quello offeso dalle singole violazioni presupposte, poiché è specifica la lesione che si determina ai diritti quando dette plurime violazioni riguardano non singoli dati ma, come nel caso di specie, una banca dati "*di particolare rilevanza e dimensioni*".

Complessivamente le entrate relative all'attività sanzionatoria, per l'anno 2012, sono state pari a 3.769.217 euro in relazione a pagamenti effettuati:

- spontaneamente dai contravventori (2.928.267 euro);
- a seguito di ordinanza-ingiunzione adottata dall'Autorità (780.950 euro);
- a seguito di ammissioni al pagamento in relazione a procedimenti sulle misure minime di sicurezza (60.000 euro).

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 sono utilizzati unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

20.4.3. Le sanzioni amministrative introdotte nel Codice con il d.lgs. 28 maggio 2012, n. 69

Come più ampiamente riportato (cfr. *supra* 2.1.), per effetto del recepimento della Direttiva europea n.136/2009/CE avvenuto con il d.lgs. 28 maggio 2012, n. 69, sono state introdotte nuove disposizioni nel Codice, in particolare con riferimento alle comunicazioni elettroniche e alle cd. "violazioni di dati" o *data breach*.

La nuova disciplina ha previsto una serie di adempimenti che i fornitori di servizi di comunicazione elettronica accessibili al pubblico devono attuare nel caso accertino che i dati personali contenuti nei loro sistemi siano stati violati.

È importante osservare che la nuova disciplina riguarda al momento solo quei soggetti che mettono a disposizione del pubblico, su reti pubbliche di comunicazione, servizi consistenti "*nella trasmissione di segnali su reti di comunicazioni elettroniche*" (art. 4, comma 2, lett. *d)* ed *e)*, del Codice), anche se nell'ambito della revisione della disciplina comunitaria si prevede una sua estensione agli altri settori.

Il mancato rispetto degli adempimenti comporta l'applicazione delle sanzioni previste dall'art. 162-*ter*, anch'esso introdotto dal d.lgs. n. 69/2012.

Tali sanzioni sono destinate solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, ma se l'erogazione dei predetti servizi è stata affidata a terzi (caso tipico è l'*outsourcer* informatico che gestisce i sistemi informativi attraverso i quali il fornitore stesso eroga i servizi ai propri clienti) anche questi sono soggetti alle sanzioni ove non abbiano comunicato "*senza indebito ritardo*", al fornitore, le informazioni necessarie ai fini di porre in essere gli adempimenti di competenza (art. 162-*ter*, comma 5).

Le condotte sanzionate riguardano:

- l'omessa (o tardiva) comunicazione della violazione di dati personali al Garante;

- l'omessa (o tardiva) comunicazione della violazione di dati personali al contraente o altra persona, quando dovuta (ovvero quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona e il fornitore non ha dimostrato al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione);

- la tenuta di un aggiornato inventario delle violazioni di dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in modo da consentire al Garante di verificare il rispetto delle disposizioni in materia.

Il regime sanzionatorio previsto dal legislatore è particolarmente severo:

- da 25.000 a 150.000 euro, in caso di violazione dell'obbligo di comunicazione al Garante;

- da 150 a 1.000 euro per ciascun contraente o altra persona nei cui confronti tale comunicazione venga omessa o ritardata.

L'apparente tenuità della sanzione non deve ingannare in quanto molto spesso, quando si verifica una violazione dei dati personali contenuti in una banca dati, la stessa può riguardare centinaia, migliaia e talvolta anche decine o centinaia di migliaia di interessati. Nel caso quindi si accerti che a fronte di una violazione dei dati che ha riguardato ad esempio mille persone, un fornitore di servizi di comunicazione elettronica abbia omesso di effettuare le comunicazioni dovute agli interessati, l'importo della pena pecuniaria sarà moltiplicato per mille.

È stata inoltre espressamente esclusa l'applicazione dell'art. 8, l. n. 689/1981, che prevede, in caso di violazione di diverse disposizioni o di più violazioni della stessa disposizione l'applicazione della sanzione prevista per la violazione più grave, aumentata sino al triplo.

Per evitare un'eccessiva afflittività della sanzione nei casi più gravi, il legislatore ha comunque stabilito che la sanzione amministrativa commisurata al numero delle omesse comunicazioni agli interessati non può essere applicata in misura superiore al 5% del volume d'affari realizzato dal soggetto sanzionato nell'ultimo esercizio chiuso anteriormente alla notificazione della contestazione della violazione amministrativa.

