In un caso specifico (ove un'Amministrazione comunale ha preteso l'esposizione sui contrassegni necessari per l'accesso delle generalità dell'intestatario dell'autovettura) sono state richieste al Comune ulteriori informazioni, richiamando il principio in base al quale i dati trattati dalle pubbliche amministrazioni devono essere pertinenti e non eccedenti rispetto alle finalità perseguite, principio che costituisce applicazione dei criteri generali di ragionevolezza e proporzionalità.

Ciò nella consapevolezza, che ha ispirato altri pareri forniti dall'Autorità, che le esposizioni dell'immagine e dei dati delle persone, non necessarie né correlate allo svolgimento di funzioni pubbliche, favoriscono interferenze che contribuiscono a limitare la sfera di effettiva autodeterminazione del singolo.

## 4.19. Trasferimento di dati all'estero.

Per essere incisiva, la protezione dei dati personali non può trascurare il fenomeno della circolazione transfrontaliera dei dati.

Questo profilo ha occupato un posto centrale sia nella Convenzione del Consiglio d'Europa, sia nella direttiva comunitaria n. 95/46/CE.

La Convenzione n. 108 del 1981, intesa a "garantire nel territorio degli Stati contraenti, ad ogni persona fisica, indipendentemente dalla sua nazionalità e dalla sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, con particolare riferimento al diritto alla vita privata, in relazione alla elaborazione automatica dei dati a carattere personale che lo riguardano" (art. 1), si occupa del flusso transfrontaliero dei dati, prevedendo, da un lato, la definizione in ciascun Paese di un sistema normativo quanto più possibile uniforme, in modo da ridurre il pericolo di abusi nell'utilizzazione di tali flussi e la conseguente elusione delle rispettive legislazioni nazionali. D'altro lato, si è proibito o sottoposto ad una autorizzazione speciale, salve eccezioni espressamente stabilite, il flusso transfrontaliero dei dati a carattere personale destinato al territorio di un'altra parte contraente.

Con l'approvazione della direttiva comunitaria n. 95/46/CE, il legislatore comunitario ha dettato regole e criteri uniformi per la protezione dei dati nel territorio comunitario, al fine di evitare che la disciplina comune possa essere elusa dal mero spostamento fisico dell'attività disciplinata nella direttiva. Il capo IV della direttiva è interamente dedicato al trasferimento dei dati verso Paesi terzi.

In particolare l'art. 28 fissa un principio importante secondo cui il trasferimento dei dati personali è consentito soltanto se il Paese terzo garantisce un livello di protezione "adeguato". La Commissione Europea svolge un ruolo centrale nella valutazione sull'adeguatezza del livello di tutela esistente negli Stati membri.

L'art. 26 della direttiva individua le condizioni in base alle quali il principio dell'adeguatezza può trovare eccezioni. In tali casi (esistenza del consenso dell'interessato, conclusione o esecuzione di un contratto, salvaguardia di interessi pubblici; utilizzo di informazioni estraibili da un elenco pubblico o accessibile al pubblico), il trasferimento di dati può essere consentito verso un Paese che non garantisce una tutela adeguata.

Lo Stato deve informare sia la Commissione CE sia gli altri Stati membri sulle autorizzazioni in deroga concesse, e deve uniformarsi alle decisioni che la Commissione può assumere.

Per tale ultimo aspetto, è stata segnalata l'esigenza di perfezionare il modello procedimentale necessario agli Stati membri per conformarsi alle decisioni demandate alla Commissione.

Le disposizioni comunitarie in materia, definite dalla stessa direttiva come inderogabili, sono state recepite nella legge n. 675/1996 all'art. 28, il quale attua il principio dell'adeguatezza ma, al tempo stesso, prevede in termini più garantisti il divieto di trasferimento dei dati "sensibili" e di alcuni dati di carattere giudiziario per il caso in cui il Paese destinatario non assicuri un grado di tutela pari a quello assicurato dalla normativa nazionale.

In tal modo, è stata assicurata una valutazione differenziata in base alla tipologia dei dati da trasferire ed in base al Paese di destinazione.

Il Garante, anche in risposta ad alcuni quesiti formulati da parte di titolari del trattamento, ha fornito indicazioni e suggerimenti allo scopo di semplificare anche in tema di flussi transfrontalieri l'applicazione della legge.

