di *marketing*. L'Autorità ha adottato un'ordinanza ingiunzione, ritenendo sussistente una violazione del consenso richiesto dall'art. 130, comma 2, del Codice (provv. 7 novembre 2013, n. 502, doc. web n. 2954163).

- Non applicabilità dei termini di cui alla l. n. 241/1990 ai procedimenti sanzionatori: in una ordinanza è stato ribadito che i termini indicati dalla l. n. 241/1990 non si applicano ai procedimenti sanzionatori che sono, invece, regolati dalla l. n. 689/1981. Il particolare procedimento sanzionatorio, che si conclude con l'adozione dell'ordinanza ingiunzione, prevede infatti il compimento di alcune attività necessarie, poste a garanzia degli interessati, e ne fissa le varie fasi con precise scansioni temporali, che sono incompatibili con quelle indicate nella l. n. 241/1990. Tale interpretazione è supportata dalla sentenza 27 aprile 2006, n. 9591 della Corte di cassazione civile S.U., a cui si è conformato recentemente anche il Tribunale di Milano con la sentenza 23 dicembre 2013, n. 27176/2013 (provv. 4 luglio 2013, n. 340, doc. web n. 2954141).
- Attivazione multipla di schede telefoniche: l'Autorità ha adottato numerosi provvedimenti sanzionatori in materia di attivazione multipla di schede telefoniche all'insaputa degli interessati da parte di rivenditori autorizzati (*dealer*). In particolare, poiché in numerosi casi, nell'ambito di indagini di polizia giudiziaria, era stata accertata l'assoluta inconsapevolezza dell'avvenuta attivazione in capo a coloro che ne risultavano intestatari, è stata contestata ai *dealer* che si erano resi responsabili degli illeciti la violazione dell'obbligo di informativa previsto dall'art. 161 del Codice. Nelle ordinanze adottate il Garante ha ritenuto non applicabile l'istituto del "cumulo giuridico" di cui all'art. 8 della l. n. 689/1981 – concernente il caso di chi "con un'azione od omissione viola diverse disposizioni che prevedono sanzioni amministrative o commette più violazioni della stessa disposizione" – trattandosi di azioni poste in essere dai *dealer* nei confronti di soggetti diversi e da ritenersi quindi distinte e indipendenti l'una dall'altra (provv. 18 aprile 2013, n. 204, doc. web n. 2691090).
- Inutilizzabilità dei dati tratti da liste elettorali per finalità di *marketing* in due ordinanze il Garante ha affrontato la questione della utilizzabilità, ai suddetti fini, dei dati tratti da liste elettorali acquisite prima dell'entrata in vigore del Codice (poiché con l'introduzione della nuova disciplina, vigente dal 1° gennaio 2004, l'acquisizione delle liste elettorali è consentita ai soli soggetti che utilizzino i dati per le finalità previste dall'art. 177, comma 5, fra le quali quelle connesse all'esercizio dell'elettorato attivo e passivo, al perseguimento di un interesse collettivo diffuso, alla ricerca e quelle socio-assistenziali). Nei casi portati all'attenzione dell'Autorità, due società nazionali operanti nel settore della fornitura di servizi per il *marketing*, utilizzavano dati tratti da liste elettorali, acquisite prima dell'entrata in vigore del Codice, per l'invio di comunicazioni promozionali da parte di terzi. Il Garante, nelle due ordinanze, ha confermato quanto già stabilito nel provvedimento del 10 giugno 2004 (doc. web n. 1068106), specificando che "sulla base della vigente normativa non vi è alcuna possibilità di utilizzare, per finalità di *marketing*, dati personali tratti da liste elettorali (a prescindere dall'epoca della raccolta) a meno che il titolare non dimostri di aver fornito agli interessati, in caso di acquisizione '*ante* 2004', un'idonea informativa nella quale sia reso esplicito l'utilizzo dei dati per la predetta finalità di *marketing* e di aver poi acquisito un consenso specifico per tale finalità". Il Garante ha inoltre chiarito che "le liste elettorali, sulla base della citata nor-

mativa, possono legittimamente essere acquisite solamente dai soggetti che annoverino fra le proprie finalità quelle previste dal citato art. 177, comma 5 del Codice" e non anche da imprese commerciali che si pongano quali intermediari fra i comuni che rilasciano le liste e gli enti *no-profit* che le utilizzano (provv.ti 10 gennaio 2013, n. 6, doc. web n. 2438949 e n. 549, doc. web n. 2954335).

L'ammontare dei pagamenti effettuati nell'anno 2013 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 4.081.760 euro di cui:

- 2.359.868 euro, pagati a titolo di definizione in via breve (entro 60 giorni dalla notifica della contestazione senza l'invio di scritti difensivi all'Autorità);
- 1.601.892 euro, a seguito di ordinanze-ingiunzione adottate dal Garante in tutti i casi in cui la parte non si è avvalsa della facoltà di definizione in via breve di cui al punto precedente;
- 120.000 euro, per la definizione in sede amministrativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza.

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo, sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e utilizzabili unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

18.6. *Le sanzioni nella proposta di regolamento europeo*

La revisione del quadro normativo comunitario in materia di protezione dei dati personali in corso a Bruxelles (e di cui si da conto nel par. 19.1) riguarderà tutta la disciplina, ivi compresi gli aspetti sanzionatori. A questo proposito, il testo dello schema di regolamento in discussione è molto più puntuale della direttiva 95/46/CE prevedendo, agli artt. 78 e 79, i criteri ai quali i legislatori degli Stati membri dovranno attenersi nella definizione del nuovo apparato sanzionatorio.

Ancorché questa parte della proposta di regolamento abbia formato oggetto di ampie discussioni nell'*iter* di approvazione sin qui percorso, si possono tuttavia trarre alcuni indici di massima che potrebbero caratterizzare il nuovo sistema sanzionatorio europeo:

- sanzioni amministrative applicate dalle autorità nazionali basate su pene pecuniarie capaci di esprimere una forte capacità dissuasiva anche per soggetti di grandi dimensioni, parametrate in percentuale al fatturato (con un limite massimo definito, nell'ultima versione, in 100.000.000 euro nel 5% del fatturato mondiale annuo);
- esimente per le violazioni non intenzionali commesse per la prima volta con invio di un ammonimento scritto;
- definizione di specifici criteri di quantificazione delle sanzioni in rapporto: alla gravità della violazione; alla natura dei dati; alla durata e all'intenzionalità o colposità della violazione; ai precedenti; alla recidività; al ravvedimento del contravventore; al nocumento causato o al fine di lucro sotteso alla violazione.

Il regolamento europeo, pur indicando ai legislatori nazionali la necessità di prevedere sanzioni amministrative efficaci, proporzionate e dissuasive, non fa nessun riferimento (come già la direttiva 95/46/CE) a possibili sanzioni di natura penale;

la loro eventuale previsione rientra nella auronomia riconosciuta a ciascuno Stato membro, che vi potrà provvedere ispirandosi a criteri di effettività, proporzionalità, capacità dissuasiva e omogeneità delle sanzioni rispetto all'apparato sanzionatorio interno e a quello degli altri Stati membri; ciò secondo un principio ormai consolidato, affermato dalla Corte di giustizia dell'Unione europea (cfr. sentenza del 21 settembre 1989, causa n. 68/88, Commissione c. Repubblica ellenica, in Racc. giur, C. giust., 1989-8, p. 2965).

In Italia, come noto, il sistema sanzionatorio in materia di protezione dei dati personali, originariamente sbilanciato a favore della sanzione penale, è stato successivamente corretto (in particolare con le modifiche intervenute con il d.l. 30 dicembre 2008, n. 207, convertito nella l. 27 febbraio 2009, n. 41) aumentando il peso delle sanzioni amministrative (ed enfatizzando così il ruolo di *enforcement* dell'Autorità chiamata ad applicarle).

