La direttiva relativa ad un quadro comune sulle firme elettroniche, adottata il 13 dicembre 1999 (1999/ 93/CE), dovrà essere trasposta negli ordinamenti nazionali dei Paesi U.E. entro il 19 luglio 2001. La previsione dell'emanazione di un decreto attuativo è contenuta nella legge comunitaria per il 2000 (Legge 29 dicembre 2000, n. 422) entro un anno dalla data di entrata in vigore della legge stessa (gennaio 2002).

La direttiva, come già evidenziato nelle precedenti relazioni, è finalizzata ad introdurre una cornice di regole armonizzate tra i paesi membri delle Comunità europee per l'utilizzo delle firme elettroniche e, quindi, a favorire lo sviluppo del commercio elettronico.

Pur riferendosi prioritariamente all'adozione di strumenti utili al settore privato, la direttiva prende in considerazione anche l'uso delle firme elettroniche nei rapporti con il settore pubblico e la pubblica amministrazione, a fini di semplificazione. Essa detta quindi regole per garantire il riconoscimento giuridico delle firme elettroniche ed evitare qualsiasi forma di discriminazione di queste, consentendo, in presenza di precisi requisiti di sicurezza, che le firme elettroniche possano avere valore di prova delle transazioni ed essere considerate pienamente equivalenti alle firme apposte manualmente.

Durante la discussione, la delegazione italiana di cui faceva parte l'Ufficio del Garante, ha lungamente insistito per far introdurre nel testo principi di rigore riguardo alla fissazione dei requisiti necessari per identificare una firma elettronica e prevedere specifiche garanzie e sistemi di verifica nei casi in cui sulla stessa si volesse fondare una presunzione di equivalenza con le firme manoscritte.

Di particolare importanza per il Garante gli articoli 6 (relativo alla definizione delle responsabilità), l'articolo 7 che disciplina gli aspetti internazionali (equivalenza dei certificati rilasciati da prestatori di servizi di certificazione stabiliti in Paesi terzi) e l'articolo 8 (relativo alla protezione dei dati personali, incluso l'uso dello pseudonimo).

Anche in questo caso sarà cura dell'Autorità formulare tutti i contributi necessari alla predisposizione del decreto legislativo di attuazione.

LA MODIFICA DELLA DIRETTIVA SULLA *PRIVACY* NELLE TELECOMUNICAZIONI E LA CONVENZIONE *CYBERCRIME*

85 LE PROSPETTIVE PER I DIRITTI DEGLI INTERESSATI

Come richiamato in precedenza, l'analisi complessiva riferita al settore delle telecomunicazioni deve tenere conto degli sviluppi intercorsi nel settore a livello comunitario.

A seguito del riesame effettuato nel corso del 1999 del quadro normativo dei servizi di comunicazione elettronica, la Commissione europea ha predisposto sei proposte intese a ridisegnare la nuova disciplina delle reti e dei servizi di comunicazione elettronica.

Le proposte, presentate il 12 luglio 2000 al Consiglio ed al Parlamento, comprendono: una direttiva-quadro che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica; una direttiva relativa all'autorizzazione per le reti e i servizi, che armonizza le norme esistenti per la loro fornitura; una direttiva relativa all'accesso alle reti ed alla interconnessione; una direttiva relativa al servizio universale ed ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica; una direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; un regolamento sull'accesso disaggregato al circuito di utente (*local loop*).

Scopo del complessivo intervento è quello di emanare regole neutrali rispetto alla tecnologia, garantendo che i servizi vengano disciplinati secondo modalità equivalenti, indipendentemente, quindi, dai mezzi e dalle modalità con cui sono prestati.

La revisione della direttiva 97/66/CE in questo quadro doveva, a parere della Commissione, essere limitato a poche modifiche, consistenti per lo più nell'adeguamento della terminologia. Gli unici interventi di merito inizialmente previsti, fermo restando il principio del rispetto del livello di tutela garantito a livello europeo nel campo della tutela dei dati personali, riguardavano: definizioni (art. 2); dati relativi al traffico e alla fatturazione (art. 6); dati relativi all'ubicazione (art. 9); elenchi degli abbonati (art. 12); comunicazioni indesiderate (art. 13).

Per quanto riguarda le definizioni, oltre al riferimento a quelle, generali, contenute nella direttiva che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica nonché nella

direttiva 95/46/CE; la proposta prevede un'apposita disciplina per alcune ipotesi in cui si è ritenuto necessario chiarire i concetti utilizzati nel testo. Sono state, ad esempio, introdotte le definizioni di dati di traffico, di dati di localizzazione, di comunicazione e di chiamata (che resta per quanto si riferisce agli ordinari e tradizionali sistemi di telefonia vocale), di servizi a valore aggiunto e di posta elettronica.

La proposta di direttiva mantiene fermi i principi-cardine dell'obbligo di provvedere alla sicurezza della rete per i fornitori, della riservatezza delle comunicazioni (art. 5) e del divieto dell'uso dei dati di traffico, con conseguente necessità di cancellare o rendere anonimi dati relativi ad una comunicazione all'atto del completamento della stessa, fatte salve le eccezioni individuate dall'articolo 6.

L'articolo 9 contiene una nuova previsione che, tenendo conto della possibilità di fornire servizi a valore aggiunto basati sulla localizzazione degli utenti mobili, introduce misure di protezione della vita privata degli utenti e degli abbonati che richiedano la fornitura di tali servizi.

La proposta contiene novità anche riguardo agli elenchi degli abbonati, per i quali prevede che sia lasciata al singolo abbonato la scelta del se comparire o meno negli elenchi e, in caso affermativo, di decidere quali dati debbano figurare, previa in ogni caso un'ampia ed esaustiva informazione delle finalità perseguite e dei possibili usi e la possibilità di ritiro del consenso prestato e le comunicazioni indesiderate, per le quali vige lo stesso principio del consenso preliminare. Da notare che il testo proposto include la posta elettronica e gli sms.

Come vedremo al paragrafo 87 il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ha dedicato una considerevole parte delle attività svolte nel corso dell'anno 2000 all'analisi degli aspetti salienti per la tutela delle persone in relazione alla revisione del quadro giuridico delle telecomunicazioni (parere 2/2000) ed in particolare, alla proposta di direttiva, sia per condividere le scelte effettuate in ordine all'uso degli elenchi pubblici per i servizi di ricerca derivata (parere 5/2000), sia per sottolineare alcuni rischi e lacune del provvedimento (parere 7/2000). Un ampio lavoro è stato svolto da un gruppo specializzato, la *Internet task force*, per individuare gli aspetti tecnici necessari per garantire la protezione dei dati *on-line;* in questo studio si prendono in esame, anche criticamente, le scelte operate dalla Commissione nella proposta di direttiva. La scelta di ampliare il campo di applicazione rispetto alla vigente direttiva 97/66/CE, infatti, se da un lato certamente risponde alle esigenze di una realtà in rapida e continua evoluzione, dall'altro esige che il livello di tutela garantito ai singoli non sia attenuato. Questo implica un'attenta lettura delle disposizioni e dei principi della direttiva 97/66/CE proprio per verificare se essi mantengono o meno intatta la loro validità.

La discussione della direttiva è iniziata nell'aprile 2001, subito dopo che il Consiglio dei ministri telecomunicazioni aveva raggiunto un accordo politico sul testo delle tre direttive "centrali" (la direttiva quadro sui servizi e reti di comunicazione elettronica e le direttive su accesso ed interconnessione e sull'autorizzazione delle reti e dei servizi).

