19 L'attività ispettiva e le sanzioni

19.1. *La programmazione dell'attività ispettiva*

L'Autorità ha proseguito, anche nell'anno 2007, il processo di sviluppo dell'attività ispettiva, già avviato nell'anno 2006. L'attività di controllo è stata essenzialmente volta a:

- incrementare il numero delle verifiche;
- sviluppare nuove metodologie di controllo attraverso l'integrazione, nei *team* ispettivi, di competenze tecniche specialistiche per l'esecuzione di accessi ai sistemi informatici e alle banche dati elettroniche;
- sperimentare controlli per categorie omogenee di titolari del trattamento secondo una metodologia predefinita denominata "a progetto".

Sotto il primo profilo, nell'anno 2007 si è registrato un ulteriore importante incremento delle attività (+30% rispetto al 2006) in linea con la tendenza generale di aumento dell'attività di controllo, già evidenziata negli anni precedenti.

Anno	2002	2003	2004	2005	2006	2007
Ispezioni	40	69	100	230	350	452

Delle quattrocentocinquantadue attività ispettive effettuate, trecentosettanta riguardano l'attuazione di programmi ispettivi semestrali disposti dall'Autorità e ottantadue esigenze istruttorie connesse a reclami, segnalazioni e ricorsi presentati dai cittadini.

Grande importanza riveste l'attività di prevenzione effettuata attraverso accertamenti *cd.* "di iniziativa", avviati d'ufficio dall'Autorità (anche in assenza di specifici atti di impulso da parte dei cittadini quali segnalazioni, reclami o ricorsi), che ha costituito la parte più consistente dell'attività di controllo (oltre l'80%).

Il Collegio determina, con cadenza semestrale, le linee di indirizzo dell'attività ispettiva di iniziativa dell'Ufficio attraverso deliberazioni di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire per il semestre e, sulla base di tali indirizzi, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo. Le linee generali della programmazione dell'attività ispettiva vengono rese pubbliche.

Questa impostazione consente, attraverso verifiche nei confronti di più soggetti operanti nello stesso settore o che effettuano tipologie omogenee di trattamento, di acquisire importanti elementi di valutazione in ordine:

- al grado di adeguamento alla legge da parte degli operatori appartenenti a un determinato settore o che utilizzano i dati personali per particolari finalità;
- a fenomeni di ampia portata che possono costituire presupposto per l'adozione di provvedimenti generali (diretti, cioè, ad un insieme indeterminato di operatori);
- alla verifica dell'impatto dei provvedimenti adottati.

Ne deriva così una valorizzazione dell'attività di controllo come strumento di governo del sistema in un'ottica non solo repressiva, ma anche conoscitiva e di indirizzo.

Nell'anno 2007 il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, fosse indirizzata ad accertamenti su profili di interesse generale per categorie di interessati nell'ambito di:

- trattamenti di dati personali effettuati da *call center* per conto di operatori telefonici;
- trattamenti di dati personali effettuati da società farmaceutiche, in relazione alla somministrazione di farmaci e prestazioni sanitarie e alla sponsorizzazione di attività di cura o di ricerca, con particolare riguardo all'informativa agli interessati e al consenso eventualmente necessario;
- trattamenti di dati personali effettuati da compagnie telefoniche con riferimento ai *cd.* "dati di traffico".

Con riferimento, invece, al periodo luglio-dicembre 2007, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante "anagrafe tributaria";
- istituti di credito, con riferimento alla gestione dei servizi di *e-banking*;
- trattamenti di dati personali effettuati da strutture sanitarie, in relazione alla somministrazione di farmaci e prestazioni sanitarie e alla sponsorizzazione di attività di cura o di ricerca.

Oltre ai temi di controllo sopra delineati, nei due semestri, sono state anche effettuate:

- verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- altre verifiche di iniziativa concernenti, in particolare, l'adempimento dell'obbligo di notificazione nei confronti di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- verifiche sulla liceità e correttezza dei trattamenti di dati personali con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

19.2. *La collaborazione con la Guardia di finanza*

Anche nel 2007 è risultato determinante, nel settore ispettivo, il rapporto con la Guardia di finanza che ha consentito all'Autorità di poter disporre di altre risorse qualificate per espletare l'attività di controllo prevista dalla legge.

Il Protocollo di intesa siglato nel 2005 consente al Garante di avvalersi del Corpo attraverso:

- la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- l'assistenza nei rapporti con l'autorità giudiziaria;
- lo sviluppo di attività ispettive delegate o sub-delegate per l'accertamento delle violazioni;
- la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
- l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in

determinati settori;
- la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

L'Autorià, quando ritiene necessario avvalersi della collaborazione del Corpo, attiva il Nucleo speciale funzione pubblica e *privacy* con sede a Roma che, disponendo di personale specializzato, provvede direttamente ad effettuare gli accertamenti, utilizzando anche, ove necessario, reparti del Corpo territorialmente competenti.

Le informazioni e i documenti acquisiti nell'ambito degli accertamenti vengono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Quando nell'ambito dell'ispezione emergono violazioni penali o amministrative la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'autorità giudiziaria e alla contestazione della sanzione amministrativa.

Sono proseguite, anche nel 2007, le attività tese a realizzare un maggior coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, compagnie e tenenze).

L'obiettivo è fruire di un dispositivo di controllo flessibile e articolato che consenta, in funzione della complessità degli accertamenti, di effettuarli direttamente a cura del dipartimento ispettivo dell'Ufficio, ovvero attraverso il Nucleo speciale, oppure, nel caso di accertamenti di non elevata complessità che concernono ad esempio la verifica di singoli adempimenti, delegando i reparti territoriali della Guardia di finanza.

In questo ambito è stata effettuata, in via sperimentale, una prima attività di controllo denominata "a progetto". Si tratta di un'attività complessa di carattere operativo che rientra nell'attuazione di linee strategiche definite di concerto con il Comando generale della Guardia di finanza e che comporta l'esecuzione di compiti correlati tra loro da parte di unità organizzative della componente speciale e di quella territoriale del Corpo, con obiettivi, tempi e assorbimento di risorse definiti.

Questa particolare tipologia di controllo è stata effettuata sulla base dell'elaborazione congiunta da parte dell'Ufficio e del Nucleo speciale di una guida per l'accertamento nell'ambito della quale sono stati definiti, in modo estremamente analitico, i passi che i *team* di ispettori avrebbero dovuto compiere successivamente e le liste dei controlli da eseguire *in loco.*

In esecuzione della prima di queste attività denominata "progetto *teleselling*" gli accertamenti sono stati indirizzati alla verifica del rispetto delle disposizioni previste dal Codice in relazione anche ai provvedimenti già adottati dall'Autorità nel settore dei *call center.* Sono stati sottoposti a controllo 76 *call center* operanti per le maggiori compagnie telefoniche (Telecom Italia S.p.A., Vodafone Omnitel NV, Wind telecomunicazioni S.p.A. e H3G S.p.A.) e gli esiti di tale attività sono tuttora all'esame dell'Autorità.