Ferma restando quindi l'auronomia circa la (teorica) possibilità di sanzionare, anche penalmente, alcune (gravi) violazioni della nuova disciplina europea, appare quanto mai necessario verificare, per non eludere il primario obiettivo di armonizzazione proprio della nuova base giuridica in corso di definizione a livello comunitario, la reale necessità della conferma di tutte le (o parte delle) disposizioni che oggi prefigurano responsabilità penali conseguenti a inosservanze della disciplina, tenendo anche in considerazione gli orientamenti degli altri Paesi nella maggioranza dei quali non sono previste sanzioni penali.

Tenuto conto di queste linee generali di prospettiva e della ormai consolidata esperienza maturata sul campo dall'Autorità in questi anni, sono state definite alcune proposte di modifica all'attuale apparato sanzionatorio previsto dal Codice (e che esplicherà i propri effetti fino all'entrata in vigore del nuovo regolamento europeo che appare difficile prevedere prima di almeno tre anni) che il Garante intende proporre al legislatore e di cui si fa cenno nel prossimo paragrafo.

18.7. *Le proposte del Garante per una revisione dell'apparato sanzionatorio del Codice e l'attualizzazione delle misure minime di sicurezza contenute nell'Allegato B al Codice*

Nell'anno 2013 il Garante ha suggerito alcune modifiche (cfr. segnalazione al Parlamento del 5 luglio 2013, doc. web n. 2521783; v. *amplius* par. 2.1.1 n. 11), inizialmente inserite nel testo del disegno di legge denominato "Misure di semplificazione degli adempimenti per i cittadini e le imprese e di riordino", approvato il 21 giugno 2013 dal Consiglio dei Ministri, che si prefiggevano di apportare alcune correzioni all'attuale apparato sanzionatorio, in continuità con le tendenze generali (cui si è fatto cenno al paragrafo precedente), con l'intento tra l'altro di:

- attenuare l'impatto economico diretto e indiretto delle sanzioni mediante accesso a formule di estinzione particolarmente favorevoli (pagando direttamente il minimo della sanzione) quando la violazione è commessa per la prima volta da soggetti che rientrano nella definizione di piccola e media impresa o da enti pubblici di piccole dimensioni (es. piccoli comuni);
- eliminare l'attuale duplicazione di sanzione (amministrativa e penale) in caso di violazione colposa delle misure minime di sicurezza, limitando la violazione penale solo al caso in cui, a causa dell'inadeguatezza delle misure di sicurezza adottate, si verifichi "la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati", abrogando contestualmente la procedura del cd. ravvedimento operoso attualmente prevista dall'art. 169, comma 2, del Codice.

Queste modifiche appaiono ancora oggi necessarie e utili nell'ottica di bilanciare ulteriormente un assetto che, nell'esperienza quotidiana dell'Autorità, appare talvolta eccessivamente pesante nei confronti di violazioni minori, con una ricaduta ridotta in termine di lesione effettiva dei diritti.

Per altro verso, invece, l'esperienza applicativa dell'Autorità dimostra che, in ambiti nei quali gli interessi economici e la competizione sul mercato tra soggetti diversi sono molto forti, l'attuale sistema sanzionatorio risulta scarsamente dissuasivo (il caso tipico è quello del fenomeno del cd. *marketing* selvaggio).

In questi casi si rende necessario semmai introdurre forme di progressivo automatico aggravamento delle sanzioni in caso di ripetute violazioni delle medesime disposizioni da parte dello stesso soggetto in un arco di tempo definito, al fine di disincentivare le pratiche scorrette.

Come già evidenziato al precedente paragrafo 18.5.1, ormai indifferibile appare la revisione delle misure minime di sicurezza contenute nel disciplinare tecnico allegato B al Codice, in ragione dell'obsolescenza di molte disposizioni (pensate ormai più di dieci anni fa) e del mutato contesto tecnologico di riferimento, con l'esigenza crescente di proteggere il dato non solo staticamente, allorché è memorizzato all'interno di una banca dati, ma, ancor di più, in tutte le occasioni (sempre più frequenti) in cui lo stesso è oggetto di trasferimenti per mezzo delle reti di comunicazione o di accesso da parte di postazioni remote.

Il processo di revisione di queste regole è affidato dalla legge (art. 36 del Codice) ad un decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa.

Nel disegno di legge "Misure di semplificazione degli adempimenti per i cittadini e le imprese e di riordino normativo", attualmente all'esame del Senato, è già prevista una modifica di questa norma, ma non nel senso auspicato dall'Autorità.

Considerata la particolare sensibilità e l'esperienza maturata sul campo nelle centinaia di ispezioni effettuate nei più diversi contesti tecnologici, apparirebbe più opportuno infatti affidare al Garante non solo un ruolo consultivo ma di iniziativa dell'*iter* di rinnovamento di quelle misure di minime di sicurezza la cui corretta implementazione, da parte di enti pubblici e soggetti privati, costituisce ormai una condizione necessaria ed essenziale di garanzia per i cittadini nella società dell'informazione, restituendogli anche il potere di semplificare tali misure in tutti quei contesti in cui la loro implementazione risulterebbe sproporzionata in relazione alla tutela degli interessi protetti.

19 Le relazioni comunitarie e internazionali

Il 2013 è stato un anno cruciale per la protezione dei dati a livello europeo e internazionale.

Sono infatti proseguite le intense attività di revisione degli strumenti normativi più importanti in materia, nell'ambito dell'Unione europea, del Consiglio d'Europa e dell'OCSE, dettate dalla necessità di rispondere alle numerose sfide poste dall'incessante sviluppo tecnologico e dalla globalizzazione, nonché dall'esigenza di pervenire a *standard* uniformi nei diversi stati.

L'Autorità ha contribuito attivamente a tali processi di riforma partecipando ai numerosi gruppi di lavoro istituiti in ambito UE ed internazionale (cfr. tabelle 1 e 21).

In particolare, a livello comunitario è proseguito il negoziato riguardo ad un nuovo quadro giuridico europeo sulla protezione dei dati, composto dalla proposta di regolamento generale (doc. web n. 2110215), volto a sostituire la direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali), e dalla proposta di direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali (settori attualmente esclusi dall'ambito di applicazione della direttiva 95/46/CE) (doc. web n. 2110225).

L'attività legata al regolamento (v. par. 19.1) è proseguita in maniera assai intensa anche in vista dell'imminente fine della legislatura del Parlamento europeo e della scadenza del mandato della Commissione, previste entrambe per il 2014. L'auspicio è di pervenire, prima della fine della legislatura, ad un testo condiviso eventualmente da perfezionare durante il semestre di Presidenza italiana (luglio-dicembre 2014).

In linea generale, il dibattito sulla proposta di direttiva è andato più a rilento rispetto a quello che ha interessato la proposta di regolamento, anche in ragione del fatto che si è ritenuto opportuno risolvere preliminarmente le questioni problematiche in sede di regolamento generale, per poi esaminare l'eventualità di riproporre, laddove opportuno, le soluzioni raggiunte nella direttiva (v. par. 19.1).

Parallelamente al pacchetto di riforma UE, nell'ambito del Consiglio d'Europa è proseguito il processo di modernizzazione della Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Con l'approvazione del documento finale contenente le proposte di revisione della Convenzione 108 da parte del Comitato consultivo T-PD, avvenuta alla fine del 2012, si è conclusa la fase tecnica del lavoro di modernizzazione della 108 e si è aperta una fase "politica", con l'istituzione di un comitato intergovernativo (CAHDATA) incaricato dal Comitato dei Ministri del Consiglio d'Europa di portare a termine la stesura di un protocollo emendativo alla Convenzione (v. par. 19.5).

