a riflettere sul futuro della supervisione su Europol, costituendo un gruppo di lavoro con il compito di approfondire il tenore dei cambiamenti ed in particolare di identificare i compiti che il Gruppo di coordinamento dovrà svolgere e la continuità/discontinuità con le attività svolte finora nonché gli aspetti logistici, organizzativi (segretariato, regolamento interno) e finanziari.

Per quanto riguarda l'attività ispettiva, nel marzo 2015, come di consueto, si è svolta l'ispezione annuale di Europol, effettuata in modo particolarmente approfondito per verificare il rispetto di tutte le prescrizioni impartite negli anni, lo stato della loro attuazione ed il livello di criticità di quelle non adempiute.

A maggio 2015, l'ACC ha poi svolto un'ispezione dedicata alle attività poste in essere da Europol in relazione all'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 (TFTP - *Terrorist Finance Tracking Program*). Nel relativo rapporto (adottato a settembre 2015, doc. web n. 4810393) – che, nel complesso, valuta l'attività svolta dal dicembre 2012 al maggio 2015 come conforme alla disciplina di riferimento – l'Aurorità ha ribadito che persiste una tensione rra l'idea di limitare la quantità di dati trasmessi ai sensi dell'art. 4 dell'Accordo con la natura dell'Accordo medesimo sulla base del quale, comunque, persiste un trasferimento massivo e regolare di informazioni finanziarie dall'Unione europea agli USA.

All'esito dell'approfondimento relativo al tema del traffico di esseri umani, avviato nel 2014 sulla scorta dell'esperienza maturata da Europol e Eurojust (che tratrano e analizzano anche i dati personali relativi alle vittime di tale rraffico trasmessi dalle autorità di contrasto degli Stati membri dell'UE e da parti terze), l'Autorità ha poi adottato un Rapporro sulle vittime della tratta di esseri umani (doc. web n. 4814921). Il documento, predisposto anche al fine di migliorare la qualità dei dati contenuti negli archivi Europol e sviluppare una maggiore attenzione all'identificazione precoce delle vittime, constata che, a livello sia nazionale che internazionale, le attività di trattamento dei dati condotte da tutte le autorità competenti (polizia, pubblici ministeri e giudici istruttori) dovrebbero essere caratterizzate da un'attenzione e un'armonizzazione maggiori. Il rispetto dei princìpi di necessità, proporzionalità, finalità e qualità dei dati relativi alle vittime della tratta risulta infatti essenziale nel quadro del più ampio fine della prorezione

22

di questi soggetti. La relazione è stata anche sostenuta dall'Autorità di controllo comune di Eurojust.

Nel 2015, è continuata anche l'attività dei sottogruppi dell'ACC. Si è infatti riunito il Comitato ricorsi e, più volte, il *New Project Group*. Quest'ultimo, in particolare, ha proseguito la propria valutazione sul progetto per la creazione di una lista europea degli individui più ricercati (*EU Most Wanted List*) in relazione al quale l'ACC ha espresso forti perplessità per la mancanza, nel quadro giuridico esistente, di una apposita base giuridica che consenra ad Europol di svolgere questo trattamento come titolare del trattamento.

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

Il Gruppo di coordinamento della supervisione SIS II ha avviato, con una visita realizzata a settembre 2015, insieme con i gruppi di coordinamento della supetvisione VIS e Eurodac (v. *infra*) un'attività di narura "conoscitiva" sui trattamenti posti in essere dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA) presso il *data center* di Strasburgo all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac. Lo scopo della visita, coordinata dai *Data Protection Officer e Data Security Officer* di EU-LISA, è stato quello di acquisire prime informazioni sull'architettura dei sistemi e sulle misure di sicurezza adottate.

Il sottogruppo sta inoltte lavorando su modelli comuni – uno per l'*audit* del SIS II e l'altro per le ispezioni – che potranno essere impiegati per attività ispettive in ambito nazionale da patte delle DPA, in modo da garantire il massimo grado di armonizzazione con le azioni svolte a livello centralizzato nel nuovo quadro di supervisione a livello EU.

Il Gruppo ha continuato ad occuparsi dei criteri per l'introduzione nel sistema delle segnalazioni concernenti i veicoli rubati con l'idea di elaborare una posizione comune su come interpretare le disposizioni relative alle azioni da intraprendere nel caso in cui un veicolo segnalato come tubato nel SIS venga localizzato in altro Paese e se debba prevalere la buone fede dell'acquirente laddove non sia richiesta la restituzione/sequestro del mezzo con conseguente cancellazione della segnalazione.

Gruppo di supervisione Eurodac

In relazione all'entrata in vigore (il 20 luglio 2015) della nuova base giuridica 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 di supervisione del sistema Eurodac (che ha eletto come presidente Elisabeth Wallis e nuovo vice Andres Ojaver) sta lavorando su un rapporto che fornisca un quadro delle modalità con cui il sistema è utilizzato nei divetsi Stati membri.