21. LE RELAZIONI INTERNAZIONALI

Si premette che in questa sezione si riferisce in merito ad attività aventi intensità ed effetti nettamente differenziati, in quanto il graduale assorbimento di competenze normative statali da parte delle Istituzioni europee, nel progressivo instaurarsi di un quadro ordinamentale sempre più tendente all'unità, comporta un impegno che, oltre al settore preposto alle relazioni internazionali, coinvolge le diverse strutture dell'Autorità, quali, solo per citarne alcune, quelle competenti in materia di tecnologie, comunicazioni elettroniche, trattamenti di dati in internet, trasferimento di dati a Paesi terzi, *cloud computing*.

In questi ambiti il ruolo del Garante è quello di una Autorità nazionale chiamata, insieme con gli omologhi degli altri Paesi UE ad interpretare, intervenire e talvolta a risolvere conflitti applicativi o approcci diversi su questioni di comune interesse tra i Garanti dei diversi Stati membri.

Ciò vale anche, dopo l'entrata in vigore del Trattato di Lisbona, non solo per i trattamenti di dati che si svolgono nei settori "disciplinati" dalle disposizioni delle Direttive nn. 95/46/CE e 136/2009/CE per il settore delle comunicazioni elettroniche, che costituiscono il quadro armonizzato a livello europeo dei princìpi di protezione dei dati personali, per i quali la "stanza di compensazione" oltre che di cooperazione è oggi il Gruppo istituito ai sensi dell'Art. 29 della Direttiva n. 95/46/CE per svolgere i compiti più specificamente descritti nell'art. 30 di quest'ultima, ma anche per la cooperazione nel settore in precedenza denominato "trattamenti di polizia e giustizia".

Le analisi e le decisioni prese nei consessi comunitari sono sempre più rilevanti, se non anche vincolanti, per le autorità ed in tal senso, come vedremo, il pacchetto di riforma del quadro giuridico europeo in materia di protezione dei dati personali presentato dalla Commissione europea il 25 gennaio 2012 contiene ulteriori espliciti obblighi.

Ne deriva una crescente importanza delle attività svolte nel settore, l'intensificarsi di impegni a Bruxelles e l'esigenza di integrare nelle priorità di lavoro quelle provenienti dalle decisioni comuni, che richiede e richiederà sempre più in futuro la disponibilità di risorse finanziarie e di personale specificamente formato (con conoscenze linguistiche, di diritto comunitario e

tecnologiche) per far fonte adeguatamente ai nuovi compiti ed alle nuove sfide dell'integrazione degli ordinamenti. Su questi aspetti è in corso un dialogo con la Commissione europea, per far in modo che il nuovo quadro regolamentare preveda, oltre ai princìpi, anche i mezzi per garantire il concreto ed ottimale funzionamento dei meccanismi in parola.

Altre attività, nell'ambito del Consiglio d'Europa e dell'OCSE, per quanto anch'esse onerose, si svolgono in un quadro di cooperazione con tempi e modalità più strutturati e programmabili.

21.1. LA RIFORMA DEL QUADRO GIURIDICO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI

Il 2012 è stato un anno cruciale per la discussione sulla riforma globale della normativa UE in materia di protezione dei dati. Preso atto dei radicali cambiamenti che hanno riguardato il trattamento dei dati a causa dell'incessante progresso tecnologico e della globalizzazione, nonché dell'esigenza di garantire una maggiore uniformità applicativa dei princìpi *privacy* nei 27 Stati membri (v. Relazione 2011 p. 190 e ss.) la Commissione, il 25 gennaio 2012, ha presentato le proposte per un nuovo quadro giuridico europeo in materia, nell'intento di rafforzare i diritti della *privacy online* e stimolare l'economia digitale europea [doc. web nn. 1895615 e 1895611]. Il pacchetto di riforma si compone di una proposta di regolamento generale sulla protezione dei dati -volta a sostituire la Direttiva n. 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali)- e di una proposta di direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (settori attualmente esclusi dal campo di applicazione della Direttiva n. 95/46/CE). Tale proposta di direttiva mira a sostituire la Decisione quadro n. 2008/977 (sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale), estendendone il campo di applicazione anche ai trattamenti "domestici" e non solo ai dati oggetto di scambio tra autorità competenti degli Stati membri.