In sede OCSE, si è invece concluso il processo di modernizzazione degli strumenti *privacy* avviato nel 2010, con l'adozione, avvenuta l'11 luglio 2013, delle nuove linee guida *privacy* OCSE che sostituiscono quelle del 1980 (v. par. 19.5).

Sia a livello europeo che internazionale, il 2013 si è anche caratterizzato per l'importante lavoro svolto dalle Autorità di protezione dei dati finalizzato ad una più stretta ed efficace cooperazione, specie in materia di *enforcement* (v. *infra*). L'accentuarsi della natura transfrontaliera delle problematiche legate all'attuazione dei principi di protezione dei dati nel mondo digitale rende infatti necessaria la predisposizione di strategie comuni sulla base di principi condivisi.

19.1. *La riforma del quadro giuridico europeo in materia di protezione dei dati*

La riforma del quadro giuridico in materia di protezione dati nell'UE proposta dalla Commissione europea il 25 gennaio 2012 comprende un regolamento generale sulla protezione dei dati ed una direttiva che disciplinerà i trattamenti di dati personali svolti per finalità di contrasto dei reati. L'adozione dei testi definitivi avverrà dopo l'approvazione da parte dei due co-legislatori (Parlamento europeo e Consiglio dell'UE), secondo la procedura introdotta dal Trattato di Lisbona.

Nel corso del 2013, l'Autorità ha continuato a partecipare attivamente al negoziato in corso al Consiglio UE, assicurando un costante flusso di contributi scritti sull'articolato del testo e contribuendo alla definizione della posizione italiana nel negoziato. I lavori del gruppo del Consiglio che esamina il pacchetto si sono concentrati principalmente sulla proposta di regolamento, giunta alla terza/quarta lettura, anche se nulla sarà definito finché non si sarà trovato l'accordo su tutto l'articolato. Pertanto alcune parti sono state analizzate più dettagliatamente per scelta delle presidenze che si sono succedute nel corso dell'anno, nel tentativo di giungere ad un comune sentire rispetto ad aspetti fondamentali e nuovi della proposta come il principio del cd. *one stop shop* (sportello unico) ed i meccanismi di mutuo riconoscimento.

La proposta di direttiva, per la quale si è arrivati alla seconda lettura di parte del testo, essendo in parte legata alla soluzione di temi generali (definizioni, principi fondamentali, obblighi dei titolari, trasferimento dei dati, supervisione e controllo) ed in parte legata ad istanze legate al mantenimento della sovranità degli Stati in ambiti quali la prevenzione, contrasto e repressione di crimini, ha avuto finora un percorso più lento.

L'intento perseguito dal Garante nella partecipazione ai lavori sul pacchetto di riforma UE è, in primo luogo, quello di assicurare che i nuovi strumenti in discussione non contengano previsioni peggiorative rispetto a quelle contenute nella direttiva 95/46/CE, recepite nella legislazione italiana, prima con la l. n. 675/1996 e, poi, con il Codice. Uno dei principali propositi della riforma UE è infatti quello di mantenere alto il livello di tutela dei diritti delle persone, pur nella semplificazione degli oneri per imprese e altri soggetti titolari del trattamento. In quest'ottica, appare ad esempio auspicabile che il perseguimento del cd. sportello unico – che individua un'unica autorità di controllo competente a controllare le attività del titolare del trattamento in tutta l'Unione, in modo da garantire la certezza giuridica e ridurre gli oneri amministrativi per i titolari del trattamento – sia accompagnato da meccanismi che rendano altrettanto agevole l'esercizio dei diritti da parte degli interessati (cd. *proximity*). Appare inoltre auspicabile che con il nuovo pacchetto di riforma si arrivi ad un quadro di sanzioni, in caso di mancato rispetto dei principi di protezione dei dati, il più possibile uniforme tra i vari Stati.

Quanto ai tempi della riforma, contrariamente a quanto auspicato anche dal Gruppo Art. 29 nella lettera alla Presidenza greca dell'11 dicembre 2013 (doc. web n. 2980372) ovverosia, l'adozione del pacchetto di riforma entro la fine della legislatura UE, il documento finale del Consiglio UE del 25 ottobre 2013 ha genericamente fatto riferimento ad una "tempestiva adozione" del pacchetto di protezione dati per consentire il pieno funzionamento del mercato unico digitale "entro il 2015". Il Garante ha a tal proposito manifestato la propria delusione auspicando invece una risposta all'altezza delle aspettative.

Va ricordato, peraltro, il voto del 21 ottobre con cui la Commissione competente del Parlamento europeo (LIBE - Libertà civili, giustizia e affari interni) ha approvato gli emendamenti ai testi delle due proposte (regolamento e direttiva).

A questo voto, giunto dopo oltre 20 mesi di intenso dibattito durante i quali sono stati presentati più di 3.000 emendamenti, ha fatto seguito la votazione finale della Plenaria avvenuta il 12 marzo 2014. Se anche l'altro co-legislatore europeo (il Consiglio UE) arriverà ad un accordo politico sul testo dei due strumenti, potranno avere inizio i negoziati attraverso il cosiddetto "trilogo" fra Parlamento, Consiglio e Commissione, auspicabilmente, sotto presidenza italiana, nel secondo semestre del 2014.

Il Parlamento ha mantenuto chiara l'impostazione iniziale ovvero che le due proposte fanno parte di un "pacchetto" di norme da gestire in modo unitario; per tale ragione molti emendamenti alla proposta di direttiva sui trattamenti di dati personali nelle attività giudiziarie e di polizia tendono a garantire uniformità con le disposizioni introdotte nel regolamento che fissa un quadro "generale" di norme in materia di protezione dati nell'UE: ciò vale, ad esempio, rispetto alle definizioni contenute nei due strumenti, ai poteri delle autorità di controllo, alla loro previa consultazione o ad alcuni strumenti (quali la valutazione di impatto-*privacy*).

Per quanto riguarda gli emendamenti approvati relativi alla proposta di regolamento, il testo mantiene in larga parte l'impostazione dell'originaria proposta della Commissione: ad esempio, in materia di consenso della persona interessata (che deve essere "esplicito" anziché solo "inequivocabile" come nell'attuale direttiva 95/46/CE) o in tema di diritto alla portabilità dei dati. Sono state inoltre mantenute, sia nel testo del regolamento che in quello della direttiva, alcune proposte innovative, quali la nomina (obbligatoria) di un "*data protection officer*" da parte di alcune categorie di titolari di trattamento (secondo criteri però diversi rispetto a quelli indicati dalla Commissione), l'introduzione di un obbligo generale per tutti i titolari di notificare eventuali violazioni di dati personali (anche agli interessati, in determinati casi), e, per altro verso, l'eliminazione dell'obbligo, oggi vigente, di notificare i trattamenti all'autorità di controllo. Gli emendamenti introducono anche versioni "semplificate" di alcune disposizioni del futuro regolamento: ad esempio, il diritto all'oblio è stato trasformato in un diritto alla rettifica o al "congelamento" dei dati.

La posizione della LIBE è stata influenzata anche dalla necessità di fornire risposte "forti" alle attività di sorveglianza di massa legate al cd. *Datagate* trapelate sugli organi di stampa a partire dal giugno 2013. Così si spiega, ad esempio, la scelta di vincolare all'autorizzazione dell'autorità di protezione dei dari competente nonché alla preventiva informativa all'interessato, l'invio di dati su richiesta di autorità giudiziarie o amministrative di Paesi terzi.