E' stato, anzitutto, evidenziato che la legge (art. 26) non prevede alcuna notificazione qualora il trasferimento di dati all'estero riguarda dati che si riferiscono a persone giuridiche pubbliche o private, enti o associazioni, ovvero nel caso in cui (art. 28, comma 1) il trasferimento di dati personali è diretto unicamente verso Paesi appartenenti all'Unione Europea, purché non si tratti di dati "sensibili" o di carattere giudiziario.

La notificazione è invece necessaria nel caso in cui i dati personali siano trasmessi verso un Paese non appartenente all'Unione Europea; in tal caso, il trasferimento può avvenire dopo 15 giorni dalla data di notifica.

Qualora si intendono trasferire all'estero dati sensibili o relativi a provvedimenti giudiziari a carico dell'interessato, è necessario notificare la circostanza al Garante e attendere 20 giorni prima di effettuare la comunicazione dei dati, indipendentemente dal fatto che lo Stato di destinazione sia appartenente o meno all'Unione Europea.

L'Autorità ha peraltro sottolineato, al pari di quanto indicato nella direttiva europea 95/46/CE, che il trasferimento di dati all'estero è comunque consentito laddove ricorra taluno dei presupposti indicato dall'art. 28, comma 4, (ad esempio, qualora l'interessato abbia espresso il proprio consenso al trasferimento, oppure quando tale operazione sia necessaria per eseguire obblighi derivanti da un contratto di cui sia parte l'interessato).

La notificazione del trasferimento dei dati può essere effettuata utilizzando il modello previsto per la notificazione "generale", ed è possibile dichiarare in un unico contesto l'intero complesso delle attività di trasferimento. La notificazione dovrà essere annotata a cura del Garante in un'apposita sezione del registro dei trattamenti.

Il Garante ha più volte precisato che il trasferimento può essere vietato a seguito di una concreta valutazione che tiene conto delle modalità di trasferimento, dei trattamenti previsti oltre frontiera, delle relative finalità, della natura dei dati e delle misure di sicurezza adottate.

E' opportuno evidenziare che l'attuale disciplina in materia di trasferimento di dati, analogamente a quanto accadrà per molti settori interessati dalla protezione dei dati, subirà importanti integrazioni con l'emanazione dei decreti delegati, in particolare per ciò che riguarda l'individuazione delle modalità di applicazione della disciplina sulla protezione dei dati ai servizi di comunicazione e di informazione offerti per via telematica (art. 1, comma 1, lett. *n)* della legge n. 676/1996).

Il decreto delegato dovrebbe interessare, in qualche modo, anche il complesso flusso di dati in ambito *Internet*.

Avvalendosi dell'indicazione contenuta nella direttiva - quadro (considerando n. 47), l'Italia sarà il primo Paese europeo ad aver emanato una disposizione di legge che prende atto della necessità di dover modulare, anche in rapporto ad *Internet*, la normativa sulla protezione dei dati.

Nell'attesa di un quadro più chiaro sul piano internazionale, il principio che sta maturando è quello di garantire il rispetto della *privacy* nell'ambito delle reti aperte attraverso una strategia diversificata e globale, consistente, tra l'altro, in:

— sviluppo di nuove tecnologie "pulite" che assicurino già sul piano tecnico elevati livelli di sicurezza e di protezione della *privacy;*

— strumenti di "autodifesa" da parte degli utenti, che permettano loro, sulla base di un'idonea informativa, di accertarsi del livello di sicurezza offerto dal fornitore di servizi cui si rivolgono;

— strumenti contrattuali e regole di autodisciplina adottate su impulso dei *provider;*

— cooperazione internazionale ed eventuale creazione di un nucleo circoscritto di regole giuridiche non soggette a rapida obsolescenza;

— diffusione della consapevolezza che *Internet*, per quanto in frenetica evoluzione e con capacità altamente diffusive, è pur sempre un *media* e, pertanto, agli abusi commessi in rete si possono applicare alcune norme riguardanti i comportamenti *off-line.*

Il decreto delegato potrà indicare soluzioni differenziate agli interrogativi esistenti sugli adempimenti, sui compiti e sulle responsabilità dei soggetti che operano quali fornitori di reti, di servizi, di accessi e di contenuti.

In tale ottica il Garante, oltre a partecipare attivamente nelle sedi internazionali competenti, si è attivato per organizzare nel prossimo 8/9 maggio un convegno internazionale da tenersi a Roma sul tema.

## 4.20. Raccolta di firme per iniziative referendarie.

Nei primi mesi di attività, sono pervenute alcune segnalazioni sulla diffusione di moduli per la raccolta di firme relative ad iniziative referendarie, nei quali è stata prospettata la possibilità di utilizzare e di divulgare i dati acquisiti anche al fine dell'invio di proposte ed informazioni commerciali, scientifiche, campioni gratuiti di prodotti ed omaggi, sondaggi di opinione.