19.3. *I settori oggetto dei controlli e i casi più rilevanti*

Nel 2007 sono state effettuate, suddivise per settore, le seguenti attività ispettive:
- centodieci controlli nei confronti di operatori telefonici con riferimento ai trattamenti effettuati tramite *call center* ;
- quaranta controlli nei confronti di enti previdenziali, istituti sanitari (pubblici e privati) e imprese/società che trattano dati sensibili, con riferimento

all'adozione delle misure minime di sicurezza;
- quaranta controlli nei confronti di istituti di credito per verificare, in particolare, il rispetto dell'obbligo di informativa con riferimento all'impiego di sistemi di rilevazione biometria e di videosorveglianza;
- quaranta controlli nei confronti di società che effettuano trattamenti per i quali è prevista la notificazione al Garante;
- trenta controlli nei confronti di soggetti pubblici e privati che utilizzano sistemi di videosorveglianza, per verificare la liceità del trattamento e il rispetto del relativo provvedimento generale del Garante;
- venti controlli nei confronti di dentisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di oculisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di istituti di preparazione privatistica agli esami, per verificare le modalità del trattamento dei dati degli studenti;
- venti controlli nei confronti di alberghi con centri benessere, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di imprese di trasporti, per verificare la correttezza dei trattamenti dei dati dei clienti e il rispetto degli adempimenti relativi all'informativa;
- venti controlli nei confronti di società che si avvalgono del servizio garanzia degli assegni fornito da *Centax* S.p.A.;
- quindici controlli nei confronti di società che hanno effettuato ricerche di personale a mezzo di annunci pubblicati sul giornale, per verificare le modalità di trattamento dei *curricula* raccolti e l'assolvimento degli adempimenti di legge;
- dieci controlli nei confronti di agenzie matrimoniali, per verificare la correttezza dei trattamenti dei dati dei clienti e il rispetto degli adempimenti relativi all'informativa e al consenso;
- dieci controlli nei confronti di autoscuole, per verificare la correttezza dei trattamenti dei dati dei clienti e il rispetto degli adempimenti relativi all'informativa e al consenso;
- dieci controlli nei confronti di società che effettuano vendita di strumenti elettronici di rilevazione ambientale, per verificare la correttezza dei trattamenti dei dati dei clienti ed il rispetto degli adempimenti relativi all'informativa ed al consenso;
- dieci controlli nei confronti di notai, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- cinque controlli nei confronti di società per verificare il trattamento dei dati personali nell'ambito di un sondaggio politico elettorale;
- quattro controlli nei confronti di società farmaceutiche, in relazione alla somministrazione di farmaci e prestazioni sanitarie e alla sponsorizzazione di attività di cura o di ricerca, con particolare riguardo all'informativa agli interessati e al consenso eventualmente necessario;
- quattro controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante "anagrafe tributaria";
- tre controlli nei confronti di compagnie telefoniche con riferimento ai *cd.* "dati di traffico";
- un controllo nei confronti di un istituto di credito, con riferimento alla gestione dei servizi di *e-banking*.

In relazione a quanto emerso dagli accertamenti sono state effettuate circa novanta proposte di adozione di provvedimenti inibitori e/o di prescrizioni per conformare il trattamento alla legge a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

In particolare si segnalano:

- il provvedimento nei confronti di un'agenzia di intermediazione immobiliare in relazione al trattamento dei dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, lo stato di salute e/o lo stato di disabilità, nonché la vita sessuale (*Provv.* 11 gennaio 2007 [doc. *web* n. 1381620]);
- il provvedimento nei confronti di un istituto di credito, in relazione alla consultazione di informazioni sulla solvibilità e affidabilità dei clienti (*Provv.* 8 marzo 2007 [doc. *web* n. 1390872]);
- il provvedimento nei confronti di una società, in relazione al servizio denominato "garanzia assegni" (*Provv.* 17 maggio 2007 [doc. *web* n. 1409251]);
- i provvedimenti nei confronti di gestori di compagnie telefoniche, in relazione all'attività di *call center* svolta anche attraverso società esterne (*Provvedimenti* 30 maggio 2007 [doc. *web* nn. 1412586, 1412557, 1412598, 1412610 e 1412626]);
- i provvedimenti nei confronti di diverse società, in relazione all'invio di comunicazioni commerciali mediante *telefax* (*Provv.* 28 giugno 2007 [doc. *web* n. 1433896]; *Provv.* 11 luglio 2007 [doc. *web* n. 1433939]; *Provv.* 4 ottobre 2007 [doc. *web* n. 1457973]; *Provv.* 31 gennaio 2008 [doc. *web* nn. 1489843 e 1488781]);
- il provvedimento nei confronti di un ente pubblico, in relazione al trattamento dei dati personali effettuato attraverso un sistema di videosorveglianza (*Provv.* 4 ottobre 2007 [doc. *web* n. 1457505]);
- i provvedimenti nei confronti di società operanti nel settore della grande distribuzione, in relazione al trattamento dei dati personali raccolti per il rilascio alla clientela di "carte di fedeltà" e utilizzati illecitamente anche a fini di *marketing* (*Provvedimenti* 15 novembre 2007 [doc. *web* nn. 1466898, 1466930, 1466971, 1466956 e 1466985]);
- il provvedimento generale nei confronti di gestori di compagnie telefoniche, in relazione alla sicurezza dei dati di traffico telefonici e telematici (*Provv.* 17 gennaio 2008 [doc. *web* n. 1482111]);
- i provvedimenti nei confronti di istituti di credito, in relazione al trattamento di dati biometrici (*Provvedimenti* 23 gennaio 2008 [doc. *web* nn. 1490382, 1490477 e 1490533]);
- il provvedimento nei confronti di una catena alberghiera, in relazione al trattamento dei dati personali dei clienti (*Provv.* 31 gennaio 2008 [doc. *web* n. 1490553]).

Riguardo all'attività ispettiva svolta dall'Ufficio nei confronti di gestori di compagnie telefoniche in relazione alla conservazione dei dati di traffico telefonico e telematico e di società farmaceutiche con riferimento alla sperimentazione dei farmaci, l'Autorità, attese le criticità emerse nell'ambito degli accertamenti e la rilevanza del pregiudizio per un'ampia platea di interessati, dopo aver definito alcune linee-guida, ha avviato una consultazione pubblica tesa a definire regole più precise e rigorose per tutti i soggetti che effettuano tali trattamenti di dati personali (*Provv.* 19 settembre 2007 [doc. *web* n. 1442463] e *Provv.* 29 novembre 2007 [doc. *web* n. 1468981]).