Il voto LIBE ha fornito una spinta al rafforzamento dei diritti degli interessati, nonché alla previsione di forti sanzioni per le imprese che violino i principi di protezione dei dati personali. Nel testo approvato è stato infatti modificato il sistema delle sanzioni amministrative, che tutte le autorità nazionali di controllo devono poter comminare, ma che sono libere di definire entro una soglia pecuniaria massima e nel rispetto di una griglia di criteri fissati nel resto, cui si aggiunge l'intervento chiarificatore e di indirizzo del Comitato europeo della protezione dati (il *board* europeo della protezione dati, "erede" dell'attuale Gruppo Art. 29). Ulteriori modifiche significative riguardano il cd. sportello unico e la collaborazione fra autorità di controllo attraverso il cd. meccanismo di coerenza: secondo il Parlamento, lo sportello unico deve permettere alle imprese multinazionali di dialogare con un unico interlocutore nell'UE (l'autorità di controllo del Paese dove hanno lo "stabilimento principale"), ma il ruolo di questa autorità capofila (cd. *lead authority*) deve consistere nel coordinamento di un processo di co-decisione cui tutte le autorità degli Stati membri interessati da un trattamento devono partecipare.

Gli aspetti che hanno suscitato perplessità in entrambi gli strumenti così come emendati nelle proposte della LIBE riguardano invece l'introduzione della definizione di "dato pseudonimo", locuzione suscettibile di generare incertezze interpretative; le norme sulla profilazione e la definizione stessa di profilazione; l'introduzione, chiesta dal Parlamento (ma solo nel regolamento), di un "certificato europeo" della protezione dati, che costituisce una sorta di "bollino-qualità" in grado di consentire ai titolari di trattamenti di beneficiare di varie deroghe ed esenzioni, e la cui vigilanza sarebbe affidata a soggetti terzi, diversi dalle autorità di controllo. Tali aspetti appaiono peraltro tra i punti (critici) evidenziati anche dal Gruppo Art. 29 che, nell'allegato alla citata lettera alla presidenza greca dell'11 dicembre 2013, ha sottolineato gli aspetti ancora migliorabili della riforma.

In tale sede il Gruppo ha comunque manifestato il proprio plauso al lavoro svolto dalla LIBE, che ha tenuto conto di molte delle raccomandazioni fornite dallo stesso WP29, ha perseguito l'idea del "pacchetto di riforma" votando su entrambe le proposte della Commissione (regolamento e direttiva) e non ha lasciato dubbi sul fatto che il regolamento si applichi tanto al settore privato quanto a quello pubblico.

Più in generale, il Gruppo Art. 29 ha seguito con attenzione il processo di riforma in atto, fornendo diversi contributi nel corso dell'anno. In particolare, nel parere n. 1/2013 adottato il 26 febbraio 2013 (doc. web n. 2980389), completando il lavoro fatto nel 2012 con i pareri nn. 1/2012 e 8/2012 (doc. web nn. 2572831 e 2133818; cfr. Relazione 2012, p. 273), si è soffermato sulla proposta di direttiva della Commissione, ed in particolare sulla necessità di: rafforzare la tutela dei dati relativi a persone non sospette, vittime di reati e terze parti; ampliare l'esercizio dei diritti dell'interessato che non deve essere oggetto di deroghe ingiustificate; applicare il principio della verifica dell'impatto *privacy* anche nell'ambito della direttiva; rafforzare e specificare i poteri delle autorità di protezione dati in questo particolare ambito.

Con il documento del 27 febbraio 2013 (doc. web n. 2980331) il Gruppo ha preso posizione su sei specifici settori del pacchetto di riforma, ed in particolare sulla necessità di: mantenere un approccio omogeneo sul trattamento di dati effettuati in ambito privato e pubblico; considerare i "dati pseudonimi" come dati personali (applicando quindi anche ad essi i principi di protezione dati); specificare che il consenso dell'interessato deve essere "esplicito"; irrobustire il ruolo delle autorità nazionali di protezione dei dati – rispetto alle quali l'imprescindibile requisito dell'indipendenza è stato ribadito dalla Corte di giustizia nella sentenza dell'8 aprile 2014 (Commissione europea c. Ungheria) (Causa C-288/12) – e del Comitato europeo della protezione dati; rafforzare la tutela dei dati che siano oggetto di trasferimento verso Paesi terzi; mantenere l'approccio fondato sulla valutazione del rischio da parte dei titolari del trattamento. Nei due allegati a tale documento il Gruppo ha altresì dedicato una particolare attenzione al tema della cd. *household exemption* ovvero la deroga ai principi di protezione dei dati ove il trattamento sia limitato a finalità esclusivamente personali (doc. web n. 2980411) e della cd. *lead authority* e delle sue competenze (doc. web n. 2980401).

Il Gruppo ha anche preso posizione sulla disciplina in materia di profilazione contenuta nella proposta di regolamento. Con l'*advice paper* del 13 maggio 2013 (doc. web n. 2980350) ha fornito indicazioni affinché nella proposta di regolamento sia garantita una maggiore trasparenza e un più efficace controllo sui propri dati da parte dell'interessato, una più ampia responsabilità dei titolari che intendano avvalersi di tecniche di profilazione, ed un approccio flessibile del testo normativo capace di fornire una tutela appropriata distinguendo le ipotesi di profilazione che abbiano ripercussioni sui diritti delle persone e quelle invece caratterizzate da un livello di intrusione meno significativo.

19.2. *Le conferenze delle Autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati si è tenuta a Varsavia dal 23 al 26 settembre 2013.

La Conferenza internazionale delle autorità di protezione dati

La Conferenza di quest'anno, alla quale hanno partecipato il Presidente e il Segretario generale dell'Autorità, si è articolata su tre macro-aree tematiche: i processi di revisione degli strumenti di protezione dei dati attualmente in corso a livello europeo e internazionale (UE, Consiglio d'Europa, e OCSE); le sfide per la *privacy* sollevate dalle nuove tecnologie; le prospettive, il ruolo e gli interessi dei diversi attori in gioco.

Nel corso della Conferenza sono state adottate otto risoluzioni. Particolare interesse riveste la risoluzione, sostenuta anche dal Garante, con la quale la Conferenza ha adottato un programma comune che impegna i governi a promuovere l'educazione digitale di tutti i cittadini, senza distinzione di età, esperienza o ruolo rivestito (doc. web n. 2681083). Il programma fissa cinque principi: assicurare una protezione particolare ai minori; garantire una formazione permanente sulla tecnologia digitale; raggiungere un giusto equilibrio tra opportunità e rischi presenti in tale ambito; promuovere il rispetto degli utenti; diffondere un pensiero critico sull'uso delle nuove tecnologie. Le altre Risoluzioni hanno invece riguardato: la necessità che imprese e governi assicurino la massima trasparenza nel trattamento dei dati dei cittadini (doc. web n. 2674966); l'esigenza che l'attività di profilazione si basi su una preliminare valutazione di impatto-*privacy*, garantisca trasparenza agli interessati e ponga particolare attenzione alla tutela dei minori (doc. web n. 2674994); l'attenzione da porre ai rischi legati al crescente ricorso al tracciamento della navigazione sul web (cd. *web tracking*), che deve essere reso più trasparente ed ispirarsi ai principi detti di *privacy by design* (doc. web n. 2675046); l'obiettivo di pervenire ad un maggiore coordinamento tre le autorità per aumentare l'efficacia delle attività di *enforcement* (doc. web n. 2681271); l'esigenza di adottare un piano strategico di azione per il biennio 2014-2015 finalizzato alla creazione di una rete globale di regolatori (doc. web n. 2674167); la necessità di un accordo internazionale vincolante che salvaguardi i diritti umani attraverso un corretto equilibrio tra sicurezza, interessi economici e libertà di espressione (doc. web n. 2674346). La Conferenza ha anche adottato una dichiarazione sui rischi e le sfide posti dal crescente uso delle *app*, che ha assunto dimensioni tali da poter parlare di una vera e propria "appificazione" della società (doc. web n. 2659319).

