dagli interessati volontariamente. L'omessa/inidonea informativa, in alcune ipotesi di comunicazione di dati personali a terzi, è stata contestata sia alla società che, avendo raccolto i dati dell'interessato, li ha poi trasmessi a un *partner* commerciale senza informare l'interessato, sia al *partner* commerciale che, avendoli ricevuti, li ha trattati (ad es., per l'invio di comunicazioni commerciali) senza rendere l'informativa agli interessati nei termini previsti dalle disposizioni. Frequenti anche le contestazioni relative alla mancata predisposizione delle informative in casi di trattamento di dati mediante sistemi di videosorveglianza.

Numerose sono state altresì le sanzioni per illecito trattamento amministrativo di dati personali di cui all'art. 162, comma 2-*bis*, del Codice, soprattutto per violazione dell'obbligo del consenso al trattamento da parte dell'interessato e per omissioni nell'adozione delle misure minime di sicurezza. Per il primo aspetto, le violazioni hanno interessato soprattutto le società che effettuano attività di *marketing* mediante fax, e-mail, *Sms*. Anche a fronte di un'informativa completa, i soggetti sanzionati non avevano documentato il consenso libero e informato degli interessati per tale specifica finalità. Per le misure di sicurezza, la violazione più frequentemente accertata è da ricondurre alla mancata designazione degli incaricati del trattamento, che comporta la non applicazione di tutte le misure di sicurezza che il disciplinare tecnico di cui all'Allegato B. del Codice riconduce all'attività degli incaricati medesimi e, segnatamente, delle regole 1-10 (autenticazione informatica), 12-15 (adozione di un sistema di autorizzazione), 22 e 23 (dati sensibili contenuti in supporti rimovibili), 27 (dati comuni contenuti in supporti cartacei), 28 e 29 (dati sensibili contenuti in supporti cartacei). Al riguardo è opportuno evidenziare che la mancata designazione degli incaricati del trattamento non costituisce un mero inadempimento formale, in quanto la parte più significativa delle misure di sicurezza da adottarsi per il trattamento dei dati personali è strettamente correlata all'attività degli incaricati stessi, (ovvero di coloro che ordinariamente operano sui dati personali) e mira a fornire loro le istruzioni per il corretto trattamento dei dati, rendendoli al contempo consapevoli delle connesse responsabilità anche attraverso il loro inserimento in specifici processi formativi in materia di *privacy* (prescritti dalla regola 19.6 del citato disciplinare tecnico in relazione all'adozione del documento programmatico sulla sicurezza).

Numerose sono state anche le contestazioni nei confronti di coloro che non hanno fornito risposta alle richieste istruttorie fatte dall'Autorità. In questi casi, di massima, oltre alla contestazione della sanzione si è proceduto anche a disporre un accertamento *in loco*, in linea di massima delegato al Nucleo speciale *privacy* della Guardia di finanza, al fine di acquisire i necessari elementi istruttori.

Assai significativi per l'importo della pena pecuniaria (da 60.000 a 180.000 euro), ancorché non particolarmente numerosi, sono invece stati i casi di inosservanza dei provvedimenti del Garante.

In un caso si è trattato di una società che ha contravvenuto al divieto del Garante di inviare comunicazioni commerciali e promozionali senza che risultasse comprovato un consenso libero ed informato degli interessati; in altri casi, invece, non sono stati osservati i provvedimenti relativamente a trattamenti di dati personali tratti da elenchi telefonici. Rilevante infine anche il caso relativo alla violazione, da parte di un'emittente televisiva, di un divieto adottato dal Garante in relazione alla messa in onda di dati personali relativi a casi di adozioni affrontati nel corso delle puntate di una trasmissione televisiva.

Nell'ambito delle attività ispettive effettuate per verificare il rispetto dei termini di conservazione dei dati di traffico telefonico e telematico da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico, sono state rilevate 4 violazioni di quanto previsto dall'art. 132 del Codice, che impone specifici limiti temporali di conservazione di tali dati per finalità di prevenzione e accertamento dei reati.

In un caso il fornitore del servizio conservava dati di traffico dei propri clienti risalenti all'anno 2001, senza aver mai provveduto a cancellarli o introdotto limiti di conservazione.

In un altro caso, la violazione è stata accertata in relazione alla conservazione di dati (l'oggetto dei messaggi di posta elettronica) che non rientravano, sulla base di quanto previsto dall'art. 3 del d.lgs. n. 109/2008, tra quelli da conservare per le finalità di cui all'art. 132 del Codice e che, essendo potenzialmente correlati al contenuto della comunicazione, non potevano essere conservati.