19.4. *L'attività sanzionatoria del Garante*

In conseguenza delle ispezioni effettuate, sono state inviate all'autorità giudiziaria quindici informative (di cui tredici a cura del Dipartimento attività ispettive e sanzioni dell'Ufficio e due da parte della Guardia di finanza) e avviati duecentoventotto procedimenti sanzionatori amministrativi (di cui centododici istruiti dal Dipartimento e centosedici della Guardia di finanza).

Per quanto riguarda le violazioni penali, esse hanno riguardato: mancata adozione delle misure minime di sicurezza (10), mancato adempimento di una deliberazione del Garante (2), trattamento illecito dei dati (2) e falsità nelle dichiarazioni e notificazioni al Garante (1).

Otto sono stati i procedimenti connessi al *cd.* "ravvedimento operoso" in materia di misure minime di sicurezza, previsto dall'art. 169, comma 2, del Codice.

Tale disposizione prevede infatti che, nel caso in cui venga rilevata una violazione di una o più delle misure minime di sicurezza specificatamente previste dal Disciplinare tecnico sulle misure minime di sicurezza (Allegato B al Codice) il Garante, a seguito di una prescrizione da impartire alla persona individuata come responsabile della predetta violazione, verificato il rispetto della prescrizione stessa, possa ammettere i destinatari della prescrizione al pagamento pari a un quarto del massimo della sanzione prevista. L'adempimento alla prescrizione e il pagamento della somma vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

L'attività in questione ha riguardato quindici persone (in qualità di titolari/responsabili dei trattamenti), per un totale di sanzioni applicate pari a 185.329 euro.

Come evidenziano i dati di seguito riportati, anche per quanto attiene l'attività sanzionatoria, nell'anno 2007, si è registrato un notevole incremento.

Anno	2002	2003	2004	2005	2006	2007
Violazioni contestate	46	27	27	84	158	228

Le sanzioni amministrative contestate, per un totale compreso tra un minimo di 725.000 euro e un massimo di 4.355.000 euro, hanno riguardato:

- omessa o inidonea informativa (duecentosedici);
- omessa notificazione (sei);
- omessa risposta alle richieste del Garante (quattro)
- codice del consumo (due).

A fronte delle contestazioni notificate sono stati riscossi 814.625 euro a titolo di definizione in via breve.

L'incidenza delle violazioni penali e amministrative riscontrate è stata pari a circa il 51% sul totale delle ispezioni.

È risultata più sanzionata la violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati al fine di rendere lo stesso interessato pienamente consapevole dell'effettivo utilizzo dei dati personali che lo riguardano.

Occorre evidenziare che tale violazione assume particolare rilevanza nei casi in cui la legge impone al titolare del trattamento di acquisire anche il consenso dell'interessato per specifiche finalità (ad esempio, per l'utilizzo dei dati per finalità di *marketing*, o per la comunicazione di dati a terzi). In questi casi, l'omessa o inidonea informativa produce effetti anche sulla validità del consenso eventualmente acquisito che, sulla

base di quanto previsto dall'art. 23, comma 3 del Codice, può ritenersi valido solo se sono state fornite all'interessato le informazioni di cui all'art. 13 del Codice.

Nel numero delle contestazioni effettuate per l'omessa o inidonea informativa, si segnala che circa il 35% sono da riferirsi a segnalazioni relative a trattamenti effettuati, attraverso *call center*, da compagnie telefoniche in relazione all'attivazione di servizi non richiesti; ciò, a riprova dello straordinario sforzo compiuto nel 2007 dall'Autorità per contrastare tale fenomeno.

20 Le relazioni internazionali

Conferenze tra autorità di protezione dei dati a livello europeo

La Conferenza annuale delle autorità europee di protezione dati che si è tenuta nel 2008 a Roma il 17 ed il 18 aprile, con la partecipazione di 38 delegazioni di oltre 30 Paesi europei, si è articolata in sei sessioni; le prime tre, relative a sicurezza, imprese e nuove tecnologie, sono state introdotte da un contributo video affidato rispettivamente a una personalità del mondo delle istituzioni, del diritto e della ricerca. Gli interventi miravano a stimolare la discussione su alcune questioni di fondo: come garantire la *privacy* in un contesto globalizzato, caratterizzato da un crescente impiego di nuove tecnologie e alle prese con seri problemi di sicurezza; quali siano le prospettive per una efficace protezione dei dati personali riguardo ai flussi transfrontalieri di dati e all'uso di informazioni commerciali a fini di perseguimento dei reati; come addivenire a regole globali per governare lo sviluppo della rete; come si configurano gli scenari presenti e futuri per l'attività delle autorità di protezione dei dati personali.

La seconda giornata è stata invece dedicata alle tematiche legate alla collaborazione giudiziaria e di polizia e all'attività del Gruppo delle autorità europee su Polizia e Giustizia (*Working Party on Police e Justice, v. infra*), presieduto da Francesco Pizzetti, nonché alle relazioni di alcuni gruppi di lavoro (*Case Handling Workshop*, Gruppo di Berlino sulla protezione dei dati nel settore delle telecomunicazioni) che riferiscono tradizionalmente alla Conferenza.

In conclusione è stata adottata una dichiarazione sulle misure di controllo delle frontiere e della circolazione di tutti i viaggiatori, in arrivo o in partenza dall'Europa, per invitare con forza tutte le istituzioni interessate a valutare l'effettiva necessità di adottare tali misure e a individuare criteri di controllo proporzionati rispetto agli obiettivi da raggiungere (*v.* anche *par.* 20.2.). Con tale dichiarazione è stato sottolineato, inoltre, che l'esigenza di controlli efficaci per garantire le frontiere deve essere conforme all'idea di un'Europa "aperta al mondo", uno degli obiettivi perseguiti in questi anni dall'Unione europea. La dichiarazione è stata inviata a tutte le istituzioni europee (Parlamento, Consiglio, Commissione).

Nel 2007 la Conferenza di Primavera è stata ospitata dal *Data Protection Commissioner* di Cipro (10-11 maggio 2007). Le oltre trenta delegazioni presenti hanno approvato tre documenti rivolti a tutte le istituzioni europee, per sottolineare la necessità sia di tutelare i diritti fondamentali dei cittadini europei nell'ambito della cooperazione giudiziaria e nelle attività di polizia, sia di rispondere con maggiore rapidità e incisività ai rischi derivanti dalla sempre più massiccia raccolta di dati personali a fini di sicurezza. Le autorità hanno convenuto sull'esigenza di un approccio uniforme europeo per garantire il rispetto dei princìpi fondamentali della protezione dei dati, attraverso strumenti utili e efficaci e una riflessione ampia e condivisa che coinvolga più direttamente i Parlamenti nazionali e le opinioni pubbliche degli Stati europei.