Nella proposta di regolamento si registrano diverse novità rispetto all'odierno quadro normativo. Restano ferme le definizioni fondamentali, ma con alcune significative aggiunte (quali quelle di dato genetico e dato biometrico); viene introdotto il principio

dell'applicazione del diritto comunitario anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi a cittadini europei o tali da consentire il monitoraggio dei comportamenti di cittadini UE; si stabilisce il diritto degli interessati alla cd. "portabilità del dato" (ad. es., nel caso in cui si intendesse trasferire i propri dati da un *social network* ad un altro); si introduce il cd. "diritto all'oblio", ossia il diritto ad ottenere la cancellazione delle informazioni personali anche *online*; scompare l'obbligo per i titolari di notificare i trattamenti di dati personali, sostituito da quello di nominare un *data protection officer*, per tutti i soggetti pubblici e per quelli privati al di sopra di un certo numero di dipendenti; viene introdotto il requisito della valutazione dell'impatto-*privacy* (*privacy impact assessment*) oltre al principio generale cd. "*privacy by design*" (cioè la previsione di misure a protezione dei dati già al momento della progettazione di un prodotto o di un *software*); si stabilisce l'obbligo per tutti i titolari di notificare all'autorità competente le violazioni dei dati personali (*personal data breach*); si fissano più specificamente poteri (anche sanzionatori) e requisiti di indipendenza delle Autorità nazionali di controllo, il cui parere sarà indispensabile qualora si intendano adottare strumenti normativi rilevanti per la protezione dei dati.

La proposta di direttiva sui trattamenti per finalità di giustizia e di polizia riprende l'impostazione del regolamento, richiamato in molte delle sue previsioni, e contiene, tuttavia, disposizioni specifiche sulle responsabilità dei titolari e sugli obblighi che su di essi incombono in materia di trasparenza ed accesso, fissa i criteri di legittimità dei trattamenti in questione, nonché i meccanismi di mutua cooperazione ed i poteri delle Autorità nazionali di controllo.

Le due proposte che formano il cd. "pacchetto protezione dati" hanno iniziato il loro *iter* legislativo presso il Parlamento europeo ed il Consiglio dell'Unione europea.

Il Consiglio UE ha affidato il compito di analizzare e discutere il progetto di riforma ad un Comitato denominato DAPIX ("protezione dati e scambio di informazioni") che ha dato inizio alle sue attività durante la presidenza danese (primo semestre 2012) e proseguito i lavori sotto la presidenza cipriota (secondo semestre 2012) ed irlandese (primo semestre 2013).

Il Garante ha partecipato attivamente sia al Gruppo Art. 29, che riunisce le Autorità europee di protezione dei dati e che ha continuato a fornire alla Commissione ed alle altre istituzioni la propria consulenza, sia al gruppo DAPIX, in qualità di esperto nella delegazione italiana.

Il Parlamento europeo, dopo aver nominato i relatori per ciascuna delle proposte, ha elaborato numerosi emendamenti che saranno auspicabilmente votati nella Commissione per le libertà civili, la giustizia e gli affari interni (Commissione LIBE) entro la primavera del 2013, per poi essere negoziati con Consiglio e Commissione nel tentativo di raggiungere un'intesa volta all'adozione del pacchetto di riforma prima del termine del mandato del Parlamento stesso.

Nonostante il forte richiamo all'esigenza di mantenere un elevato livello di tutela -pur garantendo la semplificazione di obblighi ed oneri per i titolari di trattamento (pubblici e privati)- il testo, nella sua versione iniziale, presenta diverse ambiguità e rischi, acuiti dall'andamento dei lavori in corso presso il DAPIX e dalla forte pressione dei grandi operatori commerciali sui legislatori e sulle istituzioni nazionali.

Suscita alcune perplessità la scelta dello strumento regolamentare, direttamente ed immediatamente applicabile, le cui previsioni, in settori molto diversi tra loro che talora risentono di tradizioni nazionali radicate, specie in ambito pubblico, potrebbero portare ad un "ribasso" dei livelli di protezione attualmente assicurati dai diversi ordinamenti degli Stati membri.

Come anticipato, in materia il Gruppo Art. 29 ha pubblicato diversi documenti contenenti osservazioni anche critiche nei confronti dei due testi, e numerosi suggerimenti per la Commissione europea e le altre istituzioni coinvolte nell'*iter*. Lo stesso ha fatto il Garante europeo della protezione dati, che ha una specifica competenza a formulare pareri sulle proposte legislative.

I temi più dibattuti sono stati l'applicazione del principio dello "stabilimento principale" (*main establishment*) dell'impresa che tratti dati in più di uno Stato membro quale fondamento dello "sportello unico" (*one stop shop*), per tutti gli obblighi *privacy*, in quanto l'affermazione della competenza esclusiva dell'Autorità di protezione dati dello Stato in cui

l'impresa individua il suo stabilimento principale non terrebbe conto sufficientemente dell'indipendenza e del principio di leale collaborazione delle autorità nazionali, nonché delle specifiche esigenze legate alle garanzie degli interessati; i poteri eccessivi della Commissione europea per quanto riguarda gli atti delegati e di esecuzione (che in molti casi andrebbero a precisare elementi essenziali e non accessori dei singoli meccanismi di trattamento); la rigidità del sistema sanzionatorio che impone sanzioni pecuniarie lasciando pochi margini di flessibilità per sanzioni alternative egualmente dissuasive ed efficaci quali le misure interdittive o di blocco del trattamento.