In un terzo caso, è emerso che veniva conservato tra i dati di traffico anche l'indirizzo *IP* di destinazione in relazione alla navigazione Internet effettuata dagli abbonati al servizio,

benché l'art. 3 del d.lgs. n. 109/2008 non includa, tra le categorie di dati da conservare per le finalità di cui all'art. 132 del Codice, tale informazione (anch'essa considerata potenzialmente correlata al contenuto della comunicazione).

Da segnalare infine i primi casi di procedimenti sanzionatori avviati con riferimento alla disposizione contenuta nell'art. 164-*bis*, comma 2, del Codice per le violazioni commesse da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni. Si è trattato di società che hanno commesso reiterate violazioni sanzionate dal Codice, in relazione ad un numero assai rilevante di dati personali organizzati all'interno di banche dati, cedute a terzi per essere utilizzate per finalità di *marketing*. Tali banche dati costituivano un archivio aggiornato di informazioni relative a una quota rappresentativa della popolazione e degli operatori economici presenti nel territorio italiano e, quindi, sono state considerate, sulla base di quanto previsto dall'art. 164-*bis*, comma 2, del Codice "*banche dati di particolare rilevanza o dimensioni*".

Sul nuovo apparato sanzionatorio e sulle disposizioni procedurali si fa rinvio alla *Relazione* 2009, p. 249 ss.

20. Le relazioni internazionali

Sono stati celebrati nel periodo di riferimento il trentennale delle linee-guida dell'OCSE sulla protezione e i flussi transfrontalieri dei dati (adottate il 23 settembre 1980), nonché il trentennale della Convenzione 108 del Consiglio d'Europa (adottata il 28 gennaio 1981).

Tale ricorrenza ha costituito una preziosa occasione di riflessione, per verificare se gli strumenti e le strategie operativi dall'inizio degli anni '80, ma concepiti negli anni '70, possano considerarsi ancora attuali, anche alla luce del profondo mutamento istituzionale e normativo nell'Unione europea conseguente all'entrata in vigore del Trattato di Lisbona e ai lavori in corso per la revisione della Direttiva n. 95/46/CE.

Come già indicato nella precedente *Relazione* annuale (p. 253), con il Trattato di Lisbona la protezione dei dati personali ha acquisito un nuovo e diverso ruolo: da un lato, le disposizioni della Carta dei diritti fondamentali –che, com'è noto, hanno introdotto il diritto fondamentale delle persone alla tutela dei propri dati personali (art. 8), affiancandolo al diritto alla riservatezza (art. 7)– sono divenute giuridicamente vincolanti; dall'altro, è emersa l'esigenza di pervenire ad un quadro uniforme di princìpi, come previsto dall'art. 16 del Trattato sul funzionamento dell'Unione europea, pur con i contemperamenti previsti dalle dichiarazioni allegate al Trattato.

La Commissione europea ha adottato, il 4 novembre 2010, la Comunicazione intitolata "*Un approccio globale alla protezione dei dati personali in Europa*" in cui traccia le linee di fondo secondo le quali intende articolare il proprio intervento, anche con il conforto dell'esperienza delle autorità di protezione dei dati riunite nel Gruppo Art. 29, nell'intento di presentare, entro il primo semestre del 2011, la proposta di revisione della Direttiva n. 95/46/CE.

Le innovazioni tecnologiche e il mutato scenario economico-sociale (impatto delle nuove tecnologie quali il *cloud computing*; l'accentuata globalizzazione nel trasferimento dei dati; l'utilizzo di tecniche di *behavioural advertising* sempre più sofisticate) oltre che le già menzionate innovazioni del quadro giuridico determinano, ad avviso della

Commissione, l'esigenza di mettere a punto una cornice normativa coerente e comune per il trattamento di dati personali nel contesto di tutte le politiche dell'Unione europea.

Fondamentali saranno, pertanto, gli interventi sulle definizioni contenute nella direttiva, quali la definizione di "*dato personale*" (che potrebbe includere i dati sulla geo-localizzazione ed altri non ancora contemplati dalla direttiva), nonché di "*dato sensibile*" e di "*consenso informato*". Ciò al fine di assicurare la certezza del diritto per i titolari del trattamento e gli interessati; di aumentare il grado di trasparenza che i titolari del trattamento devono garantire agli interessati –eventualmente anche estendendo l'obbligo (previsto dalla Direttiva e-*privacy* n. 2002/58/CE di recente modificata) di segnalazione delle violazioni degli obblighi in materia di protezione dati da cui possano derivare danni agli interessati ("*general personal data breach notification*")– di permettere un controllo più effettivo, da parte degli stessi interessati sul trattamento dei propri dati (diritto di accesso, rettifica, blocco, cancellazione) e di assicurare che vengano comminate sanzioni adeguate in caso di violazione della normativa posta a presidio della *privacy*.