Per valutare l'impatto dell'entrata in vigore del nuovo quadro giutidico e al fine di acquisire prime informazioni sull'architettura dei sistemi e sulle misure di sicurezza adottate, il 22 settembre, il Gruppo ha poi effettuato una visita al *data center* dell'Agenzia EU-LISA, all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac. Si è trattato di una visita ricognitiva, coordinata *dai Data Protection Officer* e *Data Security Officer* dell'Agenzia stessa, che ha consentito di avere una chiara visione delle misure di sicurezza fisiche e logiche adotrate. In tale occasione, il Gruppo ha insistito sulla necessità che EU-LISA ponga adeguata attenzione alla materia della protezione dei dati nell'opera di formazione che svolge nei confronti degli utilizzatori del sistema (tra cui, dalla data di entrata in vigore del nuovo regolamento, anche le autorità di *law enforcement*).

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

Il Gruppo di coordinamento della supervisione VIS (che ha eletto come presidente Vanna Palumbo del Garante e come vicepresidente il rappresentanre dell'autorità spagnola, Manuel Garcia) si è riunito due volte ed ha proseguito l'attività avviata nel 2015 volta a verificare il funzionamento del sistema nei diversi Paesi membri. A tal fine, sono state raccolte le risposte ai tre questionari definiti,

definiti nel 2014, volti a chiarire gli assetti nazionali del sistema in relazione all'elenco delle autorità che lo utilizzano; all'accesso al sistema per finalità di *law enforcement* e alle modalità per l'esercizio dei diritti degli interessati. Il Gruppo sta inoltre lavorando sulle forme di esternalizzazione delle procedure di raccolta dei dati nell'ambito degli *iter* amministrativi relativi al rilascio dei visti. Oggetto di valutazione saranno, in particolare, i contratti utilizzati dai Paesi membri per esternalizzare tali attività e la loro conformità rispetto agli *standard* di protezione dei dati.

Alle riunioni, come di consueto, i membri del gruppo si sono incontrati con i rappresentanti della Commissione e l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA) per discutere dello stato di avanzamento del VIS *roll-out*, i previsti ulteriori *roll-out*, i recenti sviluppi relativi alla qualità dei dati nel sistema e il ruolo dei subappaltatori.

Il Gruppo ha poi adottato il programma di lavoro per il periodo del 2015 al 2018 che individua, tra i temi da affrontare, il trasferimento di dati a Paesi terzi o organizzazioni internazionali, la cancellazione anticipata dei dati, la formazione del personale in materia di sicurezza e norme sulla protezione dei dati e l'auto-monitoraggio delle autorità che hanno accesso al VIS.

Il Gruppo ha adottato anche la relazione delle attività svolte nel biennio 2012-2014 che include un capitolo nazionale per ciascuno dei trenta Paesi che utilizzano il VIS, vale a dire tutti gli Stati Schengen, tutti e quattro gli stati membri dell'area europea di libero scambio – Islanda, Liechtenstein, Norvegia e Svizzera e Bulgaria, Croazia, Cipro e Romania, che non sono ancora parte dello spazio Schengen, ma comunque hanno una politica dei visti sulla base di Schengen.

La visita svolta il 22 settembre presso il *data center* di EU-LISA, a Strasburgo, all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac, ha infine consentito al Gruppo di avere un primo quadro sul funzionamento del sistema e sulle misure di sicurezza adottate.

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) – che come di consueto si sono riunite *back to back* due volte l'anno – hanno continuato la propria attività di supervisione del sistema informativo che raccoglie le informazioni volte a prevenire, ricercare e perseguire le operazioni contrarie alle regolamentazioni doganale o agricola (sulla base, rispettivamente, della decisione 2009/917/GAI e della decisione quadro 2008/977/GAI per i trattamenti effettuati per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali e del regolamento (EC) No 515/1997, artt. 23 e ss. relativo alle violazioni di natura amministrativa.

In particolare, l'ACC Dogane ha curato, attraverso le DPA che in essa sono rappresentate, la diffusione del *leaflet* (tradotto nelle diverse lingue dell'Unione) dal titolo "*Guide to your responsabilities under Article 13 of the CIS Decision and art. 8(2) della Data protection framework decision*" (in italiano doc. web n. 4349259) che ha lo scopo di fornire alcune indicazioni in ordine alle modalità che le Autorità competenti per il sistema sono tenute a seguire ove risulti necessario correggere, rettificare o cancellare eventuali informazioni inesatte o inserite nel sistema in violazione di legge. L'Autorità ha poi iniziato a valutare le risposte pervenute dall'Olaf e dalle autorità nazionali al questionario inviato come *follow up* delle raccomandazioni espresse dopo l'ispezione del sistema svoltasi nel 2011.

Nel corso dell'anno il Gruppo di coordinamento della supervisione del SID (che ha eletto come nuovo presidente Piotr Drobek, delegato della DPA polacca e ha esteso il proprio programma di lavoro 2014-2015 fino alla fine del 2016) ha lavorato su un possibile modello comune per le attività ispettive che le DPA, ove neces-

sario, possono porre in essere con riferimento al sistema SID e ha ultimato i lavori per la predisposizione della guida all'esercizio dei diritti di accesso allo stesso (doc. web n. 4810368). La guida fornisce indicazioni precise su come gli interessati possono esercitare i propri diritti nei diversi Stati membri, fornendo anche indicazioni sulle autorità da contattare.