Nel gruppo di lavoro, in cui l'Ufficio del Garante era presente come delegazione italiana, è stato possibile superare difficoltà e preoccupazioni di talune delegazioni, in particolare rispetto: a) alla scelta di lasciare liberi gli abbonati se comparire o meno (e se sì con quali dati) negli elenchi elettronici o cartacei; b) all'inserimento della posta elettronica e degli sms nel generale divieto di invio di comunicazioni indesiderate (che ha richiesto un apposito considerando per evitare sovrapposizioni e conflitti con la previsione dell'articolo 7 della direttiva sul commercio elettronico); c) sugli aspetti legati alle definizioni dei dati di traffico e di localizzazione.

Perplessità e difficoltà non ancora superate si sono invece riscontrate in relazione ad una forte spinta veicolata da non sufficientemente specificate "esigenze della giustizia e delle forze dell'ordine" tese ad introdurre nel testo elementi di indebolimento dei diritti. In particolare tentativi sono stati rivolti ad attenuare sia il principio della riservatezza delle comunicazioni (articolo 5), attraverso l'introduzione di ulteriori fattispecie derogatorie, sia del divieto della conservazione dei dati di traffico, previsto all'articolo 6, attraverso l'eliminazione dello stesso principio che prescrive la cancellazione o l'anonimizzazione dei dati al termine della comunicazione, fatte salve ipotesi espressamente disciplinate.

La proposta è stata anche esaminata nel Consiglio dei ministri delle telecomunicazioni nella riunione del 27 giugno 2001.

Poiché lo sviluppo e la rapida trasformazione che coinvolge in particolare l'Europa verso la "Società dell'informazione" raggiungono e toccano ogni aspetto della vita umana, inclusi lavoro, educazione, formazione, tempo libero, la Commissione, come si è ricordato, ha lanciato nel dicembre 1999 un'iniziativa, denominata *"eEurope"* per fare in modo che il continente europeo possa pienamente trarre i benefici derivanti dalle tecnologie digitali. Questo progetto, adottato dal Consiglio europeo di Feira, prevede una serie di azioni che coprono il periodo fino alla fine del 2002. Nel piano di azione grande attenzione è rivolta alla sicurezza delle reti ed alla lotta contro la criminalità informatica (*cybercrime*).

Esso tende a individuare le modalità e i mezzi per lottare al fine di prevenire lo sviluppo di attività criminali, che possono assumere le forme più varie ed avere una valenza offensiva non riconducibile ai confini nazionali. Il Consiglio d'Europa ha da tempo intrapreso l'elaborazione di una Convenzione

contro la criminalità informatica. Sul progetto di testo il Consiglio dell'Unione ha adottato una posizione comune e diversi strumenti singoli volti a comporre una strategia più generale. Recentemente, il Gruppo dei garanti dell'articolo 29 della direttiva, ha adottato il parere 4/2001 relativo al citato progetto di Convenzione.

Nella Comunicazione del 26 gennaio 2001, intitolata alla "*creazione di una società dell'informazione più sicura attraverso il miglioramento della sicurezza delle infrastrutture e la lotta alla criminalità legata all'uso del computer*", la Commissione europea, svolta un'accurata indagine sui temi di maggior criticità, propone diverse misure. Per il breve periodo, l'adozione di norme armonizzate per combattere la pornografia infantile e lo sfruttamento sessuale dei bambini. Nel medio periodo, invece, la presentazione di altre iniziative di armonizzazione per migliorare le risposte in relazione ai crimini tecnologici (*hacking* ed altri) e ad azioni contro il razzismo e la xenofobia, oltre alla proposta di applicare il principio di mutuo riconoscimento alle ordinanze emesse dai giudici in relazione ad indagini associate alla criminalità informatica che coinvolgano più di uno Stato membro.

Da notare che un aspetto cruciale della comunicazione è relativo alla conservazione dei dati. La Commissione propone che la necessità di adottare misure sul tema, in particolare di natura legislativa, sia verificata in prosieguo dalla stessa Commissione in base ai risultati di consultazioni. A tal fine ipotizza un *forum* di discussione per le forze di polizia, la magistratura, gli operatori *Internet* e quelli delle telecomunicazioni, le organizzazioni di tutela dei diritti civili, i rappresentanti dei consumatori e le autorità di protezione dei dati, nella convinzione, condivisa, che qualunque tipo di soluzione sia fondata su solide basi (normative), oltre che proporzionata e bilanciata rispetto alle diverse esigenze rappresentate.

ALTRE NOVITÀ NEL DIRITTO COMUNITARIO E NEL SETTORE GIUSTIZIA-AFFARI INTERNI

86. PROFILI GENERALI

Il gruppo di lavoro protezione dei dati del Consiglio dell'Unione ha completato la discussione in relazione alla proposta di regolamento del Parlamento e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni e degli organi della Comunità europea.

La proposta, presentata dalla Commissione nel settembre 1999, era intesa a dare attuazione al dettato dell'art. 286 del Trattato di Amsterdam e, pertanto, ad introdurre all'interno delle istituzioni e degli organismi comunitari un livello di tutela dei dati personali corrispondente a quello assicurato in ciascuno degli Stati membri con la trasposizione delle direttive comunitarie 95/46/CE e 97/66/CE, conferendo alla nuova autorità di controllo indipendente il compito di sorvegliare i trattamenti effettuati da queste.

L'Ufficio del Garante ha preso parte attiva ai lavori del gruppo ed al complessivo *iter* che ha portato all'adozione il 18 dicembre 2000 del provvedimento, divenuto poi il regolamento 45/2001 riportato nella documentazione allegata alla presente Relazione.

I principi di protezione dei dati contenuti nella proposta di regolamento sono basati sulle norme comunitarie esistenti e li integrano dettando specifiche disposizioni laddove la direttiva-quadro 95/46/CE lasci margini attuativi agli Stati.

Oltre alle regole generali che riguardano l'oggetto, le definizioni e il campo di applicazione – limitato alle attività che rientrano in tutto o in parte nell'ambito riservato al diritto comunitario – il regolamento riprende i principi della direttiva in materia di qualità e di legittimazione al trattamento, includendo disposizioni specifiche e dettagliate sul cambiamento di finalità e sul loro trasferimento. I principi sono disciplinati in tre distinti articoli, a seconda che il trattamento avvenga all'interno delle istituzioni ed organismi comunitari, verso destinatari soggetti o non soggetti alla direttiva 95/46/CE.

Particolare attenzione è prestata alle condizioni che legittimano il trattamento dei dati sensibili (articolo 10), all'informazione e ai diritti dell'interessato (di accesso, rettifica, blocco, cancellazione), comprensivi della notifica a terzi degli interventi effettuati a seguito dell'esercizio del diritto di accesso.

Si prevede inoltre l'istituzione della figura del responsabile della protezione dati all'interno di ogni istituzione ed organismo comunitario e la specificazione dei suoi compiti e diritti (articoli 24-26); si disciplinano poi le ipotesi in cui è necessario il preventivo avviso del "Garante europeo" rispetto a trattamenti di dati personali che possono comportare rischi.

Un capo apposito, il IV, è dedicato alla protezione dei dati personali e alla tutela della riservatezza nell'ambito delle reti interne di telecomunicazione, ed è ispirato in larga misura ai principi dettati dalla direttiva 97/66/CE.

L'ultimo capo prevede l'istituzione dell'autorità di controllo indipendente, denominata Garante europeo della protezione dei dati: si tratta di un organismo importante, che si colloca a fianco degli organismi comunitari esistenti, con requisiti di indipendenza marcati, sia nelle procedure di scelta, sia nei poteri conferiti ed infine nella attribuzione di ampia autonomia finanziaria ed amministrativa, con la previsione di una linea di bilancio dedicata e di una struttura amministrativa collocata alle sue dipendenze.