La raccolta e l'utilizzazione di dati personali connesse all'esercizio di un diritto politico fondamentale, come la sottoscrizione di richieste referendarie, devono essere del tutto distinte dai trattamenti delle stesse informazioni per ulteriori finalità di carattere commerciale o pubblicitario.

Mentre nel primo caso non è richiesto alcun particolare adempimento ai sensi della legge n. 675/1996, in quanto sulla base delle disposizioni vigenti i promotori del referendum sono tenuti a raccogliere i dati personali dei sottoscrittori e a darne comunicazione agli organi preposti alla verifica della regolarità delle richieste (non essendo necessario un consenso ulteriore rispetto alla sottoscrizione), nella seconda ipotesi il

Comitato avrebbe dovuto acquisire il consenso dei cittadini elettori, dando ad essi un'ampia informazione sugli specifici aspetti dei successivi trattamenti dei dati non collegati alle procedure referendarie.

Il cittadino non deve sentirsi o essere costretto, per partecipare alla presentazione di un referendum che sente di condividere, ad autorizzare un trattamento "automatico" dei suoi dati personali anche per finalità non strettamente collegate alle attività referendarie.

Sulla base di queste considerazioni, il Garante, a seguito dei chiarimenti forniti dai rappresentanti dei Comitati promotori del referendum, ha adottato a fine luglio un provvedimento con il quale ha invitato i Comitati stessi a separare dalla sottoscrizione necessaria per la richiesta referendaria la parte relativa alla dichiarazione del consenso per l'utilizzazione dei dati a fini diversi da quelli connessi all'iniziativa, oppure ad astenersi da tali richieste.

Inoltre, l'Autorità ha segnalato ai Comitati di astenersi dal compiere qualsiasi operazione di trattamento al di fuori di quanto richiesto dalla legge per le iniziative referendarie, e a fornire ai sottoscrittori un'informativa rispondente ai princìpi dalla legge n. 675/1996 (ad esempio, attraverso la lettura di un foglio disponibile presso gli uffici di raccolta delle firme), nonché un'indicazione sulla circostanza che la manifestazione di consenso riprodotta nel frontespizio dei moduli in distribuzione era da intendersi priva di ogni effetto.

## 4.21. Accertamenti e ispezioni.

Analogamente a quanto previsto per altre autorità di garanzia, il Garante può, nello svolgimento dei propri compiti, chiedere a chiunque di esibire documenti e di fornire informazioni, ad esempio con una richiesta scritta al titolare o al responsabile del trattamento o a terzi (art. 32, comma 1, legge n. 675).

La richiesta determina una soggezione del destinatario. In caso di inottemperanza, il Garante può applicare una sanzione pecuniaria e può procedere a controlli d'ufficio per appurare le circostanze oggetto della mancata verifica. Al Garante non può essere opposto il segreto professionale o d'ufficio, salvo il segreto professionale del giornalista per ciò che attiene alla fonte della notizia.

Nei casi di necessità, ai fini del controllo delle disposizioni in materia di trattamento dei dati, il Garante può disporre accessi alle banche dati o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento, o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo, avvalendosi, se necessario, della collaborazione di altri organi dello Stato.

L'eventuale accesso da parte del Garante, ovvero le ispezioni e le verifiche *in loco*, sono state delimitate e circoscritte dalle norme contenute nel richiamato articolo 32. In primo luogo, è necessaria un'autorizzazione preventiva concessa dal Presidente del tribunale competente per territorio in relazione al luogo dell'accertamento.

Le modalità di accesso e di verifica sono state precisate nel regolamento di disciplina dell'organizzazione dell'Ufficio del Garante, in corso di pubblicazione. In particolare, nel provvedimento sono stati disciplinati alcuni aspetti fra i quali assume rilievo la garanzia dell'inviolabilità del domicilio, che la legge ha individuato nell'autorizzazione del Presidente del tribunale, e che viene concettualmente meno quando l'accesso

o la verifica avvenga su richiesta o con il pieno consenso del soggetto presso il cui domicilio avviene l'accesso o la verifica. Si è ritenuto che il beneficiario del bene "domicilio", costituzionalmente garantito e tutelato, possa liberamente disporne attraverso un assenso che deve essere scritto ed informato, rendendo così superflua l'acquisizione dell'autorizzazione giudiziaria, tenuto anche conto dei tempi a volte lunghi che essa può richiedere.