Sono state approvate una decisione e due dichiarazioni, queste ultime, rispettivamente, sulla proposta di decisione quadro del Consiglio Ue sulla protezione dei dati personali trattati nell'ambito del *cd.* "Terzo pilastro" (cooperazione giudiziaria e di polizia) e sul principio di disponibilità sancito dal "Programma de L'Aja" (ossia sull'obbligo per gli Stati membri di rendere reciprocamente disponibili i dati raccolti a livello nazionale per finalità di giustizia e polizia).

Nella prima dichiarazione, i Garanti ribadiscono che la decisione quadro del Consiglio Ue, limitando la protezione ai soli dati oggetto di scambio fra gli Stati (nell'ottica della "disponibilità" suddetta), e non estendendola anche ai trattamenti effettuati a livello nazionale, rischia di introdurre "due velocità" nell'ambito del *cd.* "Terzo pilastro". Viceversa, occorre garantire uniformità di tutela a livello nazionale e sopranazionale nel trattamento dei dati raccolti per finalità di giustizia e polizia.

La seconda dichiarazione contiene indicazioni utili a valutare se, e in quale misura, strumenti normativi proposti (a livello europeo o nazionale) per facilitare lo scambio di dati siano compatibili con i princìpi di protezione dei dati. L'obiettivo è potenziare le libertà civili ampliando, al tempo stesso, le possibilità di utilizzo di informazioni da parte di forze dell'ordine e autorità giudiziarie.

Con la decisione è stato conferito al menzionato Gruppo di lavoro per le questioni di Terzo pilastro un mandato più ampio, per una risposta rapida ed efficace ai rischi derivanti dal crescente uso di banche dati a fini di sicurezza. La Conferenza ha riconosciuto che tale obiettivo potrà essere meglio raggiunto attraverso un'articolazione permanente e strutturata del *Working Party*. Il Presidente dell'Autorità italiana è stato nominato Presidente del gruppo, ridenominato *"Working Party on Police and Justice"*.

Conferenze delle autorità su scala internazionale

La 29ma Conferenza mondiale delle autorità garanti svoltasi a Montreal dal 25 al 28 settembre 2007 ha affrontato temi relativi alle nuove frontiere della protezione dei dati personali, come evidenziato dal titolo *"Terra Incognita - Gli orizzonti della protezione dei dati"*.

Il programma, particolarmente denso, ha riguardato tra l'altro la sicurezza e la globalizzazione, i rischi e le potenzialità della rete, le nuove tecnologie e il tracciamento delle persone, i dati genetici e le bio-banche.

Sono state adottate tre importanti risoluzioni.

La prima sottolinea l'urgenza di pervenire a criteri globalmente condivisi per tutelare i dati dei passeggeri, oggetto di pressioni sempre più forti da parte dei Governi di molti Paesi del mondo.

I Garanti hanno chiesto collaborazione a soggetti pubblici e privati, organizzazioni non governative e autorità di protezione dati, per garantire alcuni princìpi basilari nella raccolta e nell'utilizzazione di questi dati, sottolineando la necessità di conciliare le esigenze connesse alla lotta al terrorismo con la tutela dei diritti dei cittadini e delle imprese coinvolte. I princìpi riguardano la trasparenza nelle finalità della raccolta dei dati; la loro utilizzazione quando siano realmente indispensabili; il rispetto di criteri di proporzionalità nella raccolta; i limiti al numero dei soggetti ai quali possono essere comunicati; l'accuratezza delle informazioni; le garanzie per i cittadini che intendano esercitare diritti di accesso o rettifica dei dati stessi, a cominciare da un'adeguata informativa sulle caratteristiche del trattamento.

La seconda risoluzione riguarda la definizione di *standard* universali in materia di *privacy* in collaborazione con l'Iso (*International Organization for Standardization*). Essa evidenzia che il tentativo di tradurre i princìpi di protezione dati in regole tecnologicamente efficaci merita sostegno, benché in ambito Iso trovino appoggio soprattutto le tematiche della sicurezza dei sistemi informativi. La conferenza ha invitato tutte le autorità di protezione dati a partecipare attivamente al processo di definizione di tali *standard*, anche attraverso un migliore coordinamento delle iniziative nazionali e il coinvolgimento diffuso del mondo scientifico e della ricerca.

La terza risoluzione è stata dedicata all'esigenza di potenziare la cooperazione con gli organismi (quali l'Ocse, il Consiglio d'Europa, l'Apec) che, in maniera diversa, stanno sviluppando strumenti a sostegno della protezione dei dati e della *privacy*, nel

solco delle indicazioni fornite dalla Conferenza internazionale delle autorità tenutasi nel 2006 a Londra (*cfr. Relazione* 2006, *p.* 150).

Il presidente dell'autorità italiana ha presieduto una sessione plenaria specificamente dedicata alla protezione dei minori su Internet; nel suo intervento, ha espresso preoccupazione per la scarsa attenzione dimostrata dai giovani alla protezione della loro *privacy* nel contesto tecnologico in cui si muovono. In particolare, ha evidenziato che la comunicazione elettronica e le tecnologie dell'informazione tendono a trasformare ogni relazione interpersonale in un flusso di dati e che, pertanto, la tutela dei dati personali su Internet significa innanzitutto proteggere i rapporti tra gli individui e la loro stessa libertà. Nella società "smaterializzata" i giovani sono più esposti al rischio di manipolazioni della loro sfera privata. La diffusione di immagini su Internet, le fotografie scattate senza consapevolezza o i video girati per uso personale possono finire sulla rete generando pregiudizievoli conseguenze sui bambini. Allo stesso modo, l'utilizzo delle *chat* e lo scambio di *e-mail* senza l'adeguata consapevolezza dei rischi possono esporre i più giovani a situazioni pericolose.