Più in dettaglio, nel marzo 2012 con il parere (n. 1/2012 - WP 191 [doc. web n. 2375522]) il Gruppo Art. 29, pur condividendo lo spirito delle proposte adottate dalla Commissione europea in quanto tese a rafforzare la protezione dei dati degli interessati, a definire meglio le responsabilità per il trattamento e a consolidare la posizione delle autorità di controllo tanto a livello nazionale che internazionale, ha auspicato miglioramenti del testo che portino all'edificazione di un sistema di protezione più forte ed omogeneo nei diversi Stati.

Nel parere è stata rilevata la difficoltà di considerare il pacchetto di riforma come un quadro comprensivo ed unitario (obiettivo che la Commissione ha dichiarato come centrale) sia perché sono stati presentati due strumenti diversi, sia perché la proposta di direttiva, formulata in modo generico, lascia margini troppo ampi al legislatore nazionale, ciò inficiando il proclamato intento di "armonizzazione". Positivo è stato ritenuto l'inserimento sia delle disposizioni che incentivano i responsabili del trattamento ad investire, sin dall'inizio, in una corretta salvaguardia dei dati (nella protezione fin dalla progettazione e nella protezione di *default*, nonché mediante le valutazioni d'impatto sulla protezione dei dati), sia di quelle volte ad armonizzare i poteri e le competenze delle autorità di controllo. Critiche sono invece state espresse sulla compatibilità costituzionale del principio dell'*one stop shop* (v. *supra*) per i suoi effetti sulla legge applicabile e sulla giurisdizione, sull'effettività della tutela per trattamenti che si dirigono a cittadini europei svolti da soggetti non stabiliti nell'UE, sulla mancata previsione espressa dell'esigenza di dotare di risorse adeguate le autorità di protezione dati, nonché sulla debolezza del modello di cooperazione europea nel quale risulta prevalente il ruolo della Commissione.

Dopo la discussione svoltasi nel DAPIX a seguito della presentazione del parere nel maggio 2012, il Gruppo ha adottato, il 5 ottobre 2012, un secondo più specifico parere (n. 8/2012 - WP 199 [doc. web n. 2133818]) per fornire ulteriori indicazioni di merito e segnalare non solo al Parlamento UE, ma anche al Consiglio, la preoccupazione dei Garanti europei in relazione all'andamento della discussione nell'ambito dello stesso DAPIX. Il nuovo parere assume posizione su alcune questioni di fondo, quali la definizione di dato personale, le attività puramente "domestiche" (che si sottraggono all'applicazione dei princìpi di protezione dei dati), la nozione di consenso, indicando la perdurante validità delle definizioni fornite dalla Direttiva n. 95/46/CE e la necessità del loro mantenimento, suggerendo al contempo la possibilità di introdurre specifiche deroghe, laddove necessario nei singoli articoli, senza alterare le definizioni.

Il parere, seppur in modo non esaustivo, affronta anche alcune delle già ricordate questioni "orizzontali" che investono l'intera struttura del regolamento, quali l'opportunità del ricorso ad atti delegati da parte della Commissione, nei molti casi menzionati nella proposta (art. 86).

Buona parte delle preoccupazioni formulate dai Garanti sono rispecchiate nei *report* presentati dai due relatori alla Commissione LIBE del Parlamento europeo, incaricata di redigere la posizione finale sul testo. I *report* contengono diverse centinaia di emendamenti che segnalano la necessità di apportare numerosi aggiustamenti.

Nel quadro delle possibili evoluzioni che le proposte di regolamento e di direttiva potrebbero avere e le ripercussioni sull'attività delle autorità di protezione dati, si segnala anche la lettera del 4 aprile 2012 [doc. web n. 2375399] inviata alla Vicepresidente della Commissione Reding, riguardo alla menzionata mancanza di un'espressa previsione circa la necessità di dotare le autorità di protezione dati di risorse adeguate.

I prossimi mesi saranno decisivi per capire se l'ambizioso progetto della Commissione europea vedrà la luce sostanzialmente immutato nelle linee generali e, soprattutto, se sarà raccolta la sfida di una protezione dati che sia all'altezza degli sviluppi tecnologici e del nuovo quadro di diritti fondamentali introdotto nell'UE con il Trattato di Lisbona.

21.2. LE CONFERENZE DELLE AUTORITÀ GARANTI SU SCALA INTERNAZIONALE

La Conferenza internazionale delle autorità di protezione dati a Punta del Este

La 34ª Conferenza internazionale dei *Privacy Commissioners* si è svolta in Uruguay (Punta del Este) dal 23 al 24 ottobre 2012.