A margine della Conferenza internazionale si è tenuto il primo *workshop* del progetto europeo PHAEDRA (*Improving Practical and Helpful cooperAtion bEtween Data PRotection Authorities*) volto a migliorare la cooperazione tra le autorità di protezione dei dati. Per il secondo anno di attività, lo stesso si soffermerà su due aspetti problematici: la creazione di un quadro (vincolante o meno) per lo scambio di informazioni nonché per le ispezioni congiunte e l'individuazione degli ostacoli alla cooperazione e di possibili soluzioni (v. anche par. 19.5).

La Conferenza delle autorità europee (*Spring Conference*)

L'annuale Conferenza di primavera (*Spring Conference*) che riunisce le autorità di protezione dei dati europee, svoltasi a Lisbona dal 16 al 17 maggio, ha approvato tre importanti risoluzioni con le quali vengono fissate precise condizioni necessarie a tutelare i cittadini europei in particolare rispetto agli scenari futuri della *privacy*, al negoziato per la creazione di un'area di libero scambio USA-UE e ai trattamenti di dati effettuati da Europol.

La prima Risoluzione (doc. web n. 2980494), che concerne il futuro della protezione dei dati personali in Europa, sottolinea l'urgenza che il nuovo Regolamento generale sulla protezione dei dati e la proposta di direttiva siano adottati contestual-

mente per evitare pericolose lacune nella tutela dei cittadini europei, in particolare in un momento di crescente accesso ed uso da parte di autorità giudiziarie e forze di polizia di dati personali raccolti ed in possesso di soggetti privati. La Risoluzione incoraggia inoltre sia le imprese, sia le istituzioni pubbliche ad investire nella sicurezza dei dati e le autorità di protezione dati a cooperare tra loro.

La seconda Risoluzione (doc. web n. 2980484), promossa dall'autorità tedesca ed appoggiata tra gli altri dal Garante, tocca il delicato tema della creazione di uno spazio transatlantico di libero scambio ed auspica che nelle prossime negoziazioni tra UE ed USA il diritto fondamentale alla protezione dei dati venga promosso attraverso regole, sia sostanziali sia procedurali, volte a disciplinare lo scambio di dati e consentire controlli efficaci da parte di autorità indipendenti, anche per quanto riguarda l'accesso da parte delle autorità giudiziarie e di polizia alle banche dati delle imprese.

La terza Risoluzione (doc. web n. 2980604), che ha avuto anch'essa tra i proponenti il Garante, è dedicata al nuovo quadro legale presentato dalla Commissione europea che ridisciplina funzionamento e competenze dell'Europol, introducendo novità di grande rilievo ed impatto (ampliamento dei reati per i quali l'organizzazione è competente a raccogliere ed analizzare dati; crescita delle possibilità di comunicazione ed accesso ai dati all'interno ed all'esterno dell'organizzazione). La Risoluzione mira a scongiurare il rischio che le proposte della Commissione abbassino il livello di tutela rispetto a quello oggi vigente, impedendo il rispetto di principi essenziali (in particolare quello di finalità) che oggi limitano il riutilizzo e l'accesso ai *file* e alle informazioni talora sensibili detenute da Europol.

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

La cooperazione tra le Autorità garanti nell'UE riunite nel Gruppo Art. 29 è proseguita nel 2013 coerentemente al programma di lavoro adottato il 1° febbraio 2012 (doc. web n. 2375271).

L'obiettivo principale del Gruppo non è stato solo quello di assicurare una corretta e coerente applicazione del sistema di protezione dei dati in vigore, ma anche di proseguire il lavoro di preparazione rispetto al futuro quadro normativo sulla base delle proposte della Commissione europea del 25 gennaio 2012 (cfr. *supra* par. 19.1).

Punto chiave del lavoro dei Garanti è stata anche la riflessione su strategie comuni di *enforcement* volte a rendere più efficace l'applicazione dei principi di protezione dei dati su scala internazionale.

Inoltre il lavoro del Gruppo si è concentrato sulle numerose sfide che derivano dall'incessante sviluppo delle nuove tecnologie, sulla necessità che anche nell'ambito della libertà, sicurezza e giustizia sia assicurato un efficace sistema di tutela dei diritti degli individui, sulle sfide della globalizzazione e sul tema dei trasferimenti internazionali di dati.

Il Gruppo si è riunito in sessione plenaria cinque volte. Il lavoro preparatorio è stato svolto, come di consueto, nei sottogruppi tematici a cui l'Autorità ha attivamente partecipato.

Applicazione uniforme delle norme-chiave della direttiva 95/46/CE

Il Gruppo ha proseguito il suo lavoro sulla corretta interpretazione ed applicazione delle nozioni fondamentali della direttiva 95/46/CE con il sottogruppo denominato "*Key Provisions*". In particolare, l'attività si è concentrata sull'approfondimento del concetto di finalità del trattamento e di trattamento compatibile con l'adozione del Parere n. 3/2013 (doc. web n. 2572901).

In tale parere il Gruppo da una parte ha svolto un'analisi dettagliata del principio di finalità previsto dall'art. 6, comma 1, lett. *b*), direttiva 95/46/CE (offrendo indicazioni specifiche sulla sua applicazione alla luce del quadro normativo vigente), dall'altra ha rivolto raccomandazioni al legislatore europeo affinché il nuovo regolamento mantenga le necessarie garanzie a presidio dei diritti delle persone.

Parere sul principio di finalità

Il principio di finalità è in effetti un elemento cruciale della tutela dei dati. Tale principio, che determina i limiti dell'uso dei dati da parte dei titolari del trattamento (consentendo comunque un certo grado di flessibilità), è caratterizzato da due componenti principali: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime ed essere successivamente trattati in modo non incompatibile con tali finalità (cd. uso compatibile). La valutazione della compatibilità, da effettuarsi caso per caso, deve tenere conto delle circostanze pertinenti ed in particolare: del rapporto tra gli scopi per i quali i dati sono stati raccolti e le finalità di trattamento successivo; del contesto in cui i dati personali sono stati raccolti e delle ragionevoli aspettative degli interessati riguardo al loro ulteriore utilizzo; della natura dei dati personali e dell'impatto del trattamento ulteriore sugli interessati; delle misure di salvaguardia adottate dal titolare per garantire un trattamento equo ed evitare eccessive ripercussioni sugli interessati.

Nel parere il Gruppo ha preso posizione su un aspetto importante del principio di finalità del trattamento, chiarendo che il trattamento di dati incompatibile con le finalità della raccolta è illecito. Il titolare non può dunque legittimare tale trattamento semplicemente avvalendosi di una nuova base giuridica prevista dall'art. 7 della direttiva. Il principio di finalità può infatti essere limitato solamente alle strette condizioni previste dall'art. 13 della direttiva, quando cioè tale restrizione, prevista per legge, costituisce una misura necessaria a salvaguardare gli specifici interessi previsti dallo stesso art. 13. Una simile posizione è parsa necessaria a fronte della proposta di Regolamento della Commissione che all'art. 6, comma 4 prevede un'ampia eccezione al principio di compatibilità stabilendo che se lo scopo dell'ulteriore trattamento non è compatibile con quello per il quale i dati personali sono stati raccolti, il trattamento deve avere come base giuridica almeno uno dei requisiti di legittimità del trattamento (previsti attualmente dall'art. 7 della direttiva) fatta eccezione per il "legittimo interesse" del titolare.