20.1. *La cooperazione tra autorità garanti nell'Ue: il Gruppo art. 29*

Il Gruppo art. 29 (che riunisce i rappresentanti delle autorità per la protezione dei dati europee, ed è stato istituito ai sensi dell'art. 29 della direttiva 95/46/Ce) per rendere più effettiva la sua funzione di consulenza "indipendente" verso le istituzioni comunitarie, e *in primis* verso la Commissione, ha stabilito di definire un programma biennale di attività e di rivedere le modalità con cui promuovere la trasparenza sulle attività svolte. Il Programma di lavoro del Gruppo per gli anni 2008-2009 (WP 146) è piuttosto ambizioso e intende concentrare le attività, fatte salve le richieste di parere su iniziative legislative della Commissione, su quattro temi strategici. Il primo, relativo al miglioramento dell'applicazione della direttiva 95/46/Ce, prevede interventi volti a chiarire l'interpretazione di alcuni aspetti chiave: oltre al lavoro già svolto in relazione alla nozione di dato personale, il Gruppo intende chiarire i concetti di responsabile e di incaricato del trattamento, il diritto applicabile, la limitazione delle finalità ed i presupposti per il trattamento. Il secondo è rivolto alla necessità di garantire la protezione dei dati nei trasferimenti internazionali, in particolare in relazione all'uso di strumenti quali le *binding corporate rule* e del *Safe Harbor*; il terzo mira a garantire la protezione dei dati in relazione alle nuove tecnologie (oltre al parere adottato sui motori di ricerca, il Gruppo si occuperà di reti sociali *on-line*, di profilazione, di radiodiffusione digitale, l'uso della biometria e dell'*Rfid*). Il quarto tema, più interno, riguarda il miglioramento dell'efficacia del lavoro del Gruppo e prevede diverse azioni, alcune delle quali esposte in un recente documento sulla trasparenza (WP 135). Il programma di lavoro tiene anche conto delle ulteriori sfide cui occorre prepararsi, in particolare dell'impatto del trattato di Lisbona.

Il concetto di dato personale (WP 136)

I Garanti europei, per chiarire meglio la nozione di "dato personale", hanno approvato il parere4/2007 [doc. *web* n. 1496512], fornendo alcune indicazioni sull'applicazione della direttiva 95/46/Ce ai trattamenti effettuati con le nuove tecnologie (quali l'*Rfid*) o in contesti altamente tecnologici (*e-Government*, cartelle cliniche elettroniche, *ecc.*).

La definizione di dato personale contenuta nella direttiva (*"qualsiasi informazione concernente una persona fisica identificata o identificabile"*) è stata analizzata con esempi tratti dai casi affrontati dalle diverse autorità di protezione dei dati. Dall'analisi è emersa, anzitutto, l'ampiezza del concetto di dato personale (*"qualsiasi informazione"*),

in linea con la giurisprudenza della Corte europea dei diritti umani e della Corte europea di giustizia nei casi concernenti possibili violazioni del diritto alla vita privata. La riflessione ha consentito di proporre un'interpretazione equilibrata in base alla quale, ad esempio, rientrano nella definizione di dato personale sia le istruzioni impartite dal cliente alla propria banca e registrate, sia le immagini filmate da un impianto di videosorveglianza, nella misura in cui i singoli individui siano riconoscibili. Un dato biometrico (l'impronta digitale) è un dato personale perché identifica una persona, ma i campioni di tessuto dai quali si estraggono i dati biometrici non sono di per sé dati personali (anche se le operazioni effettuate per estrarre tali informazioni biometriche configurano un trattamento di dati personali). Un'informazione, inoltre, può "riguardare" una persona fisica identificata o identificabile sotto vari aspetti: perché oggetto dell'informazione è chiaramente una persona fisica, oppure la finalità del dato raccolto è, alla luce delle circostanze specifiche, quella di "incidere" in qualche modo su una persona specifica; oppure, perché l'informazione, se trattata, è suscettibile di effetti sui diritti e gli interessi di una determinata persona.

L'"identificabilità", secondo la direttiva, può essere "diretta" o, valutando tutte le circostanze del caso specifico, "indiretta": notizie di stampa su un vecchio procedimento penale di grande risonanza possono costituire un dato personale poiché è possibile ricostruire l'identità di una persona consultando vecchi numeri del giornale; informazioni apparentemente frammentarie e prive di riferimenti diretti all'identità di una persona (il nome) costituiscono dato personale se il titolare intende utilizzarle per identificare una determinata persona e possiede presumibilmente i mezzi per ricostruire tale identità (si pensi alla videosorveglianza diretta a favorire l'eventuale identificazione di determinati soggetti, o agli indirizzi Ip raccolti per individuare presunte violazioni del *copyright*).

Infine, la direttiva si riferisce a informazioni concernenti una *"persona fisica"*, ma, almeno in determinate circostanze, può essere rilevante anche il trattamento di dati relativi a defunti in quanto la legge nazionale lo ammette, oppure perché onore e immagine sono tutelati anche dopo la morte della persona. Della stessa tutela possono godere anche le persone giuridiche come ha chiarito la Corte europea di giustizia, in base alla quale *"nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/Ce a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun altra disposizione del diritto comunitario"* (Corte di giustizia delle Comunità europee, 6 novembre 2003, C-101/01).

Indagine sulle società assicurative

Nel 2007 il Gruppo art. 29 ha realizzato per la prima volta una verifica congiunta, sull'osservanza nei Paesi dell'Unione europea dei princìpi di protezione dati da parte delle società che offrono polizze di assistenza sanitaria integrativa. L'analisi ha preso le mosse da un questionario distribuito in tutti gli Stati membri alle compagnie di assicurazione più rappresentative in termini di quote di mercato. Dall'indagine (WP 137, rapporto n. 1/2007) è emerso il sostanziale rispetto delle norme in materia, soprattutto per quanto concerne l'informativa agli assicurati e la raccolta del necessario consenso. Tuttavia, sono state evidenziate carenze in alcuni ambiti, in particolare relativamente alla circolazione delle informazioni con riguardo ai terzi, eventuali beneficiari delle polizze assicurative e all'adozione di adeguate misure organizzative per garantire l'accuratezza, l'aggiornamento e la correzione dei dati personali.

Parere sul nuovo accordo Pnr con gli Stati Uniti d'America

Il Gruppo articolo 29 ha pubblicato il 17 agosto 2007 un parere molto critico sul nuovo accordo stipulato fra l'Ue e l'Amministrazione statunitense in materia di dati relativi ai passeggeri (*Passenger Name Record*, Pnr) (parere 5/2007, WP 138). L'accordo, che apparentemente riduce da 34 a 19 le categorie di dati oggetto di tra-

sferimento, in realtà accorpa alcuni dati in categorie più ampie; in base ad esso, inoltre, continueranno a essere trasferiti i dati sensibili, e il loro "filtraggio" sarà effettuato ancora dalle autorità americane (in particolare, il *Department for Homeland Security, Dhs*), punto sul quale il WP 29 si era dichiarato più volte contrario; il periodo di conservazione dei dati trasferiti è aumentato da 3 anni e mezzo a 7 anni e i dati possono restare accessibili (in casi specifici) per ulteriori 8 anni (l'accordo utilizza l'espressione *"in stato di sonno"* per indicare tali dati). È previsto l'"impegno" delle autorità Usa a mettere in atto il sistema *cd. "push"* (invio dei dati da parte delle compagnie aeree) anziché *"pull"* (accesso diretto ai *database* delle compagnie aeree da parte delle autorità Usa), ma a una serie di condizioni che necessitano di ulteriori precisazioni.