22

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

Consiglio d'Europa – T-PD

Nell'ambito del Consiglio d'Europa il Garante ha proseguito la partecipazione all'attività del T-PD, Comitato consultivo della Convenzione 108/1981, anche nella sua composizione ristretta (T-PD *Bureau*).

Il T-PD ha continuato a seguire il processo di modernizzazione della Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, volto ad adeguarne i princìpi al mutato scenario tecnologico e a garantire la tenuta di un alto livello di protezione dei diritti delle persone (vedi Relazione 2014, p. 183). Tale processo pur avendo portato, già nel dicembre 2014, all'adozione – da parte del comitato intergovernativo *ad hoc* CAHDATA – della Convenzione modernizzata (fondata sul testo adottato dal T-PD nella plenaria del 18 dicembre 2012, vedi Relazione 2012, p. 298), non si è ancora concluso. Il protocollo emendativo della Convenzione 108 predisposto dal segretariato del Consiglio d'Europa sulla base del documento adottato dal CAHDATA non è stato infatti ancora adottato dal Comitato dei ministri, in ragione delle persistenti riserve, tra cui quelle della Commissione europea su alcuni articoli corrispondenti a nodi non ancora sciolti dal nuovo regolamento UE.

Il T-PD ha inoltre continuato a lavorare alla predisposizione del *memorandum* esplicativo della Convenzione 108 in modo da allinearlo alle diverse novità inserite nella Convenzione modernizzata.

Nell'ambito delle attività del T-PD è inoltre proseguito il lavoro di attualizzazione dei princìpi di protezione dei dati in ambito sanitario in particolare con riferimento all'impiego di nuove tecnologie nel settore medico (fascicoli sanitari elettronici, *app* mediche, RFID, tecniche di profilazione, ecc.) che ha portato all'elaborazione di un progetto di revisione della raccomandazione (97)5 sul trattamento dei dati sanitari.

Il Comitato ha inoltre approfondito il tema *big data*, con la predisposizione di una bozza di linee guida volte ad esaminare le diverse problematiche emerse in tale settore e a declinare i princìpi di protezione dei dati.

Una prima bozza di parere sul tema delle informazioni relative ai passeggeri aerei è stata inoltre discussa dal Comitato in vista di una sua possibile adozione nel corso del 2016.

Altri temi che sono stati all'attenzione del T-PD riguardano le implicazioni sulla protezione dei dati provenienti dagli scambi automatizzati di dati tra Stati in relazione alla lotta all'evasione fiscale, al riciclaggio, al finanziamento del terrorismo e alla corruzione, ai profili di *privacy* nell'ambito delle politiche di ICANN, e al trattamento dei dati in ambito di polizia, che sarà oggetto di ulteriori approfondimenti in vista dell'elaborazione di una guida pratica per gli operatori del settore.

Il Comitato dei ministri del Consiglio d'Europa, nella riunione del 1° aprile ha adottato la raccomandazione (2015)5 sulla protezione dei dato in ambito lavorativo che ha così completato il lavoro del T-PD che aveva approvato il testo nella plenaria di giugno del 2014 (v. Relazione 2014, p. 183). La nuova raccomanda-

22

OCSE

zione sostituisce la raccomandazione (89)2, ampliandone i princìpi e declinandoli alla luce delle nuove tecnologie in uso nel mondo del lavoro, in particolare con riferimento all'impiego di *e-mail* e internet da parte del dipendente, al controllo a distanza del lavoratore, al trattamento di dati biometrici e genetici (doc. web n. 4814881).

L'Autorità ha continuato a partecipare ai lavori del SPDE (*Working Party on Security and Privacy in Digital Economy Working Party on Information Security and Privacy*) dell'OCSE. Nel 2015 il Garante, già membro del Gruppo e componente del *Bureau* dello stesso, è stato riconfermato nel *Bureau* del SPDE anche per il 2016.

Gran parte del lavoro del Gruppo è stato dedicato alla preparazione della Ministeriale 2016 che l'OCSE terrà a Cancun (Messico) il 21-23 giugno 2016. Il tema della Ministeriale è la "*Digital Economy:* Innovazione, Crescita e sociale Prosperità" e se ne discuterà in quattro sezioni, con due sezioni plenarie di apertura e chiusura. La responsabilità principale per lo SPDE è l'organizzazione del *panel* dal titolo "*Public/Private Cooperation in Managing Digital Security and Privacy Risk for Economic and Social Prosperity*". Nel corso dell'anno il Gruppo si è perranto concentrato sul tema centrale di tale sessione, ossia la protezione dati in ambito digitale con riferimento ad "un approccio basato sul rischio" (cd. *risk based approach*, come previsto anche dal regolamento europeo sulla protezione dei dati la cui pubblicazione è prevista sulla GUUE del 4 maggio 2016; v. par. 22.1). Lo SPDE ha inoltre contribuito alla preparazione di altri *Panel* della Ministeriale, in particolare delle sessioni dedicate rispettivamente ai vantaggi economici e sociali di un *Open Internet* e alla *Internet delle cose* (*IoT*).