Le altre norme contenute nel provvedimento regolamentare, concernenti le modalità di svolgimento degli accertamenti, si caratterizzano per la garanzia della correttezza e, al tempo stesso, dell'efficacia, tenendo conto anche, per ciò che riguarda i limiti temporali, della disciplina delle perquisizioni domiciliari prevista dall'articolo 251 del codice di procedura penale.

L'articolo 32, comma 4, della legge chiarisce che i destinatari degli accertamenti non possono opporre un rifiuto e sono tenuti a prestare quel minimo di attività richiesta affinché l'accesso, l'ispezione o la verifica abbiano luogo.

L'attività del Garante, in questa prima fase di applicazione della disciplina sulla protezione dei dati personali, ha curato gli adempimenti necessari per verificare le eventuali inosservanze di legge, ma ha dedicato, contemporaneamente, particolare attenzione all'informazione e alla divulgazione delle novità introdotte dalla nuova disciplina legislativa, curando, in particolare, il rapporto con i singoli cittadini e fornendo loro chiarimenti e pareri, anche telefonici, in ordine alle problematiche emerse nel corso di questo primo periodo di applicazione della legge.

Non può, tuttavia, non essere evidenziato che questa Autorità ha ritenuto prioritario l'impegno nell'attività di completamento di alcuni importanti adempimenti necessari per l'attuazione della legge e in particolare della procedura per la notificazione e del rilascio delle autorizzazioni per il trattamento dei dati sensibili.

## 4.22. Schengen: Archivi N. S.I.S. e S.I.RE.N.E.

A seguito della decisione dell'Autorità di controllo comune Schengen del 12 dicembre 1997 di effettuare una verifica sulle misure di sicurezza adottate dagli uffici SIRENE, il Garante ha ricevuto dal Dipartimento di pubblica sicurezza un rapporto scritto sulle misure di sicurezza adottate dal N-SIS e dall'Ufficio SIRENE, e si è recato in visita presso gli uffici il 2 marzo 1998.

L'N-SIS ha segnalato di non aver incontrato particolari difficoltà nel conformarsi ai protocolli e alle procedure stabiliti dalle Parti contraenti ai sensi dell'articolo 92, par. 2, della Convenzione.

In ordine alle misure di sicurezza adottate, il Garante ha attentamente valutato gli aspetti della sicurezza fisica e logica delle strutture N-SIS e SIRENE, anche attraverso un rapporto scritto.

Delle risultanze dell'accesso il Garante ha riferito alla competente commissione parlamentare di controllo nel corso dell'audizione tenutasi il 12 marzo 1998, cui ha preso parte il Presidente del Garante.

Sulla base della verifica effettuata, il Garante ha suggerito all'Autorità di controllo comune di inserire nelle future linee-guida la possibilità di:

— effettuare il tracciamento di tutte le varie operazioni relative alla base dati N-SIS (numero di interrogazioni, frequenza, orario, tipi di dati consultati, ecc.);

— rafforzare le misure di sicurezza volte a garantire che l'accesso sia limitato effettivamente ai dati per i quali i singoli operatori sono abilitati, anche attraverso la modifica periodica delle *password*;

— utilizzare adeguatamente le statistiche dei tracciamenti al fine di individuare eventuali anomalie, specie in riferimento al numero delle interrogazioni;

— invitare gli N-SIS e gli Uffici SIRENE a presentare alle autorità di controllo nazionali un rapporto sulla sicurezza con cadenza periodica, ad esempio annuale.

Peraltro, già il Presidente del Garante era stato sentito dal Comitato parlamentare nel corso dell'audizione svoltasi il 5 giugno 1997. Tale audizione ha riguardato, in particolare, il tema del coordinamento legislativo tra le disposizioni esistenti in materia di protezione dei dati personali nella legge n. 675/1996 e le specifiche norme introdotte dalle leggi n. 121/1981 (recante nuovo ordinamento della Polizia di Stato) e n. 388/1993 (di ratifica della Convenzione di Shengen), nonché del raccordo con le pertinenti disposizioni delle Convenzioni EUROPOL e SID.

## 4.23. Trattamenti effettuati dal C.E.D del Dipartimento della pubblica sicurezza.

La particolare "sensibilità" dei dati raccolti dalle forze di polizia nello svolgimento dei compiti di tutela della sicurezza pubblica, prevenzione e repressione dei reati, ha indotto a suo tempo il legislatore ad intervenire per disciplinare la materia, con alcune norme che ne regolassero anzitutto le modalità e i limiti di raccolta e di elaborazione da parte del Centro elaborazione dati del Dipartimento della pubblica sicurezza del Ministero dell'interno ove i dati confluivano (legge 1 aprile 1981, n. 121).