In tale materia, il sottogruppo che nell'ambito delle attività del Gruppo art. 29 si occupa di Pnr ha anche predisposto una bozza di risoluzione (*Resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes*) approvata dalla *World Conference* di Montreal (*cfr. supra, par.* 20).

Pareri sul Sistema di cooperazione per la tutela dei consumatori e sul Sistema di informazione del mercato interno (Imi)

I pareri del Gruppo art. 29 n. 6/2007 (WP 139) e n. 7/2007 (WP 140) sono stati richiesti dalla Commissione europea su due proposte presentate per la creazione, rispettivamente, di una base di dati per lo scambio di informazioni tra le autorità nazionali responsabili dell'applicazione delle disposizioni in materia di tutela dei consumatori e la Commissione stessa (Cpcs-*Consumer Protection Cooperation System*), e di un *database* centralizzato per lo scambio di informazioni relative alle professioni regolamentate (Imi-*Internal Market Information System*). Quanto al Cpcs, il Gruppo ha condiviso sostanzialmente le osservazioni critiche del Garante europeo della protezione dei dati, soprattutto sulla necessità di assicurare il rispetto dei princìpi di finalità (nell'utilizzo dei dati contenuti nella costituenda banca dati, che deve servire esclusivamente alla tutela dei consumatori), pertinenza e non eccedenza dei dati, nonché sull'eccessiva durata del periodo di conservazione previsto per le informazioni contenute in tale *database* (5 anni). Per l'Imi il Gruppo ha invece segnalato l'opportunità di una decisione specifica della Commissione a corredo delle direttive che prevedono la costituzione del sistema, anche ai fini della creazione di una base giuridica solida che ne renda legittimo l'utilizzo.

Livello di protezione dati a Jersey e nelle Isole Fær Øer

Il parere di adeguatezza del Gruppo art. 29 è necessario affinché la Commissione europea possa adottare una decisione formale ai sensi della direttiva 95/46/Ce sul trasferimento di dati personali in un Paese terzo senza alcuna limitazione. Con riguardo all'Isola di Jersey e al territorio delle Isole Fær Øer (pareri 8 e 9 del 2007, WP 141-142) le autorità europee si sono pronunciate favorevolmente, pur evidenziando alcune ambiguità nella legislazione emanata nel Bailato di Jersey, soprattutto con riguardo ai poteri dell'autorità di controllo.

Ottava direttiva concernente gli *"Statutory Audit"*

Con il parere 10/2007 (WP 143) il Gruppo si è occupato della comunicazione di dati relativi alle attività di *audit* finanziario e contabile fra le autorità pubbliche europee competenti in materia (in Italia la Consob) e quelle di Paesi terzi. Il parere verte, in particolare, sull'art. 47 della direttiva 2006/43/Ce, ossia sulla trasmissibilità –da parte delle autorità pubbliche competenti per la vigilanza sui controlli contabili nei Paesi Ue alle omologhe autorità dei Paesi terzi– dei dati personali inseriti nella documentazione da fornire (nominativi dei revisori, nominativi di altri soggetti interessati, eventualmente dipendenti dell'azienda, *ecc.*). La direttiva prevede due scenari, cosiddetti di "breve periodo" (trasmissione dei dati in caso di indagini specifiche su casi di presunte irregolarità) e di "medio periodo" (invio dei dati alle autorità pubbliche competenti nel Paese terzo in riferimento ai controlli contabili *standard*). In base al parere il trasferimento può essere giustificato, nel primo caso,

attraverso la deroga al divieto di trasferimento di dati verso Paesi terzi basata sull'art. 26, comma 1, lett. *d*), della direttiva 95/46/Ce (sussistenza di un interesse pubblico rilevante quale giustificazione del trasferimento). Tuttavia, tale disposizione, come già ricordato dal Gruppo nel documento del 25 novembre 2005 relativo all'interpretazione dell'art. 26(1) della direttiva 95/46/Ce (WP114), deve essere applicata e interpretata dagli Stati membri in modo restrittivo anche con riguardo alla necessità dei dati dei quali si chiede o si prevede il trasferimento. Per quanto concerne la situazione di "medio periodo", occorre garantire che negli accordi di reciprocità previsti fra le autorità competenti Ue e quelle di Paesi terzi siano soddisfatte tutte le condizioni di adeguatezza indicate nell'articolo 47(3) della direttiva 2006/43/Ce. Infine, il "regime speciale" di cui all'articolo 47(4) (trasferimento diretto da parte dei revisori contabili stabiliti in un Paese Ue alle autorità competenti del Paese terzo), per il suo carattere eccezionale e derogatorio rispetto alla norma generale, deve essere meglio definito dalla Commissione con il necessario ausilio del Gruppo art. 29.

Proposta di decisione-quadro sull'uso dei dati Pnr nelle attività di contrasto del terrorismo

Il Gruppo art. 29 e il *Working Party on Police and Justice* (*cfr. par.* 20.2) hanno adottato un parere congiunto per richiamare l'attenzione del Consiglio Ue e della Commissione sugli aspetti ritenuti contrari ai princìpi fondamentali in materia di tutela dei dati personali nella proposta di decisione-quadro del Consiglio che istituirebbe il cosiddetto "Pnr europeo", presentata dalla Commissione il 6 novembre 2007 (WP 145/WPPJ 01/07).

Attraverso tale decisione verrebbe introdotto in Europa l'obbligo di comunicare alle "autorità competenti" i dati dei passeggeri aerei diretti verso i Paesi dell'Ue, come già avviene per gli Usa.

I Garanti ritengono che la proposta comporti una grave compressione dei diritti fondamentali dei cittadini europei, che non risulta pienamente giustificata né assolutamente indispensabile "in una società democratica", come già esposto nei numerosi pareri concernenti il trasferimento dei dati Pnr negli Usa (*v. Relazione* 2006, *p.* 159).

In questo caso, non sono dimostrate né la necessità, né la proporzionalità del trattamento previsto nel progetto di decisione-quadro. Soprattutto, non ha trovato ancora piena attuazione in tutti gli Stati membri la direttiva 2004/82/Ce che prevede l'obbligo per i vettori aerei europei di raccogliere e rendere disponibile, a richiesta, i dati Api (*Advance Passenger Information*), che corrispondono in sostanza alle informazioni personali utilizzate per il *check-in*. Appare quindi quanto meno eccessivo introdurre un obbligo ulteriore per finalità di sicurezza quando non si è ancora verificata l'efficacia del sistema istituito per vigilare sulle frontiere europee.