Gli esiti della Ministeriale confluiranno in una dichiarazione ministeriale che potrebbe approvare il lavoro che l'OCSE effettua per sostenere lo sviluppo dell'economia digitale e fornire indicazioni per il lavoro futuro, anche da parte dello SPDE. Il Gruppo si è impegnato nella redazione della bozza di Dichiarazione che nella sua ultima versione di dicembre 2015 appare semplificata rispetto alla precedenti versioni. La bozza, in corso di aggiornamento, riconosce il valore e, allo stesso tempo, la pervasività delle tecnologie digitali e auspica un approccio il più possibile fondato sulla cooperazione e sull'inclusione dei diversi attori in gioco, al fine di cogliere appieno i benefici dell'economia digitale e facilitare l'adozione di standard tecnici comuni, nel rispetto della protezione dei dati personali.

Oltre al tema della Ministeriale, lo SPDE nel corso del 2015 ha anche ultimato il lavoro di revisione della raccomandazione sulla Sicurezza del 2002 (*Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security:* "OECD *Security Guidelines*"). Tale lavoro ha portato, nel mese di settembre, all'adozione della nuova raccomandazione sulla sicurezza digitale (*Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, doc. web n. 4295203). Nel documento l'OCSE sostiene che il rischio per la sicurezza digitale dovrebbe essere considerato un problema di ordine economico e non solo tecnologico, e dovrebbe essere integrato nei processi decisionali di ogni organizzazione. Il lavoro del Gruppo ha fatto emergere come un ambiente digitale globale, interconnesso, aperto e dinamico generi notevoli opportunità economiche, ancora più promettenti se si pensa alla crescente diffusione dell'internet delle cose e dei *big data*. Tuttavia, Paesi e aziende sono esposti a minacce sempre più sofisticate e crescenti che possono mettere in pericolo la sicurezza delle informazioni e compromettere la prosperità economica e sociale. La raccomandazione dell'OCSE sulla *digital security* chiede quindi a governi e vertici aziendali di assumersi la specifica responsabilità della gestione del rischio della sicurezza digitale integrandola nella pianificazione generale. L'OCSE indica otto princìpi-guida per la gestione del rischio riferito alla sicurezza

digitale, anche con riguardo alla responsabilità dei diversi soggetti, alla cooperazione tra le parti interessate e al ruolo dell'innovazione. In particolare, si raccomanda l'adozione di piani nazionali per individuare le misure utili a prevenire, affrontare e sanare le conseguenze di incidenti di sicurezza digitale. La raccomandazione rappresenta una solida base per attuare anche molti dei princìpi contenuti nelle *Privacy Guidelines* dell'OCSE (v. Relazione 2014, p. 185) e i due strumenti si integrano perfettamente. Il Gruppo di lavoro si è quindi adoperato negli ultimi mesi dell'anno nella promozione della Raccomandazione attraverso la massima divulgazione del testo.

Tra gli altri temi, si segnala infine il lavoro dell'OCSE sulla protezione e sicurezza dei dati in ambito sanitario portato avanti dallo SPDE e dal neoistituito *Oecd Advisory Expert Group*, il Gruppo consultivo di esperti per guidare lo sviluppo della proposta di Raccomandazione sull'uso dei dati sanitari (*Draft Council Recommendation on privacy protective approaches for the use of personal health data*). Nel mese di novembre si è tenuto il primo incontro della *task force*. All'incontro hanno partecipato trenta esperti (tra cui due esperti del Garante) di almeno undici Paesi e sono emerse significative differenze nei sistemi di cura della salute e nell'uso delle terminologie del settore. Oggetto dell'incontro è la stata la bozza della citata raccomandazione. Dal testo (in corso di aggiornamento) emerge come la raccomandazione miri alla ricerca di un sistema sanitario migliore e più efficiente nei Paesi OCSE, fornendo Linee guida ai decisori dei diversi Paesi nello sviluppo di *framework* di *governance* o di riforme in materia di *governance* dei dati sanitari laddove trattati per la salute pubblica, scopi scientifici e di ricerca, per statistiche del sistema sanitario e per migliorare la gestione e la fornitura di servizi di assistenza sanitaria. Il documento si basa sui princìpi enunciati nelle *Privacy Guidelines* dell'OCSE, in particolare, su specifiche previsioni in esse contenute in relazione al trattamento dei dati sanitari (dati sensibili).

Progetto *Big Data Ethical Assessment Process*

Nel 2015 il Garante ha altresì partecipato al *workshop Big Data Ethical Assessment Process*, progetto *multi-stakeholder* organizzato dall'*Accountability Foundation*, volto a indirizzare i diversi titolari del trattamento (soggetti privati) che gestiscono *big data* verso un orientamento etico e responsabile.