Da un punto di vista più generale, la proposta della Commissione si prefigge alcuni importanti obiettivi quali: la riforma del quadro regolamentare che garantisca maggiore armonizzazione tra le normative nazionali di recepimento; la revisione e semplificazione del sistema di notifica; la certezza giuridica in merito al diritto nazionale applicabile; l'osservanza delle norme da parte dei titolari del trattamento, anche attraverso sistemi di controllo e responsabilità interni (*cd.* "*accountability*").

Quanto al trattamento dati nell'ambito della cooperazione di polizia e giudiziaria in materia penale, la Comunicazione ha sottolineato che la Decisione-quadro 2008/977/GAI del Consiglio presenta non poche criticità (applicazione limitata ai dati trasmessi nell'ambito della cooperazione tra Stati membri, e non estesa a trattamenti meramente interni ad uno stesso Stato membro; armonizzazione di tipo "minimo"; problemi di coerenza con altri strumenti legislativi). La riforma del quadro regolamentare si propone di superare tali criticità estendendo, per quanto possibile e tenuto conto delle specificità del settore, le regole generali previste dalla novellata direttiva.

In materia di trasferimento dei dati extra-UE –uno dei temi più critici– la proposta ha

come obiettivo il riesame delle procedure per la valutazione del livello di "adeguatezza" degli Stati terzi ("*adequacy procedure*"), l'introduzione e disciplina delle clausole contrattuali *standard* e delle "norme vincolanti d'impresa" (BCR) per i trasferimenti infragruppo, il rafforzamento della cooperazione con organismi internazionali attivi sullo stesso tema (OCSE, Consiglio d'Europa, Nazioni Unite).

La Commissione ha altresì indicato la necessità, per una applicazione effettiva delle norme di protezione dei dati, di un rafforzamento dell'assetto istituzionale, ribadendo l'essenzialità del ruolo delle autorità nazionali di protezione dei dati personali istituite dall'art. 28 della Direttiva n. 95/46/CE, cui deve essere garantita, come di recente indicato dalla Corte di giustizia UE (sentenza 9 marzo 2010, in C-518/07, Commissione contro Repubblica federale di Germania) piena indipendenza ed attribuiti competenze, poteri e mezzi adeguati alle funzioni da svolgere. In merito al coordinamento delle autorità nazionali di protezione dati, oggi svolto dal Gruppo Art. 29, la Commissione ha menzionato la possibile istituzione di una procedura per assicurare la coerenza del coordinamento medesimo nel mercato interno sotto l'autorità della stessa Commissione.

Il lavoro del Gruppo Art. 29, come più diffusamente indicato *infra* (par. 20.2.) ha registrato un'ulteriore crescita, grazie all'ampliamento delle competenze anche ai trattamenti dei dati nell'area dell'ex *cd.* "terzo pilastro".

Occorre inoltre evidenziare il maggiore ruolo riconosciuto al Parlamento europeo, anche in ragione dei nuovi poteri attribuitigli dal Trattato di Lisbona, e la concreta possibilità di scambi diretti di informazioni e opinioni tra le autorità di protezione dei dati personali riunite nel Gruppo Art. 29.

I contributi forniti dal Parlamento hanno riguardato in particolare accordi internazionali in settori particolarmente delicati, quali l'accordo Unione europea-Stati Uniti per l'uso dei dati *Swift*, nonché il rinnovo degli accordi con Stati Uniti, Australia e Canada concernenti l'uso dei dati personali dei passeggeri aerei ("*Passenger name records*" - *PNR*).

L'entrata in vigore del Trattato di Lisbona ha comportato, altresì, il progressivo e sempre maggiore coinvolgimento dei parlamenti nazionali nella *cd.* "*fase ascendente*" del procedimento legislativo comunitario. I parlamenti nazionali, infatti, avvalendosi, in particolare,

dei poteri ad essi conferiti dall'art. 12 del Trattato sull'Unione europea e dal Protocollo sul ruolo dei parlamenti nazionali nell'Unione europea, potranno valutare con maggiore incisività il rispetto dei princìpi di sussidiarietà e di proporzionalità di ogni proposta legislativa, ivi incluse quelle che abbiano un impatto sul diritto alla protezione dei dati personali.

20.1. LE CONFERENZE DELLE AUTORITÀ SU SCALA INTERNAZIONALE

Conferenza internazionale delle autorità di protezione dati Gerusalemme 2010

La Conferenza internazionale si è tenuta a Gerusalemme dal 27 al 29 ottobre 2010; la parola chiave è stata "*Generazioni*", riferita sia alle "nuove generazioni" di utenti della Rete, sia alle tecnologie e regole di "nuova generazione", specie in relazione allo sviluppo della "*privacy by design*". Le autorità di protezione dati e alcuni rappresentanti della comunità scientifica si sono confrontati sui cambiamenti provenienti dal *cyberspazio*. Particolare attenzione è stata rivolta alla percezione della *privacy* da parte degli utenti della Rete più giovani. Una serie di sessioni a tema, organizzate parallelamente a quella plenaria, hanno riguardato i temi dell'*accountability*, della protezione dei dati *online*, del *cd.* "Internet delle cose" ("*Internet of things*"), del rapporto tra la *privacy* e la tutela dei diritti di autore e dei consumatori, del *cd.* "*diritto all'oblio*" ("*right to be forgotten*"), nonché dell'accesso dei governi ai dati in possesso di soggetti privati.