Numerosi altri aspetti della proposta sono stati giudicati problematici: le categorie di informazione oggetto di trasferimento risultano addirittura più numerose di quelle previste nell'Accordo sul Pnr-Usa; il periodo di conservazione dei dati da parte delle autorità competenti è eccessivo (tredici anni); non vi è chiarezza sulla necessità di prevedere esclusivamente un sistema del tipo *"push"*, e non *"pull"* (*v. supra*), come già indicato nei pareri sul Pnr-Usa; l'eliminazione dei dati sensibili eventualmente raccolti (il cui trattamento è riservato solo ad alcuni specifici soggetti) deve essere effettuata dai singoli vettori aerei, e non dalle autorità riceventi; troppo ampia risulta infine la discrezionalità degli Stati membri nell'attuare la decisione, soprattutto per quanto riguarda l'ambito di circolazione delle informazioni fornite dai vettori aerei.

Le autorità europee per la *privacy* hanno quindi chiesto un serio dibattito sul tema, con tutte le parti in causa.

Protezione dei dati personali dei minori

Il Gruppo art. 29 si è pronunciato sul tema della protezione dei dati relativi ai minori con il documento di lavoro del 18 febbraio 2008 (WP 147). Il documento, suddiviso in due sezioni principali, individua nella prima parte i princìpi fondamen-

tali sulla protezione del minore, anche con riferimento alla tutela dei dati; nella seconda, fornisce indicazioni per l'attuazione dei princìpi di data *protection* nel settore scolastico. I destinatari principali sono coloro che a vario titolo trattano i dati relativi ai minori, in particolare insegnanti e autorità scolastiche.

Dopo aver richiamato i princìpi fondamentali sulla protezione del minore previsti dalle convenzioni internazionali in materia, viene prestata particolare attenzione al principio dell'interesse primario del minore (*cd. "best interest of the child"*), elemento fondamentale per la risoluzione di eventuali conflitti, anche tra i minori e i loro rappresentanti. Ampio spazio è inoltre dedicato ai princìpi di qualità dei dati (correttezza, proporzionalità, sicurezza) e al principio di rappresentanza (da parte dei genitori o di chi abbia titolo), nonché alla necessità di accrescere la consapevolezza del minore con un'adeguata informativa e di coinvolgerlo nelle scelte che lo riguardano, in base al suo grado di maturità.

Nella parte generale viene anche menzionato il diritto all'oblìo, particolarmente significativo perché le informazioni relative al minore possono rapidamente divenire obsolete ed eccedenti rispetto all'originario scopo della raccolta.

Il documento affronta inoltre il tema dell'esercizio dei diritti del minore, normalmente esercitati dai rappresentanti del minore, ma che possono essere esercitati dal minore stesso a seconda della sua maturità.

La seconda parte del documento riguarda il contesto scolastico e affronta temi quali il trattamento dei dati nei *curricula* e l'impiego delle nuove tecnologie, con particolare riguardo alla videosorveglianza, all'accesso ai locali della scuola attraverso dispositivi biometrici, ai siti *web* scolastici e all'uso di videofonini in aula; sottolinea inoltre il ruolo delle scuole nella sensibilizzazione dei minori sui rischi derivanti dal trattamento dei dati che li riguardano e sull'esercizio dei loro diritti.

Si richiamano altresì i compiti delle autorità per la protezione dei dati nel promuovere la consapevolezza anche dei *policy maker* sull'importanza della protezione dei dati relativi ai minori e nel rendere i titolari del trattamento consapevoli dei loro obblighi.

Nella parte conclusiva viene segnalata l'opportunità di accordi tra le autorità per la protezione dei dati, i Ministri dell'istruzione e altre autorità competenti per rafforzare la protezione dei dati nell'ambito dei diritti fondamentali.

Protezione dei dati e attività dei motori di ricerca

Con il parere del 4 aprile 2008 (WP148) il Gruppo art. 29 ha svolto un'analisi delle principali questioni di protezione dei dati con specifico riferimento ai motori di ricerca che operano sulla rete. Il documento definisce l'insieme delle responsabilità in capo ai motori di ricerca, i quali effettuano la raccolta di dati personali in quanto fornitori di servizi (ove a*d es.*, raccolgano indirizzi Ip degli utenti, informazioni necessarie per accedere a servizi personalizzati attraverso *userID* e *password*, *ecc.*), o di contenuti (qualora memorizzino, attraverso la *cd.* "copia *cache*", i risultati di ricerche su Internet contenenti informazioni personali, ovvero forniscano profili personali o comunque informazioni organizzate relative ad un determinato soggetto).

Il parere valuta le legittime esigenze (di natura commerciale) dei motori di ricerca alla luce della necessità di garantire la tutela dei dati personali. Le autorità europee ribadiscono che la direttiva 95/46/Ce si applica pienamente anche ai trattamenti di dati personali effettuati da motori di ricerca situati al di fuori del territorio Ue e dello Spazio economico europeo, alla luce delle disposizioni contenute nell'articolo 4(1), lettera *c*), della direttiva stessa, nella misura in cui essi utilizzino per il trattamento dispositivi situati sul territorio degli Stati membri (*ad es.*, i *cookie*). Per contro, è da escludere l'applicabilità ai motori di ricerca sia della direttiva 2002/58/Ce (*cd.* "direttiva *e-Privacy*"), sia della direttiva 2006/24/Ce (*cd.* "direttiva *data retention*"). Entrambe, infatti, non riguardano i *"servizi della*

società dell'informazione" quali i motori di ricerca, esclusi espressamente dall'ambito di applicazione della direttiva *e-Privacy* (e, quindi, della direttiva sulla *"data retention"*) dall'articolo 2, lettera *c*), della direttiva-quadro sui servizi di comunicazione elettronica (2002/21/Ce).