Il Garante europeo, che dovrà essere nominato di comune accordo dal Parlamento europeo e dal Consiglio in base ad una lista predisposta dalla Commissione a seguito di un bando pubblico a presentare le candidature, resterà in carica cinque anni, con mandato rinnovabile, e sarà affiancato da un Garante aggiunto, scelto con la medesima procedura e per la stessa durata.

All'Autorità compete sovrintendere al rispetto dei diritti e delle libertà fondamentali delle persone fisiche, in particolare tutelando il diritto alla vita privata nei riguardi dei trattamenti di dati personali effettuati da istituzioni ed organismi comunitari, sorvegliando ed assicurando l'applicazione del regolamento e delle direttive comunitarie in materia, anche attraverso pareri ed indirizzi da rivolgere agli stessi organismi ed istituzioni.

Il Garante europeo della protezione dei dati collabora con le autorità nazionali di controllo in materia di protezione dei dati e con le autorità comuni di controllo istituite da convenzioni internazionali stipulate in base al titolo VI del Trattato (cooperazione in materia di affari interni e giustizia). Partecipa inoltre alle attività del Gruppo per la tutela delle persone istituito dall'articolo 29 della direttiva 95/46/CE.

Tra le funzioni più rilevanti a lui attribuite vi sono la possibilità di trattare reclami ed adottare decisioni (anche svolgendo indagini di propria iniziativa), di sorvegliare l'evoluzione delle tecnologie (in particolare dell'informazione e della comunicazione, per gli aspetti di interesse della protezione dei dati personali), di consigliare istituzioni ed organismi comunitari, di emettere provvedimenti ritenuti necessari al titolare e responsabile del trattamento; di accedere ai locali ove si svolgono i trattamenti se necessario per l'espletamento dei suoi compiti; di adire la Corte di giustizia e di intervenire nelle cause avanti a tale organo nel caso in cui le norme non prevedano la prima possibilità.

Il regolamento è entrato in vigore nel gennaio 2001 e la procedura per la nomina del Garante europeo e del garante aggiunto dovrebbe aver luogo nel breve periodo.

Per quanto concerne il settore giustizia-affari interni, per la parte seguita dal Garante, è opportuno segnalare che il gruppo "Sistemi di informazione e protezione dei dati" ha completato i lavori di predisposizione di una proposta di decisione per la costituzione di un segretariato comune, per fornire supporto alle autorità di controllo già previste ed istituite dalle convenzioni Schengen, Europol e Sistema doganale. La creazione di una struttura di tal genere era in particolare caldeggiata dall'Autorità Schengen, la quale, a seguito dell'incorporazione, con l'entrata in vigore del trattato di Amsterdam, delle strutture Schengen in quelle del Consiglio dell'Unione europea, era rimasta senza segretariato e con seri problemi di bilancio e di partecipazioni alle riunioni.

Questa struttura, collocata presso il Consiglio anche se in forma tale da garantire la sua autonomia, è ora costituita dal segretario protezione dati, nominato a seguito di una procedura di selezione aperta e dal personale assegnatogli per l'espletamento dei compiti previsti dai regolamenti interni di ciascuna delle autorità comuni. Per quanto attiene al supporto amministrativo, consistente in uffici e materiale necessario, incluse le sale riunioni ed il servizio di interpretazione, spetta al Consiglio assicurarle; al Consiglio sono imputate pure le spese amministrative generali.

La proposta è stata approvata dal Consiglio dei Ministri della giustizia e affari interni nella seduta del 17 ottobre. La decisione è stata pubblicata sulla Gazzetta ufficiale delle Comunità europee. L'operatività della decisione è fissata al 1° settembre 2001.

La concreta entrata in funzione del segretariato comune chiarirà se, come temuto da alcune delegazioni, il legame di dipendenza che viene a crearsi con il Consiglio su elementi fondanti dell'indipendenza quali la provvista di uomini, supporti strumentali e mezzi economici, sia tale da incidere sul necessario carattere di indipendenza ed autonomia delle autorità di controllo.

Come ricordato nelle precedenti relazioni, l'attività e la ricostituzione del gruppo di lavoro era scaturita da una richiesta formulata dall'Italia di avviare una riflessione sui numerosi strumenti elaborati od in corso di elaborazione nell'ambito del c.d. "terzo pilastro" del Trattato di Maastricht che istituiscono sistemi automatizzati di elaborazione e di scambi di dati con mezzi automatizzati e cartacei, onde poter valutare successivamente la congruità dell'approccio seguito nel regolare il rapporto tra la protezione dei dati e le diverse forme di cooperazione ed assistenza per esigenze di giustizia e di polizia, e formulare eventualmente nuove modalità operative.

Ciò per tener conto dell'esperienza ed evitare nei lavori successivi:
– un obiettivo sovraccarico dell'attività dei gruppi di lavoro incaricati in seno al Consiglio dell'Unione di portare avanti la cooperazione nelle materie contemplate dall'art. K1 del Trattato, considerata anche la particolarità e la tecnicità delle disposizioni attinenti alla protezione dei dati e alle connesse garanzie per le persone interessate;
– la previsione di modalità differenziate per lo scambio dei dati e per l'esercizio nei diversi Paesi dei diritti di accesso, rettifica, cancellazione, ecc. previsti in materia di protezione dei dati;
– il rischio di disarmonie e/o disparità di trattamento rispetto a situazioni pure omogenee;
– una duplicazione di mezzi e di fondi soprattutto per quel che riguarda il funzionamento delle strutture di supporto delle diverse autorità comuni di controllo.

Nei successivi lavori si è mostrata una sicura preferenza per un approccio pragmatico ai temi proposti attribuendo priorità all'ultimo dei punti appena evidenziati, vale a dire la razionalizzazione delle strutture di supporto delle autorità comuni di controllo, soddisfatta con la ricordata decisione del 17 ottobre 2000.

Non altrettanta attenzione e volontà è stata posta riguardo al tema della definizione dei principi e si è tentato di riprendere l'argomento solo con la presidenza portoghese. Da questa è stato infatti presentato un documento recante "principi generali concernenti la protezione dei dati nel terzo pilastro", documento che costituisce il frutto della riflessione sui principi comuni già esistenti in materia di protezione dei dati in quanto derivanti dalla Convenzione n. 108 del Consiglio d'Europa e dalla direttiva 95/46/CE e di quelli in applicazione nel terzo pilastro (come ad esempio la Raccomandazione 87(15) del Consiglio d'Europa sui trattamenti effettuati nel settore della polizia).

Anche in questo caso si è proceduto con varie difficoltà. Da parte della delegazione italiana, che includeva l'Ufficio del Garante, si è dichiarata una disponibilità a contribuire all'elaborazione del citato documento sull'elaborazione dei principi, pur preferendo che questa fosse preceduta da una adeguata ricognizione delle norme e delle prassi, sia a livello nazionale, sia di accordi bi-multilaterali definiti dai Paesi membri.

La richiesta italiana muoveva dalla necessità di verificare attentamente i singoli aspetti della cooperazione tra le forze di polizia, tra queste e la magistratura, nonchè l'impatto che le norme in materia di protezione dei dati avevano avuto ed hanno sulle attività da esse svolte.

La profonda convinzione che l'introduzione di norme specifiche in materia di protezione dei dati non costituisce un *vulnus* dell'attività di inquirenti e polizia nella prevenzione e repressione dei reati, ma, anzi, ne consentono una maggiore incisività e trasparenza, ha determinato il Garante a curare nell'ambito del programma Falcone, un progetto denominato *"Lotta alla criminalità organizzata e protezione dei dati"*, del quale si tratterà più ampiamente nel prosieguo.