Nel corso della sessione aperta della Conferenza, intitolata "*Privacy and Technology in balance*", sono stati discussi in particolare l'impatto degli sviluppi della società dell'informazione e le aspettative di questa riguardo a *standard* e prassi in materia di protezione dei dati. Nell'intervento di apertura della prima sessione è stata sottolineata la necessità di nuovi ed ulteriori interventi normativi per tener conto delle conseguenze della tendenza a porre in essere infrastrutture globali volte ad ottenere un impiego ottimale delle informazioni personali, sia nel settore privato, sia in quello pubblico. A tal proposito è stata rilevata l'esigenza di rileggere i princìpi base del trattamento dei dati anche per meglio garantire i diritti della persona. In particolare si è evidenziato come nel settore pubblico il diritto individuale debba essere bilanciato con altri interessi pubblici rilevanti, mentre nel settore privato c'è una chiara tendenza a trattare i dati personali come beni (una sorta di "parte commercializzabile" della propria personalità). I grandi fornitori di servizi internet (Microsoft, Google, solo per citare i maggiori) agiscono in condizioni di quasi monopolio e non sono soggetti alle norme sulla concorrenza con conseguenti limitazioni alla libertà di scelta degli utenti. Sottolineato che in questo momento regna l'incertezza nei comportamenti dei diversi attori, è stato ribadito come compito del diritto sia, costruendo sui princìpi fondamentali, dare risposte alle nuove sfide con ciò evitando che "la tecnica faccia la regola".

La seconda sessione si è occupata di *privacy* ed *e-governement* evidenziando, anche in questo settore, il problema delle grandi raccolte di dati e degli usi "non attesi" degli stessi. È stata sottolineata la necessità di aggiornare le regole di protezione dati per una nuova amministrazione, più accessibile e vicina ai cittadini. Il tema è stato approfondito anche in sessioni parallele dedicate all'*Open Government* ed all'*e-Health*. Le altre sessioni plenarie sono state dedicate ai modelli di regolazione esistenti, per individuare le buone prassi e stimolare la cooperazione tra i diversi mondi e modelli, peraltro in evoluzione (Europa, Stati Uniti, ma anche Oriente e soprattutto America latina).

Altri temi, trattati nelle sessioni parallele, hanno riguardato la geolocalizzazione pubblica e privata, la nuove sfide del web 3.0 anche per le autorità pubbliche, le tecniche informatiche per preservare le prove (*forensic tools*), la cooperazione internazionale tra le autorità di protezione dei dati e della *privacy*, il *marketing* comportamentale *online*, l'impiego della biometria, gli "*smart data*", il consenso informato, il diritto alla tutela dei dati personali come diritto fondamentale (che ha visto come relatore il Segretario generale del Garante), le sfide nascenti dall'incontro tra lotta alla pirateria e tutela della *privacy*.

La sessione chiusa della Conferenza, la cui partecipazione è limitata alle autorità di protezione dei dati -largamente ampliata nei tempi, rispetto alle precedenti conferenze- è stata dedicata ad una cospicua presentazione del tema "profilazione", con esempi tratti sia dal settore pubblico sia da quello privato, al termine della quale è stata predisposta una "dichiarazione" adottata da Jacob Konstamm (Presidente del Comitato esecutivo della Conferenza internazionale) e dall'Autorità uruguaiana [v. doc. web n. 2375042].

Nel corso della sessione sono state inoltre adottate le risoluzioni sul futuro della *privacy* [v. doc. web n. 2375251] e sul *cloud computing* [doc. web n.2375241].

Sono state altresì deliberate le ammissioni di nuove autorità come componenti (Colombia, Costa Rica, Perù, Norvegia, Serbia, Tunisia, Sud Corea) e come osservatori (AFPDP-rete delle autorità francofone, OAS-Organizzazione degli Stati Americani) ed è stata accolta la proposta dell'Autorità polacca di tenere in Polonia la 35ª Conferenza internazionale (Varsavia 24-27 settembre 2013).

La Conferenza delle autorità europee (*Spring Conference* 2012)

La *Spring Conference* del 2012, tenutasi a Lussemburgo dal 3 al 4 maggio 2012, anch'essa focalizzata sulle proposte di riforma del quadro legislativo comunitario in materia di protezione di dati, ha adottato una risoluzione [doc. web n. 2375261] con la quale ha auspicato un sempre maggiore coinvolgimento delle autorità garanti nella discussione e nell'attuazione della proposta stessa, nonché un quadro più coerente di princìpi, con meno deroghe ed eccezioni per quanto concerne i trattamenti regolati dalla proposta di direttiva.