Nel corso dell'anno si sono tenuti due incontri, rispettivamente a Madrid il 29 aprile presso l'Autorità spagnola e a Roma presso il Garante il 14 luglio. Si è discusso dei possibili strumenti da approntare al fine di assicurare un quadro di princìpi etici nella gestione dei *big data* come sfida globale per i diritti umani, inclusi il diritto alla protezione dei dati e *privacy*.

Mentre la prima riunione si è concentrata sulla possibilità di realizzare un codice etico vincolante per *big data*, prevedendo specifiche competenze in capo alle Autorità di regolamentazione per rendere applicabile tale codice di condotta anche a livello nazionale, nel secondo incontro si è proposto di focalizzare l'attenzione su una lista di raccomandazioni relative alla dimensione etica del trattamento dei dati nel contesto *big data*. In tale ambito, sono state affrontate diverse tematiche, tra cui i poteri di *enforcement* delle autorità di protezione dati e la loro effettività, l'anonimizzazione e la minimizzazione dei dati, le garanzie per assicurare un'effettiva cancellazione dei dati, la dimensione pubblica del *big data* (per la ricerca) e la promozione di una *governance* responsabile da parte delle aziende anche attraverso *standard* internazionali.

IWGDPT

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication* (IWGDPT, cd. Gruppo di Berlino) che nel corso del 2015 si è riunito a Seul il 27-28 aprile e a Berlino il 14 e 15 ottobre.

Nella prima riunione il Gruppo ha lavorato sul tema della *accountability* delle imprese in caso di accesso da parte di autorità pubbliche ai dati personali in loro possesso. Il Gruppo si è soffermato in particolare sul cd. *transparency reporting*, consistente nella pubblicazione periodica, da parte di alcune società di statistiche e

caratteristiche dei dati personali trasmessi, per finalità diverse da quelle commerciali, a terze parti, in particolare alle autorità di polizia. Con l'adozione di uno specifico documento di lavoro su tale argomento, il Gruppo ha richiamato l'attenzione sui princìpi di protezione dei dati cui tale attività deve ispirarsi ed ha fornito raccomandazioni per la loro attuazione ai diversi attori coinvolti (imprese, legislatori, autorità pubbliche che richiedono l'accesso, autorità di protezione dei dati, organizzazioni internazionali e società civile) (doc. web n. 4814944).

È stato inoltre adottato un documento di lavoro sui cd. *wearable computing devices*, dispositivi digitali indossabili che, dotati di specifici sensori, permettono la raccolta in tempo reale di dati personali (doc. web n. 4814934). Anche questo documento fornisce una serie di raccomandazioni volte a garantire il rispetto dei princìpi *privacy* nel settore, affinché sia assicurato il controllo da parte dell'interessato dei dati che lo riguardano, la trasparenza dei trattamenti effettuati (dei quali spesso – per le caratteristiche dei dispositivi stessi – l'interessato è poco consapevole), l'agevole esercizio dei diritti, e la portabilità dei dati. Particolare attenzione è dedicata al trattamento di dati sensibili, che deve essere subordinato alla prestazione del consenso esplicito dell'interessato, e all'impiego di tali dispositivi in ambito lavorativo perché sia adeguatamente tutelata la libertà di scelta del lavoratore.

Con un documento di lavoro adottato nella riunione di Berlino, il Gruppo è tornato ad occuparsi del tema della localizzazione derivante dall'impiego di dispositivi mobili (doc. web n. 4814975). Specifiche raccomandazioni mirano ad assicurare che tali trattamenti avvengano nella piena consapevolezza degli interessati, siano proporzionati alla legittima finalità perseguita, i dati siano anonimizzati non appena raggiunto lo scopo, la combinazione dei dati con altre informazioni e la comunicazione a terzi avvengano con il consenso dell'interessato e siano garantiti agli interessati idonei strumenti per esercitare il controllo sui propri dati.

Nella stessa riunione il Gruppo ha anche trattato il tema delle tecniche di *intelligent video analytics* (ad es., videosorveglianza intelligente), che consentono l'osservazione di comportamenti e caratteristiche degli individui per diverse finalità, tra cui la personalizzazione di comunicazioni commerciali e di prezzi di prodotti o servizi, la rilevazione di comportamenti anomali a fini di sicurezza e l'ottimizzazione di servizi (doc. web n. 4814956). Tali tecniche, pur perseguendo finalità legittime, devono essere congegnate e utilizzate tenendo conto del loro impatto su *privacy* e protezione dei dati personali, anche per evitare un effetto frenante sull'esercizio di alcuni diritti e libertà fondamentali, quali la libertà di espressione o di assemblea.

Tra gli altri temi trattati dal Gruppo nel corso dell'anno, anche in vista di futuri approfondimenti, si segnalano infine: il ricorso a strumenti di *e-learning* da parte dei sistemi scolastici nazionali, mediante specifiche applicazioni per terminali mobili (*tablet*), che utilizzano tecniche di identificazione dei terminali (e indirettamente degli utenti) basate sull'uso di *cookies*; nuove forme di autenticazione sul web, in particolare sulla base di tecniche di riconoscimento biometrico, non più dunque basate sull'uso di *password* e di facile impiego per gli utenti con l'obiettivo di incrementare la sicurezza; il tema del cd. *delisting* dai risultati offerti da un motore di ricerca; gli aspetti di *privacy* e sicurezza connessi all'uso di servizi VoIP; gli sviluppi in materia di standardizzazione con particolare riferimento alle modalità *user friendly* per l'acquisizione del consenso e sulla de-identificazione; le problematiche *privacy* nei *social networks*.