Proprio la sussistenza di un "legittimo interesse" in capo al titolare del trattamento, una delle possibili basi giuridiche su cui fondare il trattamento dei dati (in alternativa, ad esempio, al consenso dell'interessato), è stato un altro tema chiave della direttiva 95/46/CE affrontato nel corso dell'anno dal sottogruppo *Key Provisions*. In base all'art. 7, lett. *f*), della direttiva il trattamento di dati personali può essere effettuato ove sia necessario per il perseguimento dell'interesse legittimo del titolare del trattamento oppure dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

Parere sul "legittimo interesse"

Il tema è parso di particolare rilevanza anche alla luce del fatto che la proposta di Regolamento, introducendo l'obbligo di cd. *accountability*, tende a rafforzarne l'uso lasciando allo stesso titolare la valutazione sulla prevalenza del legittimo interesse sui diritti dell'interessato (il Codice prevede invece che il "bilanciamento" sia operato dal Garante (cfr. art. 24, comma 1, lett. *g*).

Secondo il Gruppo, il legittimo interesse costituisce un criterio di legittimità che non necessariamente deve applicarsi in via residuale, quando cioè non sia possibile avvalersi degli altri requisiti di legittimità del trattamento previsti dall'art. 7. Al contrario, può risultare il criterio più congruo – purché siano rispettati i diritti fondamentali dell'interessato – per evitare di fondare il trattamento su requisiti che non forniscano sufficienti garanzie per l'interessato (si pensi ad esempio all'ambito lavorativo, ove il

consenso del dipendente, a fronte del rapporto di per sé squilibrato tra datore di lavoro e lavoratore, difficilmente può dirsi "libero" come invece richiesto dalla direttiva).

Occorre tuttavia evitare accuratamente che il legittimo interesse possa rappresentare la facile via d'uscita per il titolare che non abbia altra base su cui fondare il trattamento.

Per tale ragione il parere in corso di elaborazione dovrà essere sufficientemente "prescrittivo" nell'individuazione dei criteri su cui basare il bilanciamento di interessi in gioco.

Anche in questo caso, l'impostazione finora data dal sottogruppo al parere si struttura su un'accurata analisi del testo dell'art. 7, lett. *f*), della direttiva e su una parte conclusiva contenente possibili raccomandazioni riguardo alla normativa in materia, con particolare riferimento al pacchetto di riforma attualmente in discussione.

Aeromobili a pilotaggio remoto (cd. droni)

Molto intensa è stata l'attività del Gruppo Art. 29 con riferimento alle sfide per la protezione dei dati sollevate dalle nuove tecnologie. In questa cornice, è stata predisposta ed inviata alla Commissione europea una risposta ad un questionario sugli aspetti di riservatezza e protezione dei dati correlati all'utilizzo di aeromobili a pilotaggio remoto (APR, cd. droni) in ambito pubblico, commerciale e privato (doc. web n. 2982766).

Il questionario era stato inoltrato al Gruppo Art. 29 dalla Commissione (DG imprese e industrie) nell'ambito di un progetto volto a integrare tali mezzi nel piano di gestione del traffico aereo europeo (ATM-*Air Traffic Management*) al fine di aprire un confronto con le autorità di protezione dei dati europee sul tema. Il Garante, in qualità di *rapporteur*, ha raccolto le risposte fatte pervenire dalle diverse autorità e ha predisposto la lettera volta a sintetizzarne il contenuto e a richiamare l'attenzione su alcuni aspetti problematici del trattamento dei dati personali (base giuridica, informativa, titolarità del trattamento, *etc.*) effettuato attraverso i sempre più avanzati sistemi di rilevazione con cui tali mezzi possono essere equipaggiati (microfoni e telecamere ad alta risoluzione e/o per la visione termica notturna, strumenti per intercettare le comunicazioni *wireless*, *etc.*). Il tema dovrebbe essere comunque oggetto di ulteriore approfondimento per la predisposizione di uno specifico parere, considerato che la Commissione europea intende adottare una comunicazione contenente proposte tese ad incentivare l'uso di tali apparecchi a fini commerciali.

Parere sulle *mobile apps*

Sempre in tema di nuove tecnologie, con l'adozione del Parere n. 2/2013 (doc. web n. 2572891), predisposto dal sottogruppo *Technology*, si è concluso il lavoro iniziato nel 2012 sui profili di protezione dei dati nell'ambito delle applicazioni per telefonia mobile (cd. *mobile apps*). Il parere, di cui il Garante è stato correlatore con specifico riferimento al profilo della sicurezza, evidenzia le problematiche emerse in seguito all'esponenziale diffusione delle applicazioni su dispositivi mobili degli ultimi anni.

Attraverso le *app* si possono raccogliere grandi quantità di dati personali relativi all'utente, spesso utilizzate per finalità ulteriori rispetto alle aspettative dell'utente medesimo. La mancanza di trasparenza, e quindi di consapevolezza da parte degli interessati, possono rendere il consenso al trattamento eventualmente manifestato non significativo (informato). Le misure di sicurezza non adeguate, la tendenza a concepire le finalità del trattamento con eccessiva elasticità e l'alto livello di frammentazione tra i diversi attori che operano nel mercato delle applicazioni sono fattori che contribuiscono ad un forte incremento dei rischi per la protezione dei dati.

Il parere, che rivolge raccomandazioni diversificate ai diversi *stakeholder* (sviluppatori delle *app*; proprietari, cd. *app stores*, *etc.*), chiarisce prima di tutto il quadro normativo applicabile, sostanzialmente fondato sulla direttiva 95/46/CE e sulla direttiva cd. *e-Privacy* (2002/58/CE), focalizza l'attenzione sulla necessità che la corretta base giuridica dei trattamenti legati alle *apps* sia il consenso dell'interessato, fornisce chiarimenti, anche ricorrendo ad esempi, sull'applicazione del principio di minimizzazione

dei dati e del principio di finalità, precisa gli obblighi relativi all'adozione di adeguate misure di sicurezza e di trasparenza rispetto agli utenti, si sofferma infine sulle particolari cautele a presidio dei minori nell'utilizzo di *apps*.

Cookies

Il Gruppo si è altresì occupato del tema dei *cookies*, in particolare con l'approvazione del documento di lavoro n. 2/2013 (doc. web n. 2982826) che fornisce indicazioni sulle modalità attraverso le quali i gestori di siti web debbano ottenere il consenso degli utenti per l'uso di tali dispositivi o di altre tecnologie che, analogamente ai *cookies*, consentono il tracciamento della navigazione.

Il Gruppo, prendendo atto che, dall'adozione della direttiva 2002/58/CE emendata nel 2009 e implementata in tutti gli Stati UE, sono state molte le tecniche per ottenere il consenso sviluppate dagli operatori di siti web, sottolinea che tali soggetti sono liberi di adoperare a tal fine i mezzi che siano più consoni alle peculiarità e al *target* del loro sito, purché il consenso raccolto rispetti i requisiti previsti dalla normativa comunitaria. Esso deve quindi fondarsi su una chiara informativa, visibile nello spazio e nel momento in cui il consenso viene richiesto, deve essere ottenuto prima che si dia inizio al trattamento di dati, deve manifestarsi con un'azione positiva o altro comportamento attivo dell'utente dal quale un operatore possa chiaramente desumere la sua volontà di acconsentire al trattamento, deve infine essere effettivamente "libero", garantendo all'utente la possibilità di fornire un consenso "granulare" ed evitando di condizionare l'accesso generale al sito all'accettazione da parte dell'utente di tutti i *cookies*.