Il gruppo, dopo aver ritenuto che l'iniziale mandato fosse troppo vago, ha ricevuto dal Co.re.per. un nuovo mandato per redigere un *"progetto di risoluzione sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea"*.

Il progetto di risoluzione (si tratta di un atto non vincolante) si applicherebbe a tutti gli strumenti adottati, dopo la sua entrata in vigore, in base alle procedure del titolo VI del trattato, concernenti la cooperazione giudiziaria e di polizia in materia penale.

Ciascuno di questi strumenti dovrebbe poi precisare quali principi individuati negli articoli successivi siano da prevedere nello strumento in questione e per quali tipi di trattamenti. Negli stessi strumenti possono essere fissate deroghe ed eccezioni ai principi ritenuti applicabili (elencati al titolo II) che si rendono necessarie tenendo conto dell'oggetto o delle specificità dello strumento. Il titolo III, unico articolo, prevede che il rispetto dei principi relativi alla protezione dei dati personali sia sorvegliato da una o più autorità di controllo indipendenti.

La cooperazione tra autorità garanti in Europa

87. Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

Gli aspetti relativi alla tutela dei dati personali sono affrontati, come già indicato nella precedente relazione, dal "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" (organismo a carattere consultivo ed indipendente composto dai rappresentanti delle autorità di controllo nazionali, istituito dall'art. 29 della direttiva) e da un Comitato (previsto dall'art. 31 della stessa, che assiste la Commissione ed esprime il suo parere su progetti sottoposti dalla Commissione).

Nel corso dell'anno il Gruppo dei Garanti, presieduto dal prof. Stefano Rodotà, ha proseguito anzitutto i suoi interventi rispetto alla valutazione e delimitazione delle condizioni necessarie per giungere ad un'ipotesi di soluzione del negoziato con gli Stati Uniti e per definire le modalità attraverso le quali può essere consentito un trasferimento di dati personali verso o da quel Paese.

Il negoziato è stato assai intenso. Il testo finale dell'Accordo non recepisce tutte le indicazioni formulate dal Gruppo in diversi pareri, ma è comunque sensibilmente più attento ai diritti delle persone rispetto alle versioni originariamente discusse.

Oltre al negoziato con gli Stati Uniti, il Gruppo dei Garanti ha espresso propri pareri anche in ordine al progetto di decisione della Commissione sulle clausole contrattuali ai fini del trasferimento dei dati verso Paesi terzi (Parere 1/2001 del 26 gennaio 2001 WP 38), alla legge canadese in materia di informazioni personali e documenti elettronici (Parere 2/2001 del 26 gennaio 2001 WP 39) ed al livello di adeguatezza della legge australiana in materia di *privacy*, dettata per il settore privato (Parere 3/2001 del 26 gennaio 2001 WP 40).

Il Gruppo ha inoltre largamente concentrato i suoi lavori sulle sfide delle nuove tecnologie, in relazione alle quali è intervenuto adottando i pareri ricordati sopra al paragrafo 79.

È inoltre intervenuto, tra l'altro, su:

alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali (Parere 1/2000 doc. WP 28 adottato il 3 febbraio 2000);

problema del genoma (Parere 6/2000 doc. WP 34 adottato il 13 luglio 2000);

attuazione della direttiva 95/46/CE (Raccomandazione 1/2000 doc. WP 30 adottata il 3 febbraio 2000);

progetto di Convenzione del Consiglio d'Europa sulla criminalità informatica (Parere 4/2001 WP 41 adottato il 22 marzo 2001);

individuazione di alcuni requisiti minimi per la raccolta *on line* di dati personali nell'Unione europea (Raccomandazione 2/2001 doc. WP 43 adottata il 17 maggio 2001).

I documenti si trovano in allegato alla presente Relazione.

Da ultimo, il Gruppo ha approvato importanti documenti sulla protezione dei dati nel rapporto di lavoro e sul *panel* incaricato di seguire i casi applicativi del *Safe Harbor*. Ha costituito poi un gruppo di lavoro sull'uso delle tecnologie a fini di controllo sui luoghi di lavoro. Specifiche iniziative sono in atto per valorizzare gli atti adottati via Internet e attraverso pubblicazioni.

88. La partecipazione ad altri comitati e gruppi di lavoro

Il Garante, anche attraverso la partecipazione di funzionari dell'Ufficio, ha seguito attivamente ed attentamente gli sviluppi di alcune iniziative settoriali consistenti sia in gruppi di lavoro specifici costituiti in seno al Gruppo dell'articolo 29, sia scaturite da esigenze manifestatesi nel corso delle conferenze annuali dei Garanti europei.

Sotto il primo profilo, merita menzione il lavoro svolto presso la *Internet Task Force*, per brevità "ITF", nata nel 1999 con l'obiettivo di fornire un supporto conoscitivo integrato e sistematico alle attività del "*Data protection Working Party*" previsto dall'art. 29 della direttiva 95/46/EC, con particolare riguardo alla rete Internet ed in generale ai sistemi informativi *on-line*.

Nel corso degli ultimi due anni la "ITF" ha predisposto le bozze di alcuni documenti che sono poi stati adottati dal *Working Party*, per lo più sotto forma di raccomandazioni, allo scopo di migliorare la comprensione dei fenomeni per la tutela della *privacy* in rete.

Recentemente, con l'obiettivo di analizzare in maniera integrata quanto disposto dalle direttive 95/46/EC e 97/66/EC in merito alla protezione dei dati personali in generale e alla medesima tutela nello specifico settore delle telecomunicazioni, la *Internet Task Force* ha predisposto un voluminoso documento di lavoro, adottato il 21 novembre 2000 dal *Working Party*, dal titolo "*Privacy on the Internet – An integrated EU Approach to on-line Data Protection*".

Nel documento la "ITF", prevalentemente composta da esperti delle strutture nazionali per la protezione dei dati personali, compie una dettagliata analisi delle diverse tipologie dei servizi disponibili sulla rete Internet e una verifica delle norme applicabili in quanto tali, segnalando i rischi per ciascuna tipologia di servizio in relazione a carenze normative e/o tecnologiche.

Un ruolo importante hanno assunto nell'anno i seminari internazionali sulla trattazione dei ricorsi e delle segnalazioni ("*Complaints Handling Workshops*").

Facendo seguito ad un'esigenza manifestata nel corso della *Spring Conference of European Data Protection Commissioners* di Helsinki (aprile 1999), nel febbraio 2000 si è tenuto a Manchester il primo

seminario di una serie dedicata allo scambio di informazioni e alla definizione di un *modus operandi* comune per quanto concerne la trattazione dei ricorsi e delle segnalazioni presentate alle autorità nazionali per la protezione dei dati, con particolare riguardo ai casi che, per la loro rilevanza o per la natura delle parti interessate, travalicano l'ambito nazionale.

Al seminario, tenutosi il 7 e l'8 febbraio 2000, hanno partecipato i rappresentanti della quasi totalità delle autorità di garanzia nazionali dell'UE ed un rappresentante della Commissione. Le due giornate di studio sono servite a mettere a punto una sorta di decalogo per garantire un approccio comune alla trattazione dei ricorsi e delle segnalazioni con valenza "internazionale". Tale decalogo prevede, in particolare, l'opportunità di dare priorità ai ricorsi "internazionali" (caso per caso), di contattare l'autorità di protezione dati competente, di trasferire ogni elemento di prova utile alla valutazione del singolo caso (in conformità alle prassi nazionali), di garantire che le singole autorità si tengano reciprocamente informate. I risultati sono stati presentati alla Conferenza di primavera del 2000 tenutasi a Stoccolma, dove è stato deciso che, indicativamente, sarebbero stati due i seminari dedicati ogni anno al tema e che vi dovranno partecipare funzionari impegnati nel settore.