Cooperazione internazionale IECWG, GPEN, PHAEDRA *project*

Nel 2015 è proseguita l'attività dei Gruppi di lavoro dedicati al coordinamento delle attività internazionali di *enforcement*, come richiesto dalla 36ª Conferenza internazionale delle autorità di protezione dati (v. Relazione 2014, p. 187) e dal lavoro del Gruppo di coordinamento delle attività internazionali di *enforcement* (IECWG).

In tale contesto, si è intensificata l'attività del *Global Privacy Enforcement Network*-GPEN, la prima rete internazionale di cooperazione transfrontaliera in tema di *enforcement* lanciata nel 2010 (v. par. 22.2). Su *input* del GPEN, il Garante (membro del Gruppo) ha svolto il 12 maggio lo *Sweep* 2015 dedicato alla protezione in rete dei minori tra gli 8 e i 13 anni. Sono stati analizzati decine di siti internet tra i più visitati da bambini e alcune delle più diffuse *app* per minori (fino a 13 anni) scaricabili su *smartphone* e *tablet*. I risultati dell'indagine svolta hanno mostrato che le *app* e i siti internet più utilizzati dai bambini italiani non tutelano adeguatamente la *privacy* dei piccoli utenti. Nello specifico, gli esperti del Garante hanno selezionato 22 *app* e 13 siti internet (appartenenti al settore *educational*, al mondo dei giochi, a servizi *online* offerti da canali televisivi per l'infanzia, ai *social network*) tra i più popolari tra i bambini, o appositamente sviluppati per loro, e ne hanno analizzato le caratteristiche. Tra i 35 casi analizzati dagli *sweepers* del Garante ben 21 hanno evidenziato gravi profili di rischio e 8 di questi richiederanno specifiche attività ispettive. È emerso un panorama critico, in linea con le problematiche riscontrate anche dalle altre Autorità internazionali. I risultati evidenziano una grave disattenzione nei confronti dei più piccoli, poca trasparenza in merito alla raccolta, all'utilizzo dei dati personali e alle autorizzazioni richieste per scaricare le *app* su *smartphone* e *tablet*, presenza di pubblicità e rischi che i bambini vengano reindirizzati verso siti non controllati (doc. web n. 4234002).

XXVII *Case Handling workshop*

Si è tenuto a Tirana, il 28 e 29 settembre, il 27° *Case Handling workshop*, l'incontro annuale nel corso del quale le autorità si confrontano sui casi pratici affrontati a livello nazionale. Diversi i temi approfonditi nel *workshop* di quest'anno, in particolare l'utilizzo dei droni e altre forme "intelligenti" di videosorveglianza, il *credit reporting*, il trattamento dei dati del sistema bancario e la profilazione. L'incontro è stato anche occasione di scambio con riferimento alle modalità di gestione di ricorsi e reclami, e alle attività di cooperazione tra diverse autorità, come quella intercorsa tra il Garante e l'autorità albanese in mareria di trattamento dei dati da parte dei *call center* (v. *infra*).

Incontri con le delegazioni estere e organizzazioni internazionali

L'Autorità ha continuato a partecipare a programmi di partenariato europeo negli ambiti di competenza, offrendo la propria esperienza per facilitare l'avvicinamento delle normative dei Paesi coinvolti al quadro comunitario in materia di protezione dei dati. Nel mese di febbraio si è tenuta la visita, presso il Garante, di una delegazione dell'Autorità per la protezione dei dati albanese. Durante la visita – che ha permesso l'approfondimento di diversi temi tra cui la possibilità di ispezioni congiunte tra il Garante italiano e quello albanese con riferimento ai *call center* – è stato firmato l'Accordo di cooperazione tra le due autorità.

Nell'ambito del Progetto TAIEX della Commissione europea, si è tenuto il 31 marzo, a Podgorica, un *workshop* in tema di protezione dei dati nel contesto della videosorveglianza, cui il Garante ha partecipato, che aveva lo scopo di richiamare l'attenzione delle autorità pubbliche montenegrine sul tema.

23 L'attività di comunicazione, informazione e di rapporto con il pubblico

23.1. *La comunicazione del Garante: profili generali*

Il Garante ha da sempre considerato l'attività di informazione e comunicazione istituzionale fondamentale per la diffusione di una cultura della protezione dei dati nel nostro Paese. In quest'ottica già da qualche anno l'Autorità ha rafforzato la sua azione anche nei canali *social*, puntando anche alla produzione multimediale destinata al web.