Alle prime garanzie introdotte nel 1981, risultate poi superate anche alla luce del contesto internazionale, si aggiungono oggi le elevate misure di protezione previste dalla legge n. 675/1996, anche per ciò che riguarda i poteri di controllo attribuiti al Garante d'ufficio o su segnalazione dell'interessato.

Il sistema degli strumenti di controllo sui "dati di polizia" si presenta quindi articolato. A fianco dei poteri attribuiti al Garante (artt. 31 e 32 della legge n. 675) ed all'autorità giudiziaria, permane anche la facoltà, per il soggetto interessato, di esercitare le consentite verifiche sulla liceità e correttezza dei dati che lo riguardano attraverso una richiesta rivolta direttamente all'ufficio del Dipartimento della pubblica sicurezza responsabile degli archivi, secondo la procedura specificata nell'articolo 10 della legge 121/1981 citata.

Al riguardo, sulla base di diverse segnalazioni pervenute, il Garante è intervenuto presso il predetto ufficio per sottolineare la necessità dell'applicazione del citato articolo 10 nella sua corretta interpretazione, secondo la quale l'"accesso" dell'interessato non è subordinato a particolari situazioni legittimanti, quali la previa pendenza di un procedimento amministrativo o giurisdizionale.

Nella stessa occasione il Garante ha sottolineato la necessità che sia rispettato dall'ufficio competente il termine di venti giorni previsto dall'articolo 10 per il riscontro delle richieste, ovvero per la comunicazione al Garante della sussistenza di motivi ostativi al riscontro stesso.

## 4.24. Accertamenti presso servizi di informazione e di sicurezza.

Il Garante, sulla base delle richieste pervenute, ha proceduto ad alcuni accertamenti relativi a trattamenti di dati personali effettuati presso il SISDE, il SISMI e il CESIS.

Le verifiche si sono svolte il 25 ed il 26 febbraio 1998 presso le varie strutture interessate, e hanno riguardato otto cittadini richiedenti.

Il controllo si è svolto con la piena collaborazione degli organismi ed è stato preceduto da una nota con la quale il Garante si è pronunciato su alcuni quesiti relativi all'attività di *intelligence*.

Il Garante ha informato i cittadini interessati dell'esito della verifica con modalità rispettose dei criteri stabiliti dall'art. 32 della legge e che tengono conto sia dell'esigenza di rassicurare il cittadino circa l'assenza di violazione di legge sia della necessità di salvaguardare, al tempo stesso, la segretezza dei trattamenti oggetto di verifica.

Il Garante si è peraltro riservato di formulare al Governo alcune ulteriori osservazioni di ordine generale, tenendo conto anche delle disposizioni amministrative di settore che gli organismi di sicurezza hanno reso disponibili nell'ambito della collaborazione prestata.

# 5. ATTIVITÀ COMUNITARIA E INTERNAZIONALE

## 5.1. Premessa.

A causa del processo di globalizzazione delle economie e delle culture in atto, ai trasferimenti di persone, beni e servizi da un Paese all'altro si affianca un altrettanto imponente flusso di informazioni contenenti dati personali. Per tale ragione, la dimensione internazionale è connaturata al tema della protezione dei dati e la regolamentazione dei trattamenti effettuati deve svilupparsi tenendo conto e cercando di dominare questi fenomeni.

La transnazionalità della materia risulta ancora più evidente se si considera l'enorme mole di transazioni, commerciali e non, fra operatori di diversa provenienza geografica, le quali presuppongono la conoscenza dei dati relativi ai soggetti interessati.

Una sfida di questa portata non può essere lasciata all'iniziativa di un solo Paese e richiede una stretta cooperazione internazionale, in particolare fra gli organismi impegnati nella protezione dei dati personali. È in quest'ottica di progressivo superamento dei confini nazionali che si collocano i principali strumenti elaborati in sede internazionale per fornire una risposta adeguata alle nuove sfide.

Nel corso degli anni Settanta ed Ottanta è emersa nei più importanti organismi internazionali la consapevolezza dell'importanza di intervenire nella materia, approntando un adeguato quadro normativo che vincolasse gli Stati ad uno *standard* comune di garanzie. Si è passati quindi dalle linee guida elaborate dall'OCSE all'adozione della Convenzione n. 108 del 1981 del Consiglio d'Europa e, quindi, alle direttive europee in materia di protezione dei dati personali (nn. 95/46 e 97/66).