Sistemi di misurazione "intelligenti"

Il Gruppo ha inoltre proseguito il suo lavoro sui sistemi di misurazione "intelligenti" nel settore energetico. La Raccomandazione della Commissione 2012/148/EU – il cui intento è quello di offrire agli Stati membri orientamenti sulla progettazione e il funzionamento delle reti e dei sistemi di misurazione intelligenti in modo da garantire il diritto fondamentale alla protezione dei dati personali – ha tra l'altro previsto che gli Stati membri adottino un modello per la valutazione dell'impatto sulla protezione dei dati (cd. *Data Protection Impact Assessment - DPIA Template*). Tale modello, la cui predisposizione è stata affidata ad uno specifico gruppo di esperti della Commissione (EG2), è stato sottoposto due volte al Gruppo Art. 29 che ha fornito indicazioni al riguardo con i due pareri nn. 4/2013 (doc. web n. 2572921) e 7/2013 (doc. web n. 2572931).

Con il primo documento il Gruppo, pur riconoscendo l'importante lavoro svolto dal *team* di esperti, ha giudicato il *template* non sufficientemente maturo soprattutto a causa della mancanza di chiarezza sulla natura e gli obiettivi della *DPIA*, di alcuni difetti metodologici del documento e della carenza di un approccio che tenga conto delle specificità del settore e dei relativi rischi per la protezione dei dati.

Con il secondo parere, il Gruppo ha riconosciuto i considerevoli miglioramenti apportati rispetto al primo modello, specie con riferimento alla precisione del metodo e alla sua fattibilità. Ciononostante, ha indicato ulteriori aspetti suscettibili di riconsiderazione: in particolare, ha raccomandato la predisposizione di un *test* che riguardi casi reali da sottoporre al Gruppo stesso al fine di dimostrare che la valutazione d'impatto costituisca un effettivo miglioramento della protezione dei dati nel settore dei sistemi di misurazione intelligenti, soprattutto riguardo alla *privacy by design* e *by default*, al principio di minimizzazione dei dati, al diritto all'oblio e alla portabilità dei dati, che sono peraltro al centro del pacchetto di riforma attualmente in discussione a livello europeo e che potrebbero dunque divenire in futuro specifici obblighi giuridici.

La *privacy policy* di Google

È proseguita l'importante iniziativa di cooperazione tra le autorità del Gruppo Art. 29 riguardo alla *privacy policy* di Google lanciata il 1° marzo 2012 dalla società di *Mountain View* e che già nell'ottobre del 2012 aveva portato il Gruppo a rivolgere a Google varie raccomandazioni per migliorare le informative, chiarire le modalità di

incrocio dei dati e, più in generale, garantire l'osservanza delle norme e dei principi in materia di prorezione dei dati con meccanismi semplificari di opposizione, raccolta del consenso espresso ai fini della combinazione dei dati per dererminate finalità, limitazione degli incroci di dati relativi ad utenti passivi (doc. web nn. 2375141 e 2375151).

Decorso il periodo previsto per l'adozione di modifiche della *privacy policy* necessarie per assicurare la conformità dei trattamenti alle disposizioni vigenti, i rappresentanti di Google Inc. hanno chiesto un incontro con la *task force* appositamente costituita per la verifica delle regole *privacy* di Google, coordinata dall'Autorità francese e composta anche dalle Autorità per la protezione dei dati di Italia, Germania (Amburgo), Regno Unito, Paesi Bassi e Spagna. A seguito dell'incontro, tenutosi a Parigi il 19 marzo 2013, la società non ha tuttavia adottato alcuna concreta iniziativa nel senso auspicato.

Le menzionate Autorità della *task force* hanno quindi annunciato in contemporanea, il 2 aprile 2013, l'apertura di istruttorie nei confronti di Google Inc. per verificare il rispetto della disciplina sulla protezione dei dati e, in particolare, la conformità dei trattamenti effettuati dalla società di *Mountain View* ai principi di pertinenza, necessità e non eccedenza dei dati trattati, nonché agli obblighi riguardanti l'informativa agli utenti e l'acquisizione del consenso.

All'esito di tali istruttorie, si segnalano allo stato le decisioni dell'Autorità di protezione dei dati olandese che ha ravvisato la violazione della normativa nazionale da parte della *privacy policy* di Google, di quella spagnola che ha risposto alle violazioni perpetrate dal motore di ricerca con una sanzione di €900.000, e dell'Autorità francese che ha sanzionato Google con il massimo finora comminato in Francia (€ 150,000) per non aver provveduto alle necessarie modifiche della sua *privacy policy* (per la parte di competenza dell'Autorità italiana cfr. par. 18.5.2).

Nel corso dell'anno il sottogruppo *technology* ha inoltre esaminato le politiche in materia di protezione dei dati anche di Microsoft. Sotto il coordinamenro delle Autorità di Lussemburgo e Francia, il Gruppo ha dato inizio ad una valutazione congiunta volta a verificare le possibili ripercussioni delle modifiche apportate dalla società a tali *policy* sui diritti degli interessati.

Parere in materia di anonimizzazione

Al Garante è stato affidato il ruolo di correlatore, insieme all'omologa Autorità francese, per la redazione di un patere del Gruppo Art. 29 in materia di anonimizzazione. Il Gruppo ha deciso, anche per chiarire l'ambito di applicazione della disciplina di protezione dei dati che, come noto, si applica ai dati che rendono identificabile una persona, di svolgere un'analisi sull'efficacia e i limiti delle tecniche di anonimizzazione esistenti e disponibili sul mercato. L'analisi ha mostrato che, pur riconoscendosi le potenzialità di tali tecniche che, specie nel caso dell'*open data*, possono rappresentare una strategia utile a mitigare i rischi per gli interessari e a valorizzarne dunque i benefici per gli individui e la società più in generale, diverse pubblicazioni scientifiche e la casistica disponibile mostrano le difficoltà di creare insiemi di dati realmente anonimi.

L'anonimizzazione, risultato di un processo che impedisce l'identificazione dell'interessato in maniera irreversibile, tenuto conto dei mezzi che "ragionevolmente" possono essere impiegati per l'identificazione da parte del titolare del trattamento o di un terzo, costituisce un'operazione ulteriore del trattamento dei dati in questione: l'opinione del Gruppo è che il trattamento ulteriore di dati personali finalizzato alla loro anonimizzazione è compatibile con il trattamento iniziale, purché il risultato finale sia un'effettiva anonimizzazione (de-identificazione irreversibile) nei termini indicati nel parere – tenendo conto del contesto dell'utilizzo dei dati anonimizzati e dei punti di forza e di debolezza delle diverse tecniche utilizzabili per l'anonimizzazione.

Nella sua analisi, il Gruppo non ha mancato di valutare anche la cd. pseudonimizzazione, sottolineando come essa possa sì dirsi un'utile misura di sicurezza che riduce

la diretta correlazione tra il dato e l'identità originale dell'interessato, ma certamente non un metodo in grado di impedire l'identificabilità di un soggetto in modo irreversibile, rimanendo quindi il dato pseudonimizzato pur sempre un "dato personale".

Il messaggio fornito dal Gruppo è che l'anonimizzazione può offrire garanzie per la *privacy* solo nella misura in cui essa sia congegnata in maniera appropriata, valutando caso per caso il contesto di adozione e gli obiettivi di tale tecnica, e tenendo a mente che anche i dati anonimizzati possono presentare rischi per gli interessati, in particolare ove sia ancora possibile ottenere informazioni su di essi attraverso altre fonti di informazioni, siano esse pubbliche o meno. È per questa ragione che è necessaria una valutazione periodica di tali rischi da parte dei titolari del trattamento.