Durante la *Spring Conference* è stato deciso di porre termine all'attività del WPPJ (*Working Party on Police and Justice* -Relazione 2011 p. 199). Il prof. Francesco Pizzetti (Presidente dell'Autorità fino a giugno), che ha assicurato la presidenza nei quattro anni di vita del

gruppo, è stato calorosamente ringraziato per l'incisiva attività svolta, così come i funzionari del Garante. La Conferenza ha, quindi, accolto la relazione conclusiva dei lavori svolti dal WPPJ e dal suo Presidente.

Su proposta del comitato di accreditamento sono entrate a far parte della Conferenza le Autorità del Montenegro e della Bosnia-Herzegovina.

L'Autorità di protezione dei dati portoghese si è offerta di organizzare la prossima Conferenza di primavera a Lisbona.

21.3. LA COOPERAZIONE TRA AUTORITÀ NELL'UE: GRUPPO ART. 29

La cooperazione tra autorità garanti nell'UE è continuata nel 2012 in seno al Gruppo Art. 29 come da programma di lavoro adottato a febbraio 2012 (WP 190 [doc. web n. 2375271]).

Il Gruppo si è riunito in sessione plenaria 5 volte, per un totale di dieci giorni. Tutto il lavoro preparatorio è stato svolto come d'abitudine, nei sottogruppi tematici che hanno tenuto complessivamente oltre trenta riunioni, molte delle quali di due giorni.

Si segnala in particolare che dei 7 pareri adottati, 2 hanno riguardato il pacchetto di riforma (1/2012 e 8/2012) curati dal sottogruppo "*Future of Privacy*" e 4 l'applicazione dei princìpi di protezione dei dati nell'ambito delle nuove tecnologie e 1 sul livello di protezione dei dati personali nel Principato di Monaco. Oltre ai pareri formali, il Gruppo ha predisposto 3 documenti di lavoro (rispettivamente riguardo le *Binding corporate rules* e il progetto *epSOS* - v. Relazione annuale 2011 p. 198) ed inviato 19 lettere, in particolare a Google Inc., riguardo ai cambiamenti della *privacy policy* degli utenti e alla DG TAXUD della Commissione sul *Foreign Account Tax Compliance Act* (FATCA, v. *infra*).

Interpretazione di disposizioni "chiave" della Direttiva n. 95/46/CE: concetto di "finalità" e "trattamento compatibile"

Il Gruppo Art. 29, mantenendo il suo ruolo di attivo interlocutore delle istituzioni comunitarie, *in primis* della Commissione europea, ha continuato nel 2012 a contribuire alla corretta interpretazione ed applicazione di nozioni fondamentali della Direttiva base n. 95/46/CE e, mediatamente, al dibattito sulla revisione del *data protection legal framework*. Il lavoro del sottogruppo *Key provisions* si è concentrato sul concetto di "finalità" e "trattamento compatibile", ai fini dell'adozione, di un parere previsto nel 2013.

Il testo del parere viene costruito in modo da fornire una vera e propria guida per l'applicazione pratica del principio di finalità, nell'attuale quadro giuridico, anche attraverso raccomandazioni per il futuro. Si parte dall'analisi del *background* storico/normativo (dalla Convenzione n. 108/81 alla Direttiva n. 95/46/CE, alla proposta di regolamento generale della protezione dati) rispetto al principio di "finalità" ed alle sue declinazioni (comprese le raccomandazioni settoriali sviluppate dal Consiglio d'Europa (CoE) nel corso degli anni), si passa poi all'analisi delle disposizioni pertinenti della Direttiva n. 95/46/CE (artt. 6 e 13, considerando 28 e 29) corredata da esempi desunti dalle esperienze nazionali, per poi concludere con alcune osservazioni in tema di prospettive e sviluppi, alla luce delle recenti proposte di modifiche della normativa (ad es., revisione del *data-protection framework*, proposte di riutilizzo dei dati del settore pubblico, ulteriore trattamento per scopi storici, statistici o scientifici; art. 13 della direttiva *e-privacy* sulle comunicazioni indesiderate, *open data*).

L'*opinion* dovrebbe ben evidenziare come il principio di finalità protegga gli interessati (fissando limiti sull'utilizzo dei loro dati), offrendo al tempo stesso un certo grado di flessibilità per i responsabili del trattamento. Il concetto di limitazione delle finalità viene costruito secondo due "blocchi principali": i dati personali devono essere raccolti per determinate, esplicite e legittime finalità e non essere successivamente trattati in modo compatibile con tali finalità. La compatibilità dell'ulteriore trattamento per uno scopo diverso, deve essere valutata caso per caso, ed a tal fine molto utili potranno risultare esempi basati sulla prassi delle autorità europee di protezione dei dati.