Al Garante italiano è stato affidato il compito di presiedere la sessione dedicata al consenso come presupposto legittimante l'uso dei dati personali. Punto di partenza del dibattito è stata la necessità di ripensare il consenso –sia nel mondo *offline*, sia in Internet– affinché esso continui ad avere un ruolo realmente efficace nel sistema di protezione dei dati. Il Presidente dell'Autorità ha sottolineato che, nell'ambito dei servizi *online*, sembra prevalere l'orientamento per cui all'interessato viene chiesto di esprimere un consenso basato non su un'informativa completa, relativa ai diversi aspetti del trattamento, bensì su un'informativa che si limita a indicare le misure adottate per garantire la sicurezza dei dati. Tale tendenza appare del resto in linea con la recente adozione, ispirata al principio della "*privacy by design*", di misure di protezione direttamente inserite nell'ambito delle diverse tecnologie in uso (soprattutto per quanto riguarda Internet, ovvero di sistemi di *cd.* "*privacy default setting*", impostazioni orientate sin dall'inizio al rispetto delle regole di

protezione dati). In tale contesto, il ruolo delle autorità di protezione dati dovrà estendersi alla individuazione di misure di sicurezza e modalità *standard* di erogazione di servizi idonee a garantire un'elevata tutela dei diritti degli utenti.

Nella sezione riservata alle sole autorità di protezione dei dati accreditate, sono state discusse le risoluzioni ed i *report* sottoposti alla Conferenza per l'adozione, nonché i risultati di un'indagine focalizzata sulle esperienze delle autorità nazionali, con specifico riferimento ai rapporti (di collaborazione e/o conflitto) con altre autorità di regolazione. È stato deciso di ammettere come membro della Conferenza la *Federal Trade Commission* statunitense e le autorità di protezione dati della Repubblica moldava, di Albania, Bulgaria, Messico nonché, senza diritto di voto, l'Autorità comune di controllo (*Joint Supervisory Body*) di EUROJUST. Sono state adottate nuove regole di accreditamento alla Conferenza ed è stata decisa l'istituzione di un comitato esecutivo ad *interim* per proseguire il lavoro intrapreso affinché la Conferenza stessa assuma una più stabile struttura organizzativa.

La Conferenza si è conclusa con l'adozione, in particolare, di una risoluzione promossa dall'Autorità francese di protezione dati, con la quale si chiede la convocazione di una conferenza intergovernativa per adottare i princìpi internazionali in materia di *privacy* approvati a Madrid lo scorso anno. È stata altresì adottata la risoluzione, promossa dall'Autorità canadese, sulla "*privacy by design*", presentata come una vera e propria impostazione di carattere generale, da includere nella configurazione e nella gestione delle tecnologie e dei sistemi dell'informazione. Al riguardo sono stati individuati alcuni princìpi fondamentali, quali la necessità di un atteggiamento preventivo e non "rimediale" rispetto alla protezione dei dati, l'introduzione di impostazioni *pro privacy* incorporate nel *design* delle tecnologie adoperate, la visibilità e la trasparenza, il rispetto per la *privacy* dell'utente.

La risoluzione si conclude con un invito alle autorità di protezione dei dati a fornire un contributo attivo nella diffusione della "*privacy by design*", in particolare attraverso apposite campagne di sensibilizzazione, al fine di incoraggiare la ricerca su tali tecniche e promuovere l'introduzione di tale concetto nella formulazione delle *privacy policy* e della relativa normativa.

Spring Conference 2010

Il 29 e 30 aprile si è svolta la consueta Conferenza di primavera dei garanti europei della protezione dei dati, quest'anno ospitata dall'Autorità ceca a Praga.

La Conferenza, che sin dal titolo ha sottolineato l'intenzione di "guardare al futuro, soppesando il passato", si è aperta con una sessione dedicata al tema "Internet delle cose" ("*Internet of things*") ed alla costante tracciabilità degli interessati, derivante dall'utilizzo delle nuove tecnologie.

Nella seconda sessione, dedicata ai minori ed alle reti sociali, diverse autorità hanno illustrato le attività intraprese per meglio comunicare con gli utenti più giovani sviluppando linguaggi accessibili ed efficaci.