Nella piena consapevolezza di tutto ciò, il Garante, fin dalla sua costituzione, ha voluto dedicare particolare impegno ai rapporti con gli organismi internazionali e con le altre autorità di garanzia, contribuendo anche all'elaborazione di diversi provvedimenti normativi internazionali.

## 5.2. La direttiva-quadro n. 95/46/CE.

La direttiva n. 95/46/CE ha rappresentato un'importante innovazione, sia sotto il profilo contenutistico, sia per il suo stesso porsi come fonte sovraordinata ai legislatori degli Stati membri e, per questo, in grado di delineare una disciplina comune in materia. Essa si fonda sulla considerazione che l'integrazione europea comporta necessariamente un aumento dei flussi di dati personali tra tutti i soggetti degli Stati membri, siano essi privati o pubblici: risulta dunque necessario superare i divari esistenti fra i diversi Paesi nella tutela accordata alle persone rispetto al trattamento dei dati, per evitare il costituirsi di gravi ostacoli alla libera circolazione.

Caratteristica principale della direttiva è quella di garantire una tutela della persona e della vita privata in quanto tali, anche indipendentemente dai rapporti contrattuali all'interno dei quali si trovi ad operare. Il legislatore comunitario ha voluto superare un'impostazione — propria, ad esempio, della normativa dettata a tutela del consumatore — in cui l'individuo è garantito solo relativamente ad una condizione soggettiva temporanea, ed ha inteso assolutizzare, in un certo qual modo, la protezione relativa al trattamento dei dati personali, pur nel rispetto delle esigenze della libera circolazione all'interno dello spazio comunitario.

Questa filosofia particolarmente avanzata è stata in parte all'origine del lungo *iter* di elaborazione della direttiva ed ha costituito un fattore di spinta decisivo per elevare la soglia di protezione accordata dalla legislazione dei diversi Paesi membri.

Il ritardo con cui è stata approvata la legge n. 675/1996 ha consentito all'Italia di recepire gran parte delle norme della direttiva e, per vari profili, anche di arricchire quanto in essa disposto, ponendosi come una delle legislazioni più avanzate nel panorama europeo in materia di protezione dei dati personali.

Inoltre, anche grazie allo strumento flessibile costituito dalle deleghe legislative contenute nella legge n. 676/1996, l'Italia continuerà a garantire agli altri Stati membri una protezione dei dati personali tale da rendere sicuri gli scambi con il nostro Paese, ed insieme potrà esercitare un ruolo di guida rispetto alle altre legislazioni nazionali, nonché alla futura produzione normativa comunitaria.

Il Garante ha operato in questa direzione attraverso un costante lavoro di promozione della conoscenza della nostra normativa negli altri Paesi della Comunità, favorendo lo scambio e il confronto con gli organi dei Paesi membri a vario titolo impegnati nella tutela dei dati personali.

L'Autorità, ai fini del controllo e dell'armonizzazione della normativa comunitaria in materia di tutela dei dati, partecipa ai lavori del Gruppo previsto dall'art. 29 della direttiva ed a quelli del Comitato disciplinato dall'art. 31. Quest'ultimo ha il compito di assistere la Commissione esprimendo pareri sui progetti di misure da adottare sottopostigli dalla Commissione stessa.

"Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" istituito dall'articolo 29 della direttiva, invece, ha carattere consultivo e indipendente, è composto dai rappresentanti di ciascuna delle autorità di controllo nazionale dei 15 Paesi che fanno parte dell'Unione europea e da un rappresentante della Commissione europea.

Il Gruppo è incaricato di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della direttiva, di formulare pareri sia sul livello di tutela nella Comunità e nei Paesi terzi sia sui codici di condotta elaborati a livello comunitario, nonché di consigliare la Commissione in merito ai progetti di modifica della direttiva, alle misure addizionali sul trattamento dei dati e a qualsiasi altro progetto di misure comunitarie che incidano sui diritti e sulle libertà delle persone fisiche con riguardo al trattamento dei dati personali.

Nel corso dei lavori fin qui svolti il Gruppo si è occupato, fra l'altro, dell'elaborazione degli archivi di analisi di Europol, del progetto di convenzione Eurodac e di quello sulla protezione degli interessi finanziari della Comunità.