Su questa linea è proseguita l'attività durante il secondo seminario, svoltosi a L'Aja presso l'Autorità garante olandese (*Registratiekamer*) (26-27 ottobre 2000). Il seminario è stato organizzato in forma di *think tank*: le delegazioni partecipanti sono state invitate a presentare un caso significativo che illustrasse le modalità di trattazione dei *complaints*, possibilmente di ambito internazionale, e a riflettere sui possibili approcci comuni. Parallelamente è stato fatto circolare un questionario in cui si chiedeva a tutti i partecipanti di illustrare se e in che modo la singola autorità nazionale utilizzasse Internet per ricevere e/o rispondere a segnalazioni di singoli cittadini, o comunque per facilitare lo scambio di informazioni. L'autorità olandese ha illustrato il proprio modello di funzionamento, in cui un *front office* è deputato a gestire i casi (segnalazioni, richieste di parere, lamentele) risolvibili con maggiore facilità e secondo modelli già consolidati. Sono stati quindi illustrati vari casi nazionali, e per l'Italia, in particolare, il caso Gratistel (v. Relazione Annuale 1999), che aveva avuto un'eco a livello europeo come esempio di attività di tipo preventivo, non motivata da segnalazioni specifiche, bensì svolta prima dell'attivazione del servizio.

Durante l'ultima parte del seminario sono stati presentati i risultati del questionario relativo all'uso di Internet, dai quali è emerso che sostanzialmente tutte le autorità nazionali di protezione dati hanno un proprio sito *web* e lo utilizzano per scambiare informazioni con i cittadini. Tutte prevedono la possibilità di notificare i trattamenti per via informatica, con l'eccezione della Francia che esclude questa modalità in modo specifico (tranne per quanto concerne la notificazione dei siti *web*). Tutti hanno indicato l'opportunità di potenziare l'uso di Internet soprattutto quale strumento di sensibilizzazione del pubblico e dei titolari di trattamenti, oltre che di segnalazione di casi di interesse, anche se pochi (D-Berlino, Norvegia) prevedono espressamente invii e risposte via *e-mail*. È stata infine illustrata una proposta che, alla luce dei risultati di questo e del precedente seminario, prevede un sistema di scambio di informazioni relativo ai *complaints* "internazionali". Tale sistema si basa sull'utilizzo di moduli standard per sintetizzare i singoli casi, e sull'invio di questi moduli via Internet ad un punto centrale di coordinamento che provvede periodicamente (sempre via Internet) ad informare tutte le altre autorità sugli sviluppi e/o i problemi segnalati. Ciò al fine di facilitare e sviluppare la cooperazione tra le stesse autorità secondo quanto previsto dall'art. 28.6.§2 della direttiva 95/46/CE.

Gli sviluppi del seminario de L'Aja sono stati analizzati durante il successivo incontro, tenutosi ad Oslo il 29-30 marzo 2001. I rappresentanti della Commissione europea e dell'Autorità olandese hanno presentato il sito *web* denominato CIRCA (*Communication & Information Resource Center Administrator*), nel cui ambito è stato realizzato lo spazio virtuale che ospiterà il sistema di scambio di informazioni relativo a ricorsi, segnalazioni, reclami, ecc. che coinvolgano più autorità o abbiano comunque rilevanza internazionale. In proposito vi è un orientamento favorevole ad estendere la partecipazione anche alle autorità omologhe di altri Paesi europei con un adeguato livello di protezione dei dati, come la Svizzera e l'Ungheria. Si tratta di una *extranet* riservata alle autorità realizzata nel quadro del programma IDA della Commissione europea (e, quindi, gestita fisicamente mediante un *server* di quest'ultima), per il cui accesso sono previste opportune cautele. All'interno di tale spazio sono previste varie sezioni e, in particolare, una configurata più propriamente come "*newsgroup*", in cui sarà possibile presentare i procedimenti relativi a ricorsi e segnalazioni rispetto ai quali si intende scambiare informazioni con i colleghi delle altre autorità europee. Nella scheda-tipo da compilare per descrivere le caratteristiche dei singoli ricorsi non saranno riportate le generalità delle persone fisiche coinvolte, mentre si potranno indicare, se la legislazione nazionale lo consente, i nominativi di società o imprese, soprattutto quando il caso abbia risvolti internazionali. Ogni autorità ha provveduto ad individuare ed indicare i funzionari che fungeranno da tramite nazionale per il sito, con l'impegno di aggiornare tempestivamente le informazioni e trasmettere eventuali richieste di assistenza o chiarimento in materia di ricorsi (si è concordato che la lingua di lavoro sarà, salvo casi particolari, l'inglese). Il seminario si è suc-

cessivamente focalizzato sull'analisi di singoli casi di rilevanza internazionale, in particolare riguardo alla raccolta e all'utilizzazione di dati effettuata da siti Internet che si rivolgono a minori (come "*Kidlink*"). Le Autorità hanno deciso di condurre accertamenti in sede nazionale e di istituire un primo *newsgroup* all'interno del sito CIRCA dedicato appunto alla trattazione del caso "*Kidlink*" in modo da garantire un approccio quanto più possibile uniforme.

La delegazione italiana ha presentato un caso relativo al diritto di accesso dei dipendenti ai dati valutativi che li riguardano, il quale ha suscitato notevole interesse con riferimento alla nozione di "dato personale" e alle modalità di esercizio dei diritti dei lavoratori interessati (il Gruppo di lavoro ex art. 29 direttiva 95/46/CE ha infatti recentemente emanato una Raccomandazione su tale specifica materia). Si è concordato di istituire un secondo *newsgroup*, sempre all'interno del sito CIRCA, dedicato al problema della *privacy* sul luogo di lavoro con l'indicazione di approcci o materiali utili a sostenere le autorità nazionali nella trattazione di casi come quello italiano – allo scopo di fornire alle autorità giudiziarie nazionali eventualmente adite indicazioni sulla posizione comunitaria in ordine alla questione sottoposta ed un panorama complessivo della normativa e della giurisprudenza degli altri Paesi dell'UE.

L'AUTORITÀ COMUNE DI CONTROLLO SCHENGEN

89. IL RAPPORTO PER IL 1999-2000

L'Autorità comune di controllo (ACC) ha proseguito nel periodo in riferimento la sua attività istituzionale di verifica e controllo del funzionamento della parte centrale del Sistema di informazione Schengen.

La quarta relazione annuale di attività, relativa al periodo marzo 1999-febbraio 2000 è allegata alla presente Relazione; la quinta, relativa al periodo marzo 2000 - febbraio 2001, è in corso di predisposizione.

La relazione annuale dell'Autorità di controllo Schengen, forma oggetto, in uno spirito di trasparenza, di una presentazione pubblica anche per rendere conto ad un pubblico quanto più vasto possibile degli sforzi da essa compiuti al fine di difendere gli interessi dell'individuo nella tutela della vita privata.

L'ACC, anche basandosi su relazioni predisposte da gruppi di lavoro interni, ha formulato raccomandazioni, pareri, proposte e suggerimenti riguardanti sia il controllo della sicurezza del SIS, sia la tutela degli interessi dei singoli individui segnalati o, ancora, l'adempimento dell'obbligo d'informazione nei confronti del cittadino.