Il tema centrale, affrontato nel corso della sessione presieduta dal Presidente del Gruppo Art. 29, è stato la protezione dei dati personali nel contesto attuale, nel quale tali diritti sono normativamente rafforzati (anche in virtù del riconoscimento come diritti fondamentali ai sensi del Trattato di Lisbona) ma, al contempo, sono di fatto affievoliti dalle criticità determinate dal "dominio" di soggetti internazionali e dai mutamenti tecnologici. Una particolare riflessione ha riguardato il ruolo del settore pubblico rispetto al trattamento dei dati. Il Presidente del Garante ha introdotto il tema del rapporto tra diritto di accesso e diritto alla riservatezza facendo riferimento ai diversi modelli di amministrazione e ai diversi gradi di trasparenza che possono accompagnare lo svolgimento di attività pubbliche.

Un *panel* specifico è stato poi dedicato alla profilazione su base etnica ed ai punti di contrasto con i princìpi di protezione dei dati personali.

Nel corso della Conferenza le autorità hanno accolto la richiesta di partecipazione presentata dall'Autorità di protezione dati albanese ed hanno preso atto della sussistenza di richieste analoghe, che saranno valutate in occasione della prossima conferenza, da parte della competenti autorità di Bosnia Erzegovina e Moldavia.

La Conferenza ha adottato quattro risoluzioni. La prima, sul futuro della protezione dei dati e della *privacy*, richiama i princìpi fondamentali in materia e chiede un'attenzione particolare agli effetti della globalizzazione e delle nuove tecnologie su tali diritti. La risoluzione, nel prendere atto del crescente ricorso –per finalità di contrasto del terrorismo

e di altri fenomeni di criminalità– a dati raccolti originariamente per finalità diverse, conferma la necessità che i titolari verifichino che i trattamenti siano basati sul consenso, laddove legittimo, e avvengano in conformità a quanto previsto da basi legali idonee, nonché alle condizioni rigorose poste dal legislatore per regolare l'"uso secondario" dei dati. La risoluzione chiede anche che ogni iniziativa legislativa e l'introduzione di nuove tecnologie sia preventivamente sottoposta ad una valutazione di impatto sulla *privacy* ed accompagnata da misure di "*privacy by design*" che riducano il più possibile l'interferenza sulla *privacy*.

La Conferenza ha altresì rinnovato la richiesta di stabilire un corpo omogeneo di regole e *standard* internazionali –che includa i trattamenti di dati per finalità di polizia e giustizia– richiamando quelli adottati a Madrid nella Conferenza internazionale del 2009 e la Convenzione del Consiglio d'Europa.

Altre due risoluzioni hanno riguardato l'uso dei "*body scanner*" negli aeroporti, evidenziando l'esigenza di rispettare i princìpi di necessità e proporzionalità, anche con riferimento al possibile negoziato per concludere un accordo sulla protezione dei dati tra Unione europea e Stati Uniti.

Un'altra risoluzione indica la necessità di azioni comuni, a livello europeo ed internazionale, per educare e rendere consapevoli le nuove generazioni. La risoluzione invita le autorità di protezione dei dati, anche attraverso azioni coordinate, a sviluppare strumenti idonei a proteggere la *privacy* dei giovani e a stimolare l'adozione da parte dei titolari del trattamento di "*privacy policy*" semplici e comprensibili. Sono state inoltre incoraggiate le azioni dei governi dirette ad adottare iniziative specifiche per rafforzare la tutela dei giovani, anche tramite campagne di informazione e di educazione.

Nell'ambito dei lavori dedicati all'attività svolta dal Gruppo di lavoro polizia e giustizia (*Working Party on Police and Justice - WPPJ*; v. *infra*) la *Spring Conference* ha approvato, dopo la presentazione svolta da Francesco Pizzetti, presidente del *WPPJ*, i documenti presentati, ed in particolare il Rapporto annuale di attività per l'anno 2009, il progetto di raccomandazioni in materia di misure attuative della Convenzione sulla criminalità informatica del Consiglio d'Europa, il progetto di decisione relativa ad una politica coordinata

di controllo (attuativa del "manuale" approvato nel corso della precedente Conferenza di primavera), il progetto di decisione relativa all'inserimento di una clausola *standard* di protezione dati negli accordi bilaterali con Paesi extraeuropei in materia di "*law enforcement*", la bozza di risoluzione proposta dall'Autorità di protezione dati tedesca a complemento del lavoro svolto dal *WPPJ* (e dal Gruppo Art. 29) con la predisposizione delle osservazioni per la consultazione aperta dalla Commissione europea sul possibile contenuto di un accordo Unione europea - Stati Uniti sui princìpi in materia di trattamento dei dati personali.