Questa analisi ha anche conseguenze per il futuro. Poiché l'art. 6(4) della proposta di regolamento sulla protezione dei dati restringe fortemente l'ambito di applicazione del principio della compatibilità, il Gruppo Art. 29 intende inserire nel parere specifiche proposte di modifica del testo.

Privacy e tecnologie

Un elemento-chiave sul quale il Gruppo Art. 29 si è concentrato nel 2012, in merito al rapporto fra protezione dati e tecnologie, ha riguardato la crescente perdita di controllo da parte dell'utente (ma anche del titolare, in taluni casi) sui propri dati. Che si tratti di tecnologie basate sul *cloud computing* o di applicazioni per telefonia mobile, o delle tecniche di profilazione basate sul monitoraggio della navigazione *online*, la cd. "autodeterminazione

informativa" -ovvero il potere dell'interessato di decidere in merito all'utilizzo dei suoi dati personali- è messa sempre più a rischio da modalità di trattamento non trasparenti e non rispettose dei princìpi fondamentali fissati nelle norme europee e nazionali in materia, soprattutto il diritto ad essere informati con chiarezza e il diritto ad esprimere un consenso pienamente valido prima di affidare i propri dati ad altri.

Parere sul *cloud computing*

Con il parere sul "*cloud computing*" (Parere n. 5/2012 - WP 196 [doc. web n. 2133003]), approvato il 1° luglio 2012, sono state fissate una serie di raccomandazioni per clienti e fornitori di servizi *cloud*, per garantire il rispetto dei princìpi di protezione dati, secondo i princìpi fissati dalla Direttiva n. 95/46/CE. Il parere, del quale l'Autorità italiana è stata co-redattrice, si concentra sulle garanzie di ordine contrattuale che dovrebbero essere rispettate sia da parte dei fornitori di servizi *cloud*, sia da coloro (pp.aa. o soggetti privati) che acquistano servizi in modalità *cloud*; evidenzia i rischi principali di queste tecnologie (perdita di controllo sui dati trasferiti nella "nuvola" e ridotta trasparenza delle operazioni di trattamento "delocalizzate"); analizza la problematica del trasferimento dei dati verso Paesi terzi; suggerisce il ricorso a forme di certificazione del fornitore *cloud* da parte di soggetti esterni ed indipendenti. Il parere contiene quindi un elenco dettagliato di misure tecnologiche di protezione per ovviare ai rischi sopra indicati, e si conclude con una serie di raccomandazioni sintetiche rivolte a fornitori e clienti su tutti gli aspetti affrontati, a partire dalla necessità per un cliente di servizi *cloud* di condurre preliminarmente una valutazione dei rischi per decidere se e come allocare dati personali nella "nuvola". Un allegato al parere illustra in sintesi le caratteristiche di funzionamento della tecnologia *cloud* ed i modelli di prestazione del servizio attualmente esistenti. Il parere evidenzia, inoltre, alcuni nodi tuttora irrisolti, *in primis* la circostanza per cui i principali fornitori di servizi *cloud* sono situati al di fuori dell'UE, ciò che rende più difficile il controllo del trattamento dei dati per le Autorità di controllo e per gli stessi utenti, ma anche per le stesse forze di polizia e giudiziarie, specialmente laddove le informazioni siano memorizzate in Paesi terzi ove non esista un livello "adeguato" di protezione dati.

Esenzione dal consenso per i *cookie*

I temi del consenso e della trasparenza sono al centro anche del parere adottato il 7 giugno 2012 (Parere n. 4/2012 - WP 194 [doc. web n. 2133013]) con cui sono state illustrate, in

particolare, le situazioni in cui si applica l'esenzione dall'obbligo generale di acquisizione del consenso per l'accesso o la registrazione di informazioni (in particolare i cd. "*cookie*" sul terminale dell'utente, ai sensi dell'art. 5(3) della Direttiva n. 2002/58/CE (direttiva "*e-privacy*") come modificata dalla Direttiva n. 2009/136/CE.