Uno dei grandi temi che nel corso del 2015 l'Autorità si è trovata nuovamente ad affrontare è stato quello del rapporto tra sicurezza *e privacy*, con particolare riferimento alle problematiche legate alle intercettazioni, alla conservazione dei dati di traffico sia telefonico che telematico, al tracciamento dei passeggeri dei voli, alla sorveglianza di massa, anche alla luce degli attacchi terroristici che si sono succeduti in ogni parte del mondo, giungendo fin nel cuore dell'Europa. Proprio il bisogno di sicurezza ed il ricorso all'uso di avanzate tecnologie per il controllo di massa rischiano di compromettere i modelli di protezione dei dati personali e le libertà fondamentali delle società democratiche. Su tali delicate questioni il Garante è più volte intervenuto sottolineando la necessità di assicurare un bilanciamento tra i menzionati diritti tra loro in tensione.

Riguardo, in particolare, alla lotta al terrorismo l'Autorità ha affermato che occorre mettere in campo una raccolta selettiva e non generalizzata delle informazioni in quanto l'enorme accumulazione di informazioni fin qui realizzata in grandi banche dati pubbliche e private non sufficientemente protette rischiano di allargare a dismisura la superficie di attacco del terrorismo. La minaccia più grave oggi è rappresentata dal *cybercrime* e diventa dunque primaria la necessità che le grandi infrastrutture strategiche del nostro Paese vengano protette in maniera efficace è indispensabile.

In relazione allo sviluppo di una forte consapevolezza del valore dei dati personali e dell'importanza di una loro tutela soprattutto nel mondo *online*, il Garante ha concentrato il suo impegno su alcune grandi problematiche: i *social network* e i pericoli derivanti dalla diffamazione in rete: *l'hate speech* e il *cyberbullismo*; il diritto all'oblio, il *cybercrime* ed il furto d'identità; l'interner delle cose (Iot). Proprio quest'ultimo tema è stato al centro dei lavori del convegno "Il pianeta connesso. La nuova dimensione della *privacy*", organizzato dal Garante in occasione della celebrazione della Giornata europea della protezione dei dati personali.

Altre questioni di particolare rilievo sociale trattate nel periodo di riferimento sono state la trasparenza della p.a. *online* e le garanzie da assicurare ai cittadini, il fisco e la tutela delle riservatezza dei contribuenti, l'uso delle nuove tecnologie sul posto di lavoro, il *telemarketing* selvaggio, i diritti dei consumatori, la scuola, i partiti e i movimenti politici, la dichiarazione di volontà per la donazione degli organi sui documenti di identità. Anche il settore della sanità ha rappresentato un altro ambito sul quale si è concentrato l'impegno dell'Autorità, a partire dal fascicolo e dal *dossier* sanitario elettronico sino alle tutele da riservare agli assistiti riguardo alla sicurezza dei loro dati personali.

È stata condotta dall'Autorità italiana, in collaborazione con altre ventisette autorità internazionali facenti parte del *Global Privacy Enforcement Network* (GPEN) una speciale indagine sulla *privacy* dei bambini e, in occasione del "*Privacy Sweep* 2015" dedicato alla protezione in rete dei bambini tra gli 8 e i 13 anni, ne sono stati resi noti gli esiti principali. I risultati dell'indagine hanno evidenziato che le *app* e i siti internet più utilizzati dai bambini italiani non tutelano a dovere la *privacy* dei piccoli utenti (in merito v. *amplius* par. 22.5).

Riguardo al preoccupante fenomeno del *cyberbullismo* e sulle azioni da mettere in campo per contrastarlo, il Garante ha dato il proprio contributo al Miur per l'elaborazione delle "Linee di orientamento per azioni di prevenzione e contrasto al *cyberbullismo*" presentate dal Ministro nel mese di aprile e trasmesse a tutte le scuole italiane.

L'Autorità ha inoltre fornito indicazioni per l'elaborazione di un sito informativo "Vivere in un mondo connesso" (www.mondoconnesso.info), realizzato da Facebook e lanciato anche in Germania, Austria e Francia, dedicato alla tutela dei dati personali su internet e nella vita quotidiana. Il sito, corredato anche di uno strumento di autovalutazione delle competenze in materia di *privacy online* sviluppato da Unione nazionale consumatori, consente di raggiungere in maniera diretta gli utenti dei *social network* affinché prestino maggiore attenzione alla tutela della *privacy* in rete.

I *media* hanno mantenuto una costante attenzione alle tematiche riguardanti la protezione dei dati personali e all'attività del Garante. Nel 2015 il Servizio relazioni esterne e *media* ha selezionato circa 57.200 articoli di interesse per l'Autorità. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali, delle testate *online* e *blog* che hanno trattato i temi legati alla *privacy* sono stare 14.685, delle quali 4.293 dedicate esclusivamente all'attività del Garante. Le prime pagine sono state oltre 980, di cui 212 riguardanti la sola Autorità. Le interviste, gli interventi e le dichiarazioni del presidente e dei componenti pubblicate sulla carta stampata sono state complessivamente 251, 343 quelle *online* e 34 quelle andate in onda su tv e radio nazionali e locali. Le citazioni relative al tema della *privacy* e all'attività del Garante in programmi televisivi e radiofonici nazionali sono state oltre 200.