20.2. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

Il Gruppo Art. 29, mantenendo il suo ruolo di stimolo e di attivo interlocutore delle istituzioni comunitarie, *in primis* della Commissione europea, ha attivamente contribuito al dibattito in materia di valutazione dell'attualità della Direttiva n. 95/46/CE e ai lavori preparatori per la possibile revisione della stessa.

Più in generale, il Gruppo ha analizzato sia il quadro giuridico vigente –per un'applicazione più coerente e corretta dei princìpi di protezione dei dati– sia le nuove sfide connesse allo sviluppo tecnologico, alla globalizzazione e al mutato scenario istituzionale dell'Unione europea conseguente all'entrata in vigore del Trattato di Lisbona.

Tale impegno risulta dal programma di lavoro 2010-2011 (WP 170), che si articola secondo quattro direttive fondamentali: 1) assicurare la corretta applicazione del quadro giuridico vigente e preparare quello futuro (attraverso l'interpretazione delle disposizioni chiave della Direttiva n. 95/46/CE, l'attuazione della direttiva e-*privacy*, recentemente modificata dalla Direttiva n. 2009/136/CE, la valutazione delle conseguenze dell'entrata in vigore del Trattato di Lisbona); 2) affrontare la globalizzazione intervenendo sulla disciplina relativa ai flussi transfrontalieri di dati personali, ovvero sulle "norme vincolanti d'impresa" ("*binding corporate rules*"), sull'attuazione degli accordi di "approdo sicuro" ("*Safe Harbor*"), nonché sulla valutazione di adeguatezza dei Paesi terzi e partecipando ai lavori sulla standardizzazione; 3) rispondere alle *cd.* "sfide tecnologiche", dedicando particolare attenzione alle tematiche del "*cloud computing*", dei "motori di ricerca" (in

particolare, le garanzie del "diritto all'oblio" rispetto all'utilizzo dei sistemi di ricerca *online*) dei servizi di *social network*; 4) migliorare l'efficacia dell'azione di *enforcement* del Gruppo Art. 29 e delle autorità per la protezione dei dati, sviluppando i metodi d'indagine delle autorità nazionali e promuovendo strumenti e forme di cooperazione tra di esse.

Nell'affrontare i molteplici impegni evidenziati, ivi compresa l'interpretazione del diritto vigente, particolare attenzione è stata dedicata al concetto di legge applicabile. In merito è stato adottato il parere WP 179 del 16 dicembre 2010 (v. *infra*) che ha affrontato i principali problemi interpretativi posti dai criteri di territorialità previsti dalla Direttiva n. 95/46/CE, soprattutto con riferimento a situazioni in cui l'attività di trattamento dei dati sia effettuata nel territorio di più Stati membri. Tale lavoro si è basato sull'attività di approfondimento intrapresa nel corso del 2009, conclusasi nel febbraio 2010 con l'adozione di un importante e documentato parere (WP 169 del 16 febbraio 2010, v. *infra*).

Sempre con riferimento all'interpretazione della Direttiva n. 95/46/CE, il Gruppo ha altresì iniziato ad esaminare il tema del "consenso" dell'interessato nel sistema delle garanzie per la protezione dei dati, per precisare fino a che punto lo stesso possa legittimare al trattamento dei dati personali, tenendo anche conto dei servizi di comunicazione elettronica, caratterizzati da asimmetrie informative tra operatori economici e utenti e dalle difficoltà pratiche legate alla manifestazione del consenso *online*.

In merito all'attività volta alla revisione della direttiva ed all'individuazione delle sfide poste dal mutato scenario istituzionale e tecnologico, hanno costituito oggetto di particolare attenzione da parte del Gruppo Art. 29 i seguenti aspetti, già rappresentati in sintesi nel "*Contributo alla consultazione pubblica sul futuro della protezione dati*" WP 168 del 1° dicembre 2009 (v. *Relazione* 2009, p. 264): 1) la disciplina delle categorie particolari di dati (*cd.* "dati sensibili"); 2) il sistema di notificazione, delineato dall'art. 18 della direttiva, soprattutto per una possibile semplificazione; 3) le forme di cooperazione tra le autorità di protezione dei dati, previste dall'art. 28, par. 6, della direttiva.

Del parere del Gruppo Art. 29 sui temi fin qui richiamati terrà conto la Commissione europea nell'elaborazione della proposta di revisione della Direttiva n. 95/46/CE, prevista entro la fine del primo semestre del 2011.

In proposito si rileva, da un lato, che per quanto concerne la semplificazione degli oneri di notificazione, l'individuazione di un denominatore comune tra le posizioni espresse dalle autorità nazionali dovrebbe consentire di pervenire all'adozione del relativo parere nel corso della prima parte del 2011, dall'altro, che il tema della cooperazione tra autorità nazionali di protezione dei dati, soprattutto nella prospettiva di individuare strumenti di coordinamento e di collaborazione in relazione alle tematiche di rilevanza transnazionale o alle ipotesi in cui giurisdizione e legge applicabile non coincidano, presenta non poche criticità (prima tra tutte, i diversi poteri, anche sanzionatori, delle suddette autorità).