L'Autorità lamenta con decisione come, soprattutto a seguito dell'incorporazione di Schengen nelle strutture del Consiglio dell'Unione europea avvenuta con il Trattato di Amsterdam, il trattamento riservato alle sue proposte ed opinioni si è largamente deteriorato. L'ACC arriva a parlare di "trattamento ingeneroso riservato all'ACC, soprattutto per quanto concerne il debito rispetto della sua autonomia e rigorosa indipendenza e l'assegnazione delle risorse finanziarie necessarie per garantirle". Come già rilevato in precedenza è per questo che l'ACC ha salutato con favore la proposta di costituire un'unica struttura di supporto amministrativo per tutte le autorità operanti nel terzo pilastro e di cercare di prevedere effettivi riconoscimenti in termini di autonomia finanziaria ed organizzativa.

Tra i temi di maggior rilievo si segnalano:

Sicurezza degli uffici SIRENE

È proseguita l'opera di sensibilizzazione e di proposta. Sul punto della regolare verifica dei motivi di una interrogazione del SIS le autorità governative si sono dichiarate poco disponibili ad introdurre cambiamenti.

L'ACC, nel prendere atto della risposta, ha deciso di perseverare affinché la sicurezza degli uffici SIRENE sia migliorata e uniformata. Ha convenuto in particolare di stendere un questionario uniforme che permetta alle autorità nazionali di controllo per la protezione dei dati di effettuare le verifiche in modo armonizzato.

Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

Si tratta dell'interpretazione dell'articolo 102, paragrafo 1, della Convenzione, relativo alla conservazione dei documenti ad avvenuta cancellazione di una segnalazione, per il quale gli Stati membri agiscono in modo non uniforme: alcuni, infatti, conservano i documenti relativi alle segnalazioni dopo che queste sono state cancellate e li utilizzano per completare gli schedari di polizia. È in corso una valutazione da parte dei gruppi di lavoro in relazione alle osservazioni dell'ACC per verificare se occorra modificare il manuale SIRENE.

Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata

In caso di usurpazione d'identità alcuni Stati membri introducono nel SIS il nome del legittimo titolare dell'identità usurpata, mentre il bersaglio è piuttosto l'usurpatore.

Dopo un primo parere, cui hanno fatto seguito osservazioni e proposte, l'ACC, esaminate queste proposte nel dicembre 1999 e nel febbraio 2000, ha adottato un secondo parere, complementare al primo, nel marzo 2000. In esso si ribadisce il principio di proporzionalità, in virtù del quale non tutti i casi di usurpazione d'identità giustificano la segnalazione del nome del titolare legittimo e si sottolinea che l'elaborazione dei dati relativi alle persone la cui identità è stata usurpata potrà essere consentita solo previo libero ed esplicito accordo delle stesse o dietro loro richiesta. Nel parere si richiede anche che vengano previste altre misure, quali la possibilità di rilasciare al titolare legittimo dell'identità usurpata un documento supplementare, ad esempio integrativo al passaporto, che attesti che il titolare non è la persona che usurpa l'identità.

Controllo del C.SIS

Il gruppo tecnico appositamente creato dall'ACC costituito di esperti delle autorità di controllo nazionali, coordinato dal rappresentante lussemburghese, ha effettuato a suo tempo, su deliberazione dell'ACC, una visita di controllo. Dalla visita è emersa la possibilità di migliorare la sicurezza del sistema, per la quale sono state formulate specifiche raccomandazioni. Il livello di sicurezza è stato ritenuto globalmente soddisfacente. La relazione riservata sulla visita di controllo è stata approvata nel febbraio 2000 ed è stata trasmessa, corredata di una sintesi, al Comitato dell'articolo 36.

Campagna d'informazione sui diritti dei cittadini nei confronti del SIS

L'ACC ha valutato gli esiti della campagna di informazione svolta in quasi tutti i Paesi Schengen, ritenendola soddisfacente. Come risulta anche per l'Italia, l'efficacia della campagna informativa si può misurare considerando l'aumento delle richieste di verifica e, in generale, del ricorso alle autorità di protezione dei dati personali da parte di persone cui è stato in particolare negato un ingresso od un visto in relazione a dati personali contenuti nelle sezioni nazionali del SIS.

Va infine segnalato che dal 1° gennaio 2000 vi è stato un cambiamento ai vertici dell'ACC, del quale il segretario generale del Garante mantiene la vice presidenza. Il mandato del presidente e del vicepresidente è stato rinnovato per un anno nella riunione del 13 dicembre 2000.

EUROPOL

20. L'ATTIVITÀ DELL'AUTORITÀ COMUNE DI CONTROLLO E I PRIMI CASI DI CONTENZIOSO

L'Autorità comune di controllo sui trattamenti effettuati da Europol ha largamente concentrato i suoi lavori sulla valutazione dei progetti di apertura di archivi di analisi suggerendo, ove necessario, integrazioni e specificazioni alle Autorità Europol.

Ha inoltre espresso pareri informali con riguardo all'apertura delle trattative per la stipulazione di accordi con Stati ed organismi terzi ed Europol per lo scambio di dati ed informazioni e successivamente, per alcuni Stati, in relazione all'apertura dei negoziati.

L'Autorità ha inoltre affrontato temi legati a modi e forme con cui assicurare visibilità alla sua attività e agli atti adottati ed ha iniziato al riguardo una riflessione sui tipi di documenti per i quali può essere consentito l'accesso al pubblico.

Quanto al primo aspetto si sta lavorando per predisporre un documento di presentazione dell'Autorità e dei suoi compiti che sarà collocato nel formato elettronico nel sito di Europol ed in un opuscolo da distribuire.

Nel corso del 2001 è prevista la redazione della prima relazione di attività che, per l'Italia, sarà allegata, come quella dell'ACC Schengen, alla relazione annuale del Garante.

Al comitato ricorsi è stato sottoposto un primo caso, attualmente all'esame preliminare per valutarne l'ammissibilità.

IL CONTROLLO SUL SISTEMA INFORMATIVO DOGANALE

91. LA CREAZIONE DELL'AUTORITÀ DI CONTROLLO

L'Autorità di controllo non ha iniziato formalmente la propria attività poiché mancano ancora le designazioni di alcuni Stati membri, e la sua composizione non è al momento sufficiente per consentirne l'operatività.

Anche questa Autorità comunque potrà avvalersi del menzionato segretariato comune.

EURODAC

92. COLLABORAZIONE TRA STATI MEMBRI E GARANZIE PER GLI INTERESSATI

A seguito dell'entrata in vigore del regolamento istitutivo del Garante europeo, i compiti di supervisione e controllo sui trattamenti effettuati ai sensi del regolamento Eurodac saranno sottoposte a questa figura di garanzia.

CONSIGLIO D'EUROPA

93. LA CONVENZIONE SUL *CYBERCRIME*

Il Consiglio d'Europa è stato uno dei primi organismi internazionali a dedicare specifiche iniziative alla tutela delle persone rispetto al trattamento dei dati personali. Dopo l'adozione di una serie di provvedimenti settoriali, nel 1981 si è giunti come è noto all'approvazione della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, che costituisce uno dei documenti fondamentali in tema di protezione dati e rappresenta il fondamento sul quale sono state costruite le successive regolamentazioni in ambito comunitario e nazionale.

L'attività del Consiglio d'Europa in materia non si è esaurita con l'approvazione della Convenzione, essendosi sviluppata in un'intensa attività di elaborazione della normativa di settore cristallizzata nelle note Raccomandazioni, nonché proseguendo con l'aggiornamento di quella preesistente.