Il Gruppo può inoltre formulare, di propria iniziativa, raccomandazioni su qualsiasi questione attinente alla materia. Fra quelle adottate si segnalano, per la particolare rilevanza, una raccomandazione recante norme in materia di protezione dei dati e di mezzi di comunicazione e due raccomandazioni concernenti la tutela della riservatezza e dell'anonimato degli utenti di Internet.

Il Garante partecipa a tale Gruppo di lavoro nella persona del prof. Stefano Rodotà (il quale è stato recentemente eletto quale vice presidente del Gruppo stesso), del prof. Ugo De Siervo e del dott. Giovanni Buttarelli.

## 5.3. La direttiva n. 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni.

La Direttiva 97/66/CE del 15 dicembre 1997" sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni", è stata elaborata a seguito di due risoluzioni con le quali il Parlamento europeo, nel 1986-1988, chiese alla Commissione europea di presentare proposte specifiche nella materia delle telecomunicazioni, tenendo conto della prospettiva dell'apertura dei mercati, al fine di assicurare un livello di riservatezza dei dati personali adeguato alla modernità dei servizi.

La Commissione formulò la sua proposta nel 1990. Successivamente, però, la contestualità dei lavori sulla direttiva n. 95/46/CE ha finito per allungarne i tempi di approfondimento e di discussione.

Nel giugno 1994, dopo il vertice di Edimburgo, la Commissione ha presentato una versione modificata della proposta, semplificandola alla luce del principio di sussidiarietà.

Nel 1995, sotto la presidenza spagnola, il Gruppo ha ipotizzato alcune modifiche alla luce della liberalizzazione dei servizi di telecomunicazione, ed è solo dal 1996 che il Data Protection Working Group ha esaminato la proposta nei dettagli.

La direttiva è apparsa necessaria perché le reti digitali di telecomunicazione permettono la trasmissione della voce, dei dati, delle immagini, dei testi e dei suoni in forma di servizi del tutto nuovi. La digitalizzazione delle reti favorisce lo sviluppo di attività e di funzioni "intelligenti" che incidono in termini nuovi sulla sfera della vita privata e impongono, così, norme più specifiche di quelle contenute nella 95/46/CE, al fine di assicurare un uso corretto dei dati e dei servizi e di garantire, che le reti digitali siano accettate socialmente (basti pensare, ad esempio, al *video-on-demand* e alla *interactive television*).

Ben si può, quindi, definire la direttiva come una direttiva-figlia, visto che essa precisa e integra la direttiva n. 95/46/CE.

Uno dei punti più dibattuti è stato quello riguardante i servizi coinvolti (analogici e/o digitali). La soluzione di compromesso che è stata adottata consente, oggi, di applicare la direttiva a qualunque servizio (via ISDN; reti digitali mobili; reti analogiche ecc.) e questa applicazione non sarà condizionata da valutazioni di economicità. Gli Stati membri potranno unicamente, informando la Commissione, non applicare alle reti analogiche gli articoli riguardanti la presentazione dell'identificazione della linea chiamante e il trasferimento automatico di chiamata,

quando questa applicazione, considerato il minor livello tecnologico delle reti analogiche, non sia tecnicamente possibile o comporti un impegno economico sproporzionato.

Si può affermare che con la direttiva in esame l'impianto comunitario in materia sia stato in grande parte realizzato.

Venendo all'ambito di applicazione, si deve affermare che la direttiva reca una clausola che esclude le attività che ricadono fuori dal diritto comunitario; parimenti, essa non sarà applicabile al *radio-and television broadcasting*, sempreché queste attività siano effettuate nel senso tradizionale del termine.

I nuovi servizi *point-to-point* quali l'*interactive television* e il *video-on-demand* sono disciplinati dalla direttiva. Inoltre essa si occupa di sicurezza e riservatezza delle telecomunicazioni, dati sul traffico e sulla fatturazione, identificazione del numero chiamante, trasferimento automatico della chiamata e chiamate indesiderate, elenchi degli abbonati.

L'aspetto principale della direttiva è relativo al trattamento dei dati inerente il traffico e la fatturazione.

Il delicato argomento concernente la fatturazione dettagliata è stato risolto riconoscendo agli abbonati il diritto di non ricevere questo genere di servizio mentre, per coloro che la ricevono, gli Stati membri devono garantire che gli abbonati e utenti dispongano di sufficienti modalità alternative per le comunicazioni o per i pagamenti (art. 7, par. 1 e 2).