Con riferimento all'attività di *Google* sul territorio di diversi Stati membri nell'ambito del servizio "*Street View*", il lavoro svolto attraverso il coordinamento delle posizioni e delle azioni delle autorità nazionali nell'ambito del Gruppo Art. 29, ha costituito un emblematico esempio di efficace cooperazione tra autorità nazionali di protezione dati. Infatti, la circostanza che le operazioni di raccolta e trattamento dei dati effettuate da *Google* siano state indagate e valutate da parte di più autorità nazionali ha reso sicuramente opportuno l'intervento del Gruppo Art. 29 nell'attività di *enforcement*, pur nel rispetto delle specificità dei singoli casi e delle normative nazionali applicabili. Allo scopo di coordinare e uniformare le risposte alle eventuali violazioni della *privacy*, il Gruppo Art. 29 ha raccolto dalle singole autorità nazionali informazioni relative alle esperienze di monitoraggio, ed ha posto in essere un'analisi congiunta per comprendere la natura e la tipologia dei dati raccolti e trattati da *Google*, soprattutto con riferimento alle possibilità di controllo continuo delle reti *Wi Fi* effettuato nel corso della raccolta di immagini per il servizio *Street View*.

È altresì stata sottolineata l'importanza delle problematiche connesse all'uso delle tecnologie informatiche, soprattutto in relazione all'utilizzo di reti *wireless* o sistemi *GPS*, in grado di localizzare la posizione dell'individuo e monitorarne gli spostamenti.

Dopo una accurata analisi è stato adottato dal Gruppo Art. 29 un parere dedicato alla *cd.* "pubblicità comportamentale", quale forma invasiva di *marketing* fondato sulla profilazione degli utenti in rete. A questo ha fatto seguito un'attività di consultazione dei principali operatori del settore, in merito agli aspetti tecnici richiamati nel documento succitato (*Parere*

2/2010 sulla pubblicità comportamentale *online* - WP 171, v. *infra*; "*Letter from the Article 29 Working Party addressed to the Ad Network Providers*" e "*Letter from the Article 29 Working Party addressed to the Browser Providers*", entrambe del 29 ottobre 2010, v. *infra*).

Sempre con particolare attenzione al settore degli scambi di dati in un contesto dal carattere marcatamente commerciale, sono state approfondite le tematiche legate ai flussi transfrontalieri di informazioni, sia attraverso la semplificazione del sistema di adozione delle "norme vincolanti d'impresa" ("*binding corporate rules*") ad uso delle società di carattere multinazionale, sia tramite l'estensione della platea dei Paesi terzi considerati adeguati (WP 177 in merito all'adeguatezza dell'Uruguay, v. *infra*).

La crescente importanza della circolazione dei dati personali nell'ambito del mercato globalizzato, inoltre, ha indotto il Gruppo ad esaminare il concetto di "*accountability*" (inteso come regola complessiva di responsabilità ed impegno assunta dal titolare del trattamento, che permea l'intera organizzazione aziendale al rispetto dei princìpi di protezione dei dati) e ad esprimersi in modo favorevole all'introduzione di tale principio nel nuovo quadro giuridico europeo di protezione dei dati, con il parere del 13 luglio 2010 (WP 173, v. *infra*).

Il Gruppo ha poi continuato ad occuparsi del trasferimento e trattamento di dati finanziari, soprattutto in relazione al perdurante accesso del "*US Department of Treasury*" ai dati contenuti nel *database* di *Swift*. Per consentire l'accesso a questi dati da parte degli Stati Uniti è stato infatti negoziato dalla Commissione un accordo sulla trasmissione dei dati di messaggistica finanziaria tra Unione europea e Stati Uniti, direttamente vincolante per gli Stati membri dell'UE a partire dal 1° agosto 2010 (Accordo *cd.* "*TFTP2*" –"*Terrorist Finance Tracking Program*"– di cui alla Decisione del Consiglio del 13 luglio 2010, pubblicata nella *G.U.U.E.* L 195 del 27 luglio 2010).

Parimenti approfondito è stato l'esame, anche con rappresentanti del settore finanziario e della Direzione generale mercato interno della Commissione europea, dell'impatto, in materia di protezione dei dati, delle direttive antiriciclaggio e per la prevenzione del finanziamento del terrorismo, in particolare con riferimento all'applicazione della normativa nazionale di recepimento.