Il Garante, sin dalla sua costituzione, ha continuato a prendere parte alle diverse attività del Consiglio d'Europa, contribuendo significativamente all'elaborazione dei diversi testi in discussione.

In particolare è continuato l'esame e l'approfondimento dello studio sulla Convenzione concernente il *cybercrime* per la lotta alla "criminalità informatica", vale a dire delle attività criminali realizzate attraverso l'impiego di strumenti telematici. La Convenzione mira a favorire la cooperazione internazionale nella lotta alla criminalità informatica attraverso l'armonizzazione delle procedure e il potenziamento dell'assistenza giudiziaria in questi settori. L'Assemblea Parlamentare del Consiglio d'Europa e ha espresso il 24 aprile 2001 un avviso che condivide le preoccupazioni dei Garanti europei.

Il testo predisposto ha destato infatti preoccupazioni nel Gruppo dell'articolo 29, che ha voluto esplicitare, nel parere 4/2001, i rischi che esso comporta sotto il profilo della protezione dei diritti umani fondamentali e della vita privata in particolare. Ulteriori note sono state poi inviate dal presidente del Gruppo.

Un punto esplicitamente e specificamente trattato, oramai divenuto un tema centrale su cui anche recentemente le autorità garanti europee si sono espresse negativamente con fermezza nelle Conferenze di Stoccolma ed Atene, concerne la conservazione più o meno generalizzata dei dati di traffico.

94. L'ATTIVITÀ DEI GRUPPI DI ESPERTI

È stato adottato dal gruppo CJ-PD che si occupa dell'elaborazione dei progetti di raccomandazione in materia di dati personali, il documento finale relativo al progetto di Raccomandazione che concerne la tutela dei dati personali raccolti e trattati a fini assicurativi, trasmesso per competenza, al Consiglio dei Ministri.

Altre iniziative hanno riguardato:

a) il parere del gruppo J-PD sul progetto di raccomandazione DH-S-AC per l'accesso ai documenti ufficiali;

b) la riorganizzazione degli organismi che hanno competenza in materia di protezione dati e le nuove metodologie di lavoro;

c) la celebrazione del ventesimo anniversario della Convenzione, anche in occasione della conferenza multilaterale di Varsavia sulla protezione dei dati promossa dal Consiglio d'Europa e dall'Autorità garante polacca il 19/20 novembre 2001;

È stato inoltre costituito un qualificato gruppo di lavoro, di cui fa parte anche il segretario generale del Garante, per approfondire, anche alla luce dei risultati del "Progetto Falcone", gli aspetti relativi all'applicazione dei principi di protezione dei dati all'attività di polizia (e giudiziaria) e per una valutazione della Raccomandazione 87/15 del Consiglio d'Europa.

95. LINEE-GUIDA IN MATERIA DI SORVEGLIANZA

In particolare, per le attività di videosorveglianza che presentano specifiche problematiche per la protezione dati, il Consiglio d'Europa ha conferito uno specifico incarico al segretario generale del Garante, per predisporre un dettagliato rapporto finalizzato alla ricerca di un corretto bilanciamento tra le esigenze di sicurezza e di controllo anticrimine e il diritto dei cittadini a difendere la loro sfera privata e la loro libertà.

Come è noto, il radicarsi di un fenomeno di espansione incontrollata del numero di impianti di videosorveglianza in luoghi pubblici e privati solleva non poche preoccupazioni nella società di oggi, attesa la loro invasività, specie in mancanza di una tutela diretta, salvo quella rappresentata, a livello embrionale, da una legge generale come la legge italiana n. 675/1996.

Il rapporto predisposto e pubblicato è volto, in particolare, alla protezione dei dati personali in relazione ai sistemi di videosorveglianza che ricadono, in senso lato, nell'ambito applicativo della Convenzione n. 108/1981 della Convenzione sulla tutela dei diritti dell'uomo e delle libertà fondamen-

tali, nonché di alcune Raccomandazioni del Consiglio d'Europa (in particolare, la N.R. (87) 15 in materia di trattamenti nell'ambito della pubblica sicurezza; la N.R. (89) 2 sulla protezione dei dati personali nel rapporto di lavoro e la N.R. (95) relativa alla protezione dei dati personali nel settore dei servizi di telecomunicazione, adottate in settori che pur non riferendosi espressamente alla tematica della videosorveglianza recano disposizioni e garanzie rilevanti sotto tale profilo).

In tale documento, presentato sotto forma di decalogo, sono state anche tracciate le prime linee-guida finalizzate alla piena garanzia e tutela del privato.

Le regole di base ivi enucleate si riportano di seguito sinteticamente:

– verificare che l'attività di sorveglianza si esplichi su base legale per fini leciti, espliciti e legittimi;

– adottare tutte le misure volte ad assicurare che l'attività sia conforme alla normativa in materia di protezione dei dati personali;

– ricorrere alla videosorveglianza solo quando non sia possibile utilizzare sistemi meno invasivi ed intrusivi della *privacy*;

– rispettare il principio di selettività e di proporzionalità in rapporto agli scopi perseguiti nei singoli casi, in modo da prevenire conseguenze irragionevoli sulle libertà e sui comportamenti degli interessati;

– rispettare il principio di pertinenza e di non eccedenza rispetto a immagini, suoni e dati biometrici raccolti, con particolare attenzione alle modalità di raccolta onde evitare che le informazioni raccolte siano registrate, indicizzate o conservate per lunghi periodi;

– evitare che l'attività di videosorveglianza possa determinare discriminazioni o possa essere disposta nei confronti di soggetti per il solo fatto di avere determinate opinioni, convinzioni o comportamenti di tipo sessuale;

– svolgere l'attività nel rispetto del principio di trasparenza e di pubblicità;

– assicurare maggiori garanzie in presenza di particolari rischi per gli interessati e di controllo;

– escludere, in linea di principio, la diffusione e la comunicazione dei dati personali a soggetti non interessati all'attività di sorveglianza;

– regolamentare il diritto di accesso, nonché gli altri diritti delle persone interessate;

– assicurare un'adeguata informativa ai lavoratori interessati e una possibile intesa con le organizzazioni sindacali per esigenze organizzative e/o produttive o per ragioni di sicurezza del lavoro che possano comportare un controllo a distanza.

Il rapporto e le linee-guida, dopo l'esame da parte del Gruppo, sono stati pubblicati, per un'ampia consultazione, sul sito web del Consiglio d'Europa. Quest'ultimo, dopo il parere favorevole del Gruppo di cui all'articolo 29 e un nuovo positivo esame da parte del CJ-PD-GC si accinge ad adottarlo formalmente.

O.C.S.E.

96. I RISULTATI CONSEGUITI NEL 2000

Il Garante, nel processo avviato dall'Organizzazione per la cooperazione e lo sviluppo economico, incentrato sui principi affermati nelle linee-guida sulla tutela della *privacy* per favorire la libera circolazione delle informazioni tra gli Stati membri, ha svolto, nel corso del 2000, un'intensa attività attraverso il Comitato ICCP (Comitato per la politica dell'informazione istituito all'interno della Direzione scienza, tecnologia e industria OCSE).

Tale attività è stata principalmente finalizzata a risolvere i problemi legati al commercio elettronico, alla sicurezza dell'informazione, alla protezione della *privacy* e all'infrastruttura della società dell'informazione.

Particolare valenza ha avuto la partecipazione del Garante alla riunione del sottogruppo WISP del Comitato ICCP, che espleta attività per la sicurezza dell'informazione e sulla *privacy*.