In base all'art. 5(3) della Direttiva n. 2002/58/CE, il previo consenso non è richiesto se il *cookie* serve al solo scopo di veicolare la trasmissione di una comunicazione sulla rete, oppure se "strettamente necessario" alla fornitura di un servizio della società dell'informazione richiesto espressamente dall'utente/contraente. Va sottolineato che l'art. 5(3) menziona il diritto a conoscere preventivamente ed autorizzare l'accesso o la registrazione di "informazioni" sul proprio terminale (si pensi, ad es., a programmi *spyware* o ad altre forme di intervento illecito sul terminale dell'utente/contraente). L'analisi dettagliata condotta nel parere evidenzia come, sostanzialmente, i *cookie* impiantati nel terminale dell'utente/contraente direttamente dal titolare del singolo sito web (cd. "*first-party cookies*") non necessitano del previo consenso se non sono utilizzati per altri scopi come *cookie* di sessione utilizzati per "riempire il carrello" in caso di acquisti *online*; quelli utilizzati per contenuti multimediali tipo *flash player* se non superano la durata della sessione, ed infine quelli di personalizzazione linguistica. Viceversa, per i *cookie* impiantati da "terze parti" (diverse dal titolare), in particolare per scopi di natura pubblicitaria, permane l'esigenza del consenso perché essi non soddisfano nessuno dei due requisiti sopra ricordati, come già segnalato dal Gruppo Art. 29 in precedenti pareri sul tema "pubblicità comportamentale" (*Behavioural Advertising* - v. Relazione 2011 p. 192). Anche i *cookie* utilizzati per fini di analisi degli accessi o delle visite al proprio sito (*analytics cookies*) non richiedono il previo consenso se perseguono esclusivamente scopi statistici e raccolgono informazioni in forma aggregata, a condizione che l'informativa fornita dal sito web sia chiara e adeguata e si offrano agli utenti modalità semplici per opporsi al loro impianto (*opt-out*, meccanismi di anonimizzazione). Il parere ricorda che, in caso di dubbio sull'applicabilità dell'esonero, è preferibile chiedere il consenso degli utenti/contraenti, al fine di garantire la liceità dei trattamenti svolti.

Mobile apps (applicazioni per telefonia mobile)

Nel 2012 il Gruppo ha lavorato alla predisposizione di un parere sulle *mobile apps* (applicazioni per telefonia mobile), in particolare esaminando gli obblighi e le raccomandazioni

da rivolgere ai diversi soggetti coinvolti nella creazione e distribuzione di tali applicazioni (sviluppatori, rivenditori/distributori, produttori dei sistemi operativi e degli apparecchi di telefonia mobile, soggetti terzi quali i fornitori di pubblicità o servizi di analisi). È stata in particolare evidenziata la mancanza di consapevolezza degli utenti sul trattamento dei loro dati, specie sensibili, da parte di soggetti terzi (si pensi al caso dei dati sanitari caricati con un'*app* sanitaria o alle informazioni bancarie che vengono comunicate ad un *app store*, o alle informazioni di localizzazione). Lo schema di parere evidenzia, quindi, da un lato le deficienze del sistema di sviluppo, produzione e distribuzione delle *app*, scarsa trasparenza per quanto riguarda le finalità dei trattamenti, l'assenza di un vero consenso da parte degli utenti finali; l'insufficienza delle misure di sicurezza; la tendenza alla "massimizzazione dei dati" e l'eccessiva elasticità degli scopi per i quali si procede a trattamenti ulteriori dei dati personali raccolti. Dall'altro canto, si richiamano i diversi soggetti coinvolti alle rispettive responsabilità. In primo luogo, gli sviluppatori di *app,* che devono ottenere il previo consenso degli interessati (specifico, informato, revocabile) e raccogliere solo i dati necessari per la funzionalità prescelta. Gli sviluppatori hanno un ruolo da svolgere anche nel promuovere buone prassi attraverso il "*rating*", cioè l'assegnazione di un punteggio di valutazione delle proprie *app*, sulla base dei meccanismi di *privacy* e sicurezza disponibili quali una *privacy policy* comprensibile e di facile accessibilità, nonché meccanismi a misura di utente per esercitare i diritti riconosciuti dalla direttiva e dal Codice. In tal modo gli interessati sarebbero sensibilizzati rispetto alla scelta delle *app*, che avverrebbe anche in base a quanto un'*app* sia "a misura di *privacy*". Ai distributori di *app* compete di facilitare il compito degli sviluppatori, indirizzando gli utenti verso le informazioni corrette, ed ai produttori di sistemi operativi e dispositivi "*smart*" quello di rendere tecnicamente possibile la realizzazione dei princìpi di trasparenza, correttezza, pertinenza e necessità nonché la raccolta di un consenso cd. "granulare", ossia un consenso adeguatamente modulato in relazione alle specifiche finalità del trattamento. Fondamentale è quest'ultimo requisito anche nei confronti dei soggetti terzi (pubblicitari, fornitori di servizi) che partecipino al sistema *app* a qualunque titolo: ad esempio, i soggetti operanti nel settore pubblicitario devono astenersi dall'invio di annunci pubblicitari estranei al contesto delle *app*, a meno di ottenere il previo consenso inequivocabile dell'utente; quindi non è consentito