Continua e costante attenzione è stata mantenuta riguardo al trattamento dei dati dei passeggeri in relazione all'obbligo per i vettori aerei di fornire in anticipo, e a pena di sanzioni, dati di prenotazione ed altri dati identificativi del passeggero alle autorità competenti dei Paesi di destinazione. Sono in corso di rinegoziazione, da parte della Commissione, accordi al fine di regolare l'uso di tali dati da parte, al momento, degli Stati Uniti, del Canada e dell'Australia.

Il Gruppo Art. 29 ha valutato l'approccio generale da seguire per la salvaguardia dei requisiti posti dalla legislazione in materia di protezione dei dati personali nella negoziazione di tali accordi (Parere 7/2010 sulla comunicazione della Commissione europea sull'approccio globale ai trasferimenti di dati *PNR* verso Paesi terzi (WP 178, v. *infra*), formulando considerazioni anche con riferimento alla possibile adozione di un sistema di trattamento dei dati "*Passenger Name Records*" (*PNR*) europeo, nonché con riferimento al programma "*Electronic System for Travel Authorization*" (*ESTA*) adottato dagli Stati Uniti ed alla possibile adozione di un sistema *ESTA* europeo.

Sul lato *enforcement* l'Autorità ha coordinato, in qualità di *rapporteur*, l'azione comune sull'applicazione della direttiva europea in materia di conservazione dei dati di comunicazione elettronica a fini di prevenzione e contrasto della criminalità (Direttiva n. 2006/24/CE, *cd.* "*direttiva Frattini*") ed ha redatto la sintesi e le raccomandazioni per la valutazione del Gruppo.

Il Gruppo Art. 29 ha adottato il *report* nella forma di parere (*Report 01/2010 on the second joint enforcement action* - WP 172 del 13 luglio 2010, v. *infra*) e lo ha presentato pubblicamente, anche in occasione della Conferenza del 3 dicembre 2010, organizzata dalla Commissione europea per analizzare in dettaglio i punti fondamentali della direttiva.

Il lavoro, che ha evidenziato la non uniforme, e talvolta anche non corretta, applicazione delle disposizioni della direttiva "*data retention*" da parte degli Stati membri, ha determinato forti prese di posizione da parte delle autorità di protezione dati in merito alla necessità di modifiche della stessa, anche alla luce delle sentenze adottate dalle corti costituzionali di diversi Paesi, e non mancherà di influenzare il Rapporto che la Commissione deve presentare sull'applicazione della direttiva.

Infine, sono stati istituiti nuovi gruppi di lavoro o ricostituiti sottogruppi che avevano già svolto i compiti originariamente previsti dai rispettivi mandati. È il caso specifico del gruppo "*Health data*", del sottogruppo "*e-Government*" e del gruppo di lavoro "*Biometrics*".

Al primo è stato attribuito lo studio dell'impatto *privacy* del progetto "*European Patient Smart Open Services*" (*epSOS*), relativo alla trasmissione dei dati sanitari concernenti uno stesso paziente tra Stati membri dell'Unione europea, con il principale compito di esaminare la normativa e la prassi degli Stati membri che prevedono la registrazione elettronica di dati sanitari.

Al sottogruppo "*e-Government*" è stato dato mandato di analizzare gli aspetti di protezione dei dati personali legati al progetto *STORK*, volto a creare una piattaforma interattiva per lo scambio di informazioni relative all'identità dei cittadini con prevalente applicazione nel settore dell'*e-Government*. Il programma dovrebbe consentire l'accesso *online*, mediante semplice presentazione delle credenziali identificative del soggetto (*cd.* "*eID*"), a servizi per lo più di carattere amministrativo, in tutta l'Unione europea.

Infine, al gruppo "*Biometrics*" spetterà il compito di procedere all'aggiornamento del documento di lavoro sulla biometria (WP 80), adottato dal Gruppo il 1° agosto 2003, anche in considerazione del crescente utilizzo dei dati biometrici negli Stati membri, da parte di operatori sia pubblici che privati.

Di alcuni dei pareri e documenti citati in questo paragrafo si dà di seguito un sintetico resoconto, raggruppandoli in base ai temi trattati:

a. Interpretazione della Direttiva n. 95/46/CE

Parere 1/2010 sui concetti di titolare e responsabile (WP 169)

Il Gruppo ha analizzato la definizione di "titolare" ("*data controller*") del trattamento dei dati, e la sua interazione col soggetto responsabile ("*data processor*"), figure centrali nell'applicazione della Direttiva n. 95/46/CE (per ciò che riguarda l'individuazione del soggetto che risponde dell'osservanza delle norme di protezione dei dati, la determinazione della legge applicabile, l'individuazione del soggetto di fronte al quale gli interessati possono esercitare i loro diritti). Il parere non tiene conto della terza figura soggettiva (l'incaricato) prevista dalla normativa italiana, la cui individuazione non ha fino ad ora posto particolari problematiche, trattandosi