Il parere sottolinea inoltre che i motori di ricerca sono tenuti a valutare attentamente la natura delle operazioni o dei servizi che essi gestiscono, in particolare per la conservazione dei dati personali raccolti, che devono essere distrutti o resi anonimi (con procedure realmente efficaci) se non necessari agli scopi del trattamento. I Garanti ribadiscono inoltre la necessità che i motori di ricerca incorporino i requisiti fondamentali in materia di protezione dati nei propri meccanismi operativi (*cd. "privacy by design"*). A tale scopo, viene formulata una serie di indicazioni e raccomandazioni: fornire un'adeguata informativa agli utenti (specificando il soggetto titolare del trattamento, la natura dei dati raccolti, gli scopi del trattamento); ottenere il consenso degli utenti per l'attività di profilazione o comunque per raffronti con altre informazioni in possesso del motore di ricerca stesso; effettuare la cancellazione (o l'anonimizzazione) dei dati non più necessari per le specifiche finalità per le quali sono stati raccolti. Il Gruppo sottolinea infine che spetta ai motori di ricerca giustificare la conservazione prolungata (in linea di principio, non superiore a 6 mesi) dei dati personali eventualmente in loro possesso. In tal senso, deve essere garantito il diritto all'oblìo delle persone i cui dati siano memorizzati nella *cd.* copia *"cache"*, evitando che permangano in rete informazioni superate e con ciò garantendo agli interessati l'esercizio effettivo dei diritti di accesso, rettifica e cancellazione previsti dalla direttiva 95/46/Ce.

Il Gruppo, in sintonia con quanto fatto dal Garante europeo, ha posto all'ordine del giorno un parere sulla proposta presentata dalla Commissione nel novembre 2007 di modifica del quadro normativo in materia di comunicazioni elettroniche, che include anche limitate proposte di modifica alla direttiva 2002/58/Ce. Nella proposta l'impianto generale della direttiva resta sostanzialmente immutato, mentre si precisano alcuni obblighi in materia di sicurezza.

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

Nel 2007 si è cercato di ricostituire e rendere più efficace l'attività di cooperazione tra le autorità europee di protezione dei dati personali. La Conferenza di primavera delle Autorità ha deliberato infatti più incisive competenze e un nuovo nome per il *Working Party on Police and Justice* ed ha chiamato a presiederlo il Presidente del Garante. La nuova composizione e articolazione del *Working Party* e la maggior autonomia consentiranno di intervenire in modo più tempestivo e mirato, per far conoscere le valutazioni delle autorità di protezione dei dati sulle misure comunitarie suscettibili di avere un impatto sulla protezione dei dati personali.

In tal modo (*v. par.* 20.1), pur in assenza di un quadro normativo adeguato, le autorità di protezione dei dati hanno trovato la possibilità di sviluppare azioni congiunte con il Gruppo dei Garanti europei su temi che, a livello europeo, sono trattati separatamente, quali la conservazione e utilizzo a fini di polizia dei dati raccolti da privati (vettori aerei, gestori e fornitori di servizi di comunicazione elettronica e di sistemi di pagamento, *ecc.*) per fornire servizi commerciali, o i controlli alle frontiere e le politiche di ingresso e soggiorno. Il WPPJ mantiene tuttavia il suo carattere volontario e ufficioso; ciò, se da un lato non rende obbligatorio per il legislatore europeo richiedere il parere del gruppo sulle iniziative legislative, facilita, dall'altro,

la visibilità delle autorità di protezione dei dati a livello europeo in un settore in cui non esiste ancora –anche per la distinzione in pilastri delle competenze ora prevista dal Trattato– un quadro comune e condiviso di princìpi che regoli le condizioni di liceità del trattamento dei dati personali.

A tal proposito occorre peraltro ricordare che l'approvazione del Trattato di Lisbona, abolendo tendenzialmente l'attuale articolazione in pilastri, favorisce in prospettiva una disciplina il più possibile unitaria della protezione dei dati personali, anche rendendo cogente il contenuto dell'articolo 8 della Carta dei diritti fondamentali.

Nonostante l'avvicinarsi di tale scadenza, il legislatore comunitario ha continuato a presentare proposte e a sollecitare l'adozione di quelle *in itinere.* Si deve peraltro registrare un certo ritardo per l'entrata in vigore di importanti sistemi informativi, quali il sistema informativo visti e la seconda generazione del Sis (Sis II). Il Trattato di Prüm, trasformato in iniziativa legislativa dell'Unione europea, ha ricevuto un generale accordo, che tuttavia subisce anch'esso rallentamenti nella definizione degli aspetti applicativi dello scambio dei dati.

Parte del "ritardo" è dovuta alla mancata adozione di princìpi per il trattamento dei dati personali nel Terzo pilastro, elemento richiamato dal programma dell'Aja come necessario quadro di riferimento per la cooperazione tra forze di polizia e magistratura nella prevenzione e repressione dei reati. Tali princìpi, presentati dalla Commissione europea nella forma di una proposta di decisione-quadro, sono stati resi sempre più vaghi e generici nel corso dell'esame da parte del Consiglio. Nonostante le forti critiche espresse dai garanti della protezione dei dati e dal Parlamento europeo, la presidenza del Consiglio è riuscita ad ottenere, nel novembre 2007, un accordo politico sul testo. Questo deve essere però nuovamente sottoposto al parere del Parlamento europeo e quindi si spera in qualche margine di manovra per riequilibrare la proposta.

Le autorità di protezione dei dati hanno segnalato con preoccupazione sempre maggiore il progressivo venir meno di "momenti istituzionali" (presso il Consiglio e, in parte, presso la Commissione) per la valutazione dell'impatto delle misure adottate sui diritti fondamentali e, più specificamente, sulla tutela dei dati personali. Nel Terzo pilastro, gli unici organismi che, per gli aspetti di specifica competenza attribuiti dalle Convenzioni cui si riferiscono, svolgono attività di supervisione e controllo sulla legittimità dei trattamenti dei dati sono le Autorità comuni di controllo Schengen, Europol e Dogane, oltre all'autorità comune Eurojust, nella cui composizione non è pero presente il Garante. La supervisione sui trattamenti effettuati nell'unità centrale è passata dall'Autorità comune di controllo Eurodac al Garante europeo recentemente istituito.

Questo modello di supervisione sarà applicato, una volta entrati in funzione, anche per il Vis (sistema informativo visti) e per il Sis II.

Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso

L'attività dell'Autorità di controllo comune (Acc) nel periodo considerato si è concentrata in particolare sulla proposta di decisione per l'integrazione di Europol tra le strutture dell'Unione europea e la definizione del quadro generale di riferimento per lo svolgimento della sua attività.

L'Acc ha espresso un parere molto articolato sul testo, formulando specifiche raccomandazioni, in particolare riguardo alla divergenza introdotta nel nuovo testo tra obiettivi di Europol e le più ridotte competenze attribuite all'organismo, nonché ai nuovi compiti di Europol di elaborazione di informazioni fornite non più solo dagli Stati membri, ma anche da Paesi terzi e da entità pubbliche e private. Poiché questo determina un notevole incremento dei dati raccolti ed analizzati, l'Acc ha richiamato l'attenzione sulla necessità di prevedere chiaramente se e come Europol potrà aver accesso ai dati e quali le responsabilità.