Nel corso della riunione indetta il 4- 5 maggio 2000 a Parigi sono state affrontate ed approfondite le principali tematiche relative:

– allo studio per la realizzazione e predisposizione a livello internazionale della Convenzione sui crimini informatici e, in ambito nazionale, la predisposizione di una specifica legge per combattere il c.d. *cybersquatting*;

– alla previsione dei criteri da utilizzare per la revisione delle linee guida sulla cifratura adottata dall'OCSE nel 1988;

– all'utilizzo del *software "generator"*, costituito da una serie di maschere da riempire con dati sensibili che vengono richiesti all'utente e che nel futuro formeranno oggetto di una raccolta di dati utilizzabile da organizzazioni che operano nel campo dell'*e-commerce*;

– alla predisposizione di un documento riguardante l'adozione di soluzioni contrattuali volte a consentire flussi transnazionali di dati TBDF (*Transborder data flow*) nel rispetto dei principi in tema di *privacy*.

Il gruppo si è adoperato, inoltre, per offrire strumenti metodologici e tecnici in relazione alle azioni da intraprendere ed indicando i tempi da rispettare per il raggiungimento dei suddetti importanti obiettivi.

ULTERIORI INIZIATIVE

97. IL "PROGRAMMA FALCONE" E LE ALTRE ATTIVITÀ

Il programma è stato avviato con il contributo finanziario delle istituzioni comunitarie per sostenere l'azione degli Stati membri volta ad intensificare la cooperazione in materia di giustizia ed affari interni.

Il Garante ha presentato nei primi mesi del 1999 una domanda per il cofinanziamento, nell'ambito del "Programma Falcone", di un progetto denominato "Attività di contrasto del crimine e tutela dei dati personali".

Per lo svolgimento dei seminari sono stati scelti due luoghi simbolicamente importanti: la sede di Europol a L'Aja per il primo (27 e 28 marzo 2000) e la Scuola nazionale della magistratura a Parigi per il secondo (6 e 7 luglio 2000).

Il progetto prevedeva una giornata conclusiva per presentare il lavoro svolto e formulare eventuali osservazioni e proposte, che si è svolta a Roma il 20 dicembre 2000; all'incontro, ospitato dalla Camera dei deputati, vi è stata un'ampia partecipazione e numerosi relatori.

Il progetto è stato indirizzato a magistrati, appartenenti alle forze di polizia e funzionari pubblici che nei Paesi membri dell'Unione svolgono prevalentemente la propria attività nel settore della prevenzione e contrasto della criminalità organizzata.

Al fine di individuare i soggetti dotati della competenza specifica per poter partecipare ai seminari dell'Aja e di Parigi, si è chiesta la collaborazione delle altre Autorità garanti in materia di protezione dei dati, nonché quella dei Ministeri della giustizia e dell'interno dei Paesi destinatari dell'azione. La finalità del progetto era quella di verificare gli aspetti dell'azione di polizia e giudiziaria legati alla raccolta, al trattamento, all'analisi dei dati, considerato l'intenso sviluppo di forme di collaborazione nelle attività di polizia e, più recentemente, giudiziarie in relazione al perseguimento dei compiti di prevenzione e repressione della criminalità, che determina un uso sempre maggiore di strumenti informativi e, talora, la creazione di veri e propri "sistemi". Attraverso lo stimolo della partecipazione attiva nei seminari si voleva ottenere un approccio "multidisciplinare", nel senso di confrontare le specifiche esperienze professionali con la normativa di tutela dei dati personali anche in linea con quanto suggerito dalla ricordata azione comune. In essa si fa infatti riferimento alla possibilità di definire norme e metodologie comuni al fine di facilitare l'individuazione del fenomeno e la raccolta dei dati da ottenere, però, tenendo conto della legislazione degli Stati membri in materia di protezione dei dati.

Gli approfondimenti condotti nei seminari e le risposte fornite ai questionari hanno evidenziato come su alcune questioni importanti i cittadini dei Paesi dell'Unione ricevono, nei rispettivi ordinamenti nazionali, trattamenti diversificati sotto il profilo dei diritti. In alcuni casi attività svolte dagli uffici di polizia non sono puntualmente o affatto disciplinate.

Ad esempio, per quanto riguarda la videosorveglianza non è risultato che vi sia una base giuridica uniforme: in alcuni Paesi si applicano i principi generali in materia di protezione dei dati personali, ma esistono poche norme specifiche che disciplinano i termini della conservazione delle immagini e registrazioni effettuate. Le osservazioni scaturite dal dibattito e la recente esperienza del Consiglio d'Europa sul tema costituiscono senza dubbio utili indicatori ai fini di un eventuale intervento armonizzatore.

Analogamente il problema si pone per i tempi e le modalità di conservazione dei dati relativi al traffico telefonico, per le modalità di accesso delle forze di polizia e dell'autorità giudiziaria agli elenchi degli abbonati di servizi telefonici, inclusi quelli di telefonia mobile. Per quanto concerne poi le carte telefoniche ricaricabili, varie soluzioni volte a consentire l'individuazione degli acquirenti sono basate solo sulla prassi e non su norme specifiche. L'esigenza di armonizzazione che sembra porsi anche in questo campo potrà forse essere considerata in occasione della discussione delle proposte di direttiva presentate recentemente dalla Commissione al Consiglio telecomunicazioni.

Anche riguardo alle modalità di raccolta e di trattamento dei dati genetici, l'utilizzo degli stessi, i tempi di conservazione ed i diritti delle persone cui si riferiscono mancano disposizioni adeguate nei sistemi processuali e certamente gli argomenti richiederanno un'ulteriore riflessione ed armonizzazione.

L'esperienza del Progetto ha mostrato come vi sia la crescente tendenza a prevedere obblighi, in via legislativa od anche amministrativa, di raccolta e conservazione di consistenti masse di informazioni. Rispettando la necessità di disporre, per l'azione di contrasto della criminalità, di un ampio materiale investigativo, manca un'armonizzazione o un indirizzo comune. Dall'analisi delle risposte ai questionari emerge senz'altro un problema rispetto alla rilevazione delle presenze alberghiere. L'Accordo di Schengen obbliga ad identificare i cittadini stranieri e comunitari, ma nei diritti nazionali variano le modalità di rilevazione (che in taluni casi riguardano i soli stranieri, in altri tutti i clienti, anche se cittadini del medesimo Paese). Sono diversi gli strumenti di rilevazione, in alcuni casi cartacei, in altri accessibili *on-line* per le forze di polizia e gli inquirenti. Variano ancora le modalità ed i tempi di conservazione, né sono noti i sistemi seguiti per la classificazione di queste informazioni (*files disgiunti* o creazione di un'unica banca dati).

La questione è però molto più ampia; andrà riproposto nel prossimo futuro il tema dell'imposizione a terzi, siano essi un *provider* per l'accesso ad Internet o singoli cittadini, dell'obbligo di consentire la raccolta o la conservazione di masse di informazioni.

Per quanto concerne le attività di competenza della magistratura penale, che recentemente ha iniziato a disporre di forme di supporto e cooperazione a livello europeo, si sono riscontrate maggiori difficoltà nell'accettazione delle disposizioni in materia di protezione dei dati, ritenendo alcuni che debba tenersi in maggior conto la speciale collocazione dell'ordine giudiziario nella disciplina dell'ambito di competenza delle autorità amministrative ed indipendenti di controllo.

Per il Garante, l'esperienza è stata di grande interesse ed utilità, sia per approfondire alcuni temi di rilevante attualità nel nostro Paese, sia per valutare la possibilità di operare suggerimenti per proseguire l'opera di individuazione e di definizione di norme specifiche per la tutela dei diritti nell'ambito delle attività di polizia e giustizia.