Data breach notification

Il Gruppo ha svolto un approfondimento sulla notificazione in caso di violazione dei dati (cd. *data breach notification*), in particolare rivolto alla individuazione dei criteri di valutazione della severità di tale violazione, con l'obiettivo di fornire ai titolari più chiari parametri sui casi in cui notificare l'evento agli interessati coinvolti (essendo obbligatoria in ogni caso la notifica all'autorità competente, anche alla luce del Regolamento n. 611/2013 adottato in tal senso dalla Commissione europea nel mese di giugno).

Tale attività è stata svolta parallelamente al lavoro dell'*European Union Agency for Network and Information Security* (ENISA) con la quale il Gruppo ha interagito anche attraverso specifici incontri.

Cloud computing

È stata altresì avviata una riflessione sul codice di condotta in materia di *cloud computing* annunciato dalla Commissione con l'obiettivo di individuare uno schema di *governance* del *cloud* valido a livello europeo. Una volta ultimato, tale codice di condotta dovrebbe essere sottoposto al parere del Gruppo Art. 29 in base all'art. 27 della direttiva 95/46/CE.

Altri temi legati alla protezione dei dati nell'ambito delle nuove tecnologie su cui il Gruppo ha avviato una riflessione riguardano la internet delle cose, il cd. *device fingerprinting* (utilizzazione di elementi informativi al fine di consentire l'identificazione univoca ed il tracciamento degli utenti), e il cd. *wearable computing* (dispositivi che possono essere indossati – si pensi al caso di *Google Glass*).

A tal proposito il Gruppo ha sottoscritto una lettera il 18 giugno 2013 (doc. web n. 2985738), di cui è stata promotrice l'Autorità di protezione dei dati canadese, con la quale ha invitato Google ad impegnarsi in un dialogo con le autorità di protezione dei dati dei diversi paesi per chiarire i numerosi profili *privacy* inerenti ai cd. *glasses* (gli occhiali per la cd. realtà "aumentata" progettati dalla società). I Garanti hanno in particolare richiesto chiarimenti in merito alle misure pro *privacy* adottate dagli sviluppatori del prodotto, alle tipologie di dati raccolti da Google attraverso *Glass* e condivise con terze parti, le finalità dei trattamenti in essere, ed eventuali valutazioni di rischio messe in atto da Google.

Altrettanto intensa è stata l'attività del Gruppo in materia di *e-government*.

Parere sulla nuova direttiva *open data*

Subito dopo l'adozione della direttiva 2013/37/UE che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico (cd. direttiva "*open data*"), il Gruppo Art. 29, con il parere n. 6/2013 (doc. web n. 2572941), si è rivolto agli Stati membri per fornire precise indicazioni affinché la trasposizione della stessa negli ordinamenti nazionali avvenga in modo il più possibile omogeneo e tenga conto degli aspetti di protezione dei dati in esso rappresentati.

A differenza della direttiva 2003/98/CE – che si limitava ad armonizzare le condizioni per il riutilizzo delle informazioni del settore pubblico, lasciando tuttavia gli Stati membri liberi di decidere se rendere effettivamente disponibili per il riutilizzo tali informazioni –, la direttiva adottata a giugno 2013 ha introdotto il principio per cui tutte le informazioni detenute dal settore pubblico accessibili in base al diritto nazio-

nale sono riutilizzabili per finalità commerciali e non, a condizione però che tale riutilizzo non pregiudichi le disposizioni in materia di protezione dei dati personali.

Ogniqualvolta un documento pubblico contenga dati personali, infatti, il suo riutilizzo ricade nell'ambito di applicazione della disciplina dettata dalla direttiva 95/46/CE e dalle normative nazionali di recepimento. Alla luce di ciò, il Gruppo, come già nel precedente parere n. 7/2003 reso sul tema (doc. web n. 1609442), ha ricordato che nei casi in cui i soggetti pubblici intendano rendere disponibili per il riutilizzo, oltre a dati aggregati – il cui utilizzo dovrebbe essere sempre privilegiato –, anche dati personali, sarà necessario individuare, in concreto, una solida base giuridica e tenere in considerazione il rispetto dei principi in materia di protezione dei dati personali (e, tra essi, in particolare, i principi di necessità, di proporzionalità e di finalità). Il soggetto pubblico interessato non potrà pertanto limitarsi ad invocare sistematicamente, quale base giuridica per il trattamento, la necessità di rispettare la disciplina sul riutilizzo dei dati pubblici.

Il Gruppo suggerisce, quale buona prassi, l'adozione di misure legislative che specifichino chiaramente e sin dall'inizio quali dati possano essere resi pubblici, per quali finalità e in che misura e a quali condizioni il loro riutilizzo sia possibile. Nell'operare tale valutazione, gli Stati membri saranno tenuti a verificare che la *disclosure* di tali informazioni sia necessaria e proporzionata al legittimo scopo perseguito dalla legge (cfr. Corte europea di giustizia, sentenze del 20 maggio 2003, *Österreichischer Rundfunk*, e del 9 novembre 2010, *Volker und Markus Schecke*).

In questo contesto, cruciale diviene anche il ruolo dei principi di "*privacy by design*" e "*privacy by default*", nonché della valutazione di impatto *privacy* attraverso cui legislatori e soggetti pubblici potranno valutare gli aspetti relativi alla protezione dei dati prima che gli stessi siano resi disponibili per il riutilizzo. Sulla scorta degli esiti di tali valutazioni, i soggetti pubblici interessati potranno identificare misure appropriate per minimizzare i rischi e adottare ogni necessaria misura tecnica, giuridica e organizzativa (quali, ad esempio, specifiche licenze per il riutilizzo o accorgimenti tecnici per evitare la raccolta massiva di informazioni personali) ovvero decidere di non rendere disponibili per il riutilizzo alcuni dati.

Il parere, grazie ad esempi concreti tratti dalle diverse esperienze nazionali, fornisce un quadro di casi in cui la disciplina sul riutilizzo può trovare applicazione e casi di deroga alla stessa e si sofferma sui rischi legati alle tecniche di aggregazione e anonimizzazione di dati, richiamando l'attenzione, in particolare, sulle accresciute possibilità di re-identificazione degli interessati nel nuovo contesto tecnologico.

Lettera su proposta di Regolamento su *e-identity ed e-signature*

Sempre in tema di *e-government*, il Gruppo ha inviato alla Commissaria UE per l'agenda digitale Neelie Kroes una lettera sulla proposta di regolamento sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato unico digitale (COM/2012/0238 final) (doc. web n. 2983174). La proposta in questione mira a creare, nell'ambito dell'Unione, un quadro completo e omogeneo che garantisca transazioni elettroniche sicure e che comprenda l'identificazione, l'autenticazione e la firma elettronica, sostituendo la disciplina dettata dalla direttiva 1999/93/CE che si limita essenzialmente alle firme elettroniche.

Dopo aver suggerito l'utilizzo di definizioni in linea con quelle di comune uso internazionale per termini quali "autenticazione" e "identificazione elettronica", la lettera del Gruppo si sofferma sui rischi di un approccio, quale quello attuale della proposta di regolamento, basato sulla necessità di utilizzare sempre identificatori "univoci" per accedere ai servizi. Tale approccio – a parere del Gruppo – non tiene debitamente conto del fatto che rivelare la propria identità non è sempre necessario e che, in molti casi, sarebbe possibile utilizzare tecnologie o regole maggiormente rispettose del principio di minimizzazione dei dati personali (vedi, ad es., l'utilizzo di sistemi di