23.2. *I prodotti informativi*

Nel 2015 sono stati diffusi 34 comunicati stampa e 13 *newsletter*, pubblicazione periodica giunta al suo XVII anno di diffusione (per un totale di 410 numeri e di 1.411 notizie), che consente un'approfondita divulgazione dei più importanti provvedimenti adottati dall'Autorità, della sua attività in ambito europeo ed internazionale e delle molteplici iniziative promosse. Le notizie pubblicate vengono redatte a cura del Servizio relazioni esterne e *media*, composte graficamente e completate con l'aggiunta di immagini per la versione web. La *newsletter* – che conta nella lista di distribuzione circa 8.000 destinatari – viene inviata via *e-mail* a redazioni, professionisti, operatori delle pp.aa., imprese e singoli cittadini che ne fanno richiesta. Sul sito del Garante è attiva l'opzione "Iscriviti alla *newsletter*" (a disposizione di tutti i visitatori, allo scopo di favorire una più ampia utilizzazione di questo importante strumento di informazione). È poi possibile consultare l'archivio tematico completo della *newsletter* che raccoglie tutti gli articoli finora pubblicati (cfr. sez. IV, tab. 2).

23.3. *I prodotti editoriali e multimediali*

Nuovi prodotti editoriali e multimediali si sono aggiunti alla già ricca collezione dell'Autorità.

Nell'ambito della Collana editoriale del Garante, "Contributi", è stato pubblicato il volume "Il pianeta connesso. La nuova dimensione della *privacy*" che raccoglie i contributi degli studiosi e degli esperti intervenuti al convegno organizzato dall'Autorità in occasione della celebrazione della Giornata europea della protezione dei dati personali 2015. Il Servizio ha curato l'*editing* dei testi ed il progetto grafico oltre che l'ideazione e la realizzazione della copertina.

È stata altresì curata l'edizione del nuovo volume cartaceo del Codice *privacy*, aggiornato alle più recenti innovazioni legislative.

È stato avviato il lavoro sulla nuova edizione aggiornata del *vademecum* dedicato alla tutela della *privacy* nella scuola per offrire indicazioni generali, tratte da provvedimenti, pareri e note del Garante riguardanti il delicato rapporto tra studenti, professori e famiglie, anche alla luce della nuova dimensione digitale.

Un altro apprezzato prodotto è stato il *vademecum* "*Privacy* e lavoro", con le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati soprattutto con riferimento ai cartellini identificativi, bacheche aziendali, posta elettronica aziendale, controllo a distanza e geolocalizzazione dei lavoratori. La pubblicazione è stata realizzata nella sola versione digitale (a disposizione degli utenti sul sito istituzionale) ed è in programma una edizione aggiornata alla nuove regole introdotte dal *Jobs Act*.

Con un bassissimo costo in termini economici e utilizzando esclusivamente risorse interne, si è riusciti anche quest'anno a realizzare prodotti multimediali (provvedendo autonomamente alla scrittura e adattamento dei testi, sceneggiatura, sviluppo dell'animazione e selezione/costruzione degli elementi visivi, scelta delle musiche e sincronizzazione, registrazione dei testi, adattamento audio, montaggio e postproduzione). Sono state inoltre predisposte e diffuse nuove schede informative su varie tematiche, nuove pagine web e video.

La pagina dei "Consigli *flash*" si è arricchita di una nuova scheda su come tutelare la *privacy* con buone *password* (doc. web n. 4248578). Le schede *flash*, offrono spunti e orientamenti di base per tutelare i propri dati nella vita di tutti i giorni, con particolare attenzione all'uso delle nuove tecnologie. I suggerimenti proposti dalle schede invitano a riflettere su abitudini e comportamenti di cui ognuno di noi può fare tesoro per difendere la propria riservatezza.

È stata ideata e prodotta una campagna informativa dedicata alle *app* per *smartphone* e *tablet* intitolata "*App*-prova di *privacy*" corredata anche da un video *tutorial* divulgativo, ovvero un filmato di animazione che illustra le principali cautele da seguire quando si utilizzano applicazioni per *device* mobili e si vuole tutelare efficacemente la propria riservatezza. La campagna è stata integrata da azioni di comunicazione virale che hanno riscosso un deciso successo sui *social media*.

L'uso innovativo di tecniche di comunicazione virale è servito anche a riproporre, secondo il principio della "coda lunga", i numerosi materiali informativi e di comunicazione prodotti dal Garante nel corso del tempo. In particolare, sfruttando i canali *social*, sono stati ideari e diffusi *banner* grafici con immagini e *claim* che hanno permesso di riproporre e implementare l'attenzione e l'interesse per specifici contenuti nel corso del tempo, moltiplicando esponenzialmente la visibilità e il pubblico.

È stato progettato e lanciato il nuovo profilo del Gatante su Google+ (https://plus.google.com/u/1/+GarantedatipersonaliGP), che arricchisce la presenza *online* dell'Autorità, affiancandosi e integrandosi agli spazi di informazione e intera-