I dati sul traffico dovranno essere cancellati o resi anonimi al termine della chiamata, ferma restando la possibilità di trattare ulteriormente alcuni dati a fini di fatturazione per l'abbonato e dei pagamenti di interconnessione. Sarà anche possibile trattare i medesimi dati per fini di commercializzazione dei servizi del fornitore qualora vi sia il consenso dell'abbonato. Per quest'ultima finalità, quindi, una mera soluzione di *opt-out* quindi, non è stata ritenuta sufficiente.

Quanto alla forma del consenso, varranno le disposizioni attuative della direttiva quadro-generale che richiedono una manifestazione di volontà libera, specifica ed informata.

Sull'argomento occorre però aggiungere che, in deroga a quanto disposto per la commercializzazione dei servizi di telecomunicazione, il consenso non è richiesto per il trattamento già in corso alla data di entrata in vigore delle disposizioni nazionali di attuazione.

Uno degli aspetti più rilevanti concerne il meccanismo da tempo introdotto in altri Stati europei, di identificazione della linea chiamante, reso possibile dalla tecnologia digitale. In base a tale sistema, si è contemperata la scelta di restare anonimi per mezzo della soppressione del loro numero identificativo con il concorrente diritto a non essere disturbati da singole chiamate.

Altre disposizioni significative attengono, infine, all'inclusione dei nominativi degli abbonati negli elenchi, alle chiamate pubblicitarie indesiderate, alle chiamate moleste e alla tutela della vita privata degli utenti chiamanti e degli abbonati chiamati, in caso di fatturazioni dettagliate. La direttiva doveva essere recepita entro il 24 ottobre 1998, e cioè entro lo stesso termine previsto dalla direttiva quadro-generale (art. 16, par. 1). Gli Stati membri possono peraltro conformarsi all'articolo 5 sulla "riservatezza delle comunicazioni" al più tardi e non oltre il 24 ottobre 2000.

L'Italia ha attuato la direttiva con il citato decreto legislativo del 9 aprile 1998 intervenuto durante la stampa della presente relazione.

## 5.4. La cooperazione europea nei settori giustizia e affari interni.

Nell'ambito della collaborazione fra Paesi europei in materia di giustizia e affari interni (c.d. terzo pilastro del Trattato di Maastricht) sono state elaborate o sono in corso di elaborazione diverse convenzioni.

Si fa riferimento, in particolare, a quelle relative all'istituzione e al funzionamento di un Ufficio europeo di polizia (EUROPOL), al Sistema di informazione doganale (SID), alla rilevazione delle impronte digitali dei richiedenti asilo (EURODAC) nonché alle forme di cooperazione previste dalla convenzione di applicazione dell'Accordo di Schengen.

Ogni Convenzione o progetto di Convenzione — di cui si parlerà più diffusamente avanti — prevede l'istituzione di un sistema automatizzato di elaborazione dei dati, nonché flussi di dati scambiati con altri mezzi automatizzati e cartacei.

Per ciascuno di questi trattamenti di dati svolti per finalità di giustizia o di ordine e sicurezza pubblica vengono definite le misure necessarie per garantire la protezione dei dati, secondo norme spesso collegate alla Convenzione n. 108 citata e alla Raccomandazione N.R. (87)15 del Consiglio d'Europa.

Su proposta italiana, valutata con favore dal Garante, il Consiglio dei ministri europeo giustizia-affari interni discuterà nel mese di maggio un documento volto ad aprire una riflessione sull'incremento degli accordi e delle autorità comuni di controllo previste in materia di dati, anche al fine di ridurre le eventuali incongruenze o duplicazioni e di favorire una maggiore omogeneità della tutela.

Le Convenzioni prevedono inoltre l'attribuzione di competenze in materia di protezione dei dati ad autorità nazionali di controllo; allo stesso tempo individuano un'autorità comune cui sono affidati compiti di controllo su determinati archivi.

### 5.4.1. Schengen.

In tale contesto assume particolare rilevanza l'Accordo di Schengen, firmato il 14 giugno 1985, nonché la successiva Convenzione di applicazione firmata nel 1990 e resa esecutiva in Italia con la legge n. 388/1993.

Le finalità dell'Accordo, reso operativo in Italia il 26 ottobre 1997, sono quelle di creare uno spazio comune per la libera circolazione delle persone e delle merci, sopprimendo progressivamente i controlli alle frontiere. La Convenzione del 1990 disciplina più specificamente le necessarie forme di cooperazione di polizia, doganale e giudiziaria, e istituisce il Sistema d'informazione Schengen (SIS), attraverso il quale la predetta cooperazione trova un momento applicativo di estrema importanza.

Per un corretto funzionamento del SIS, la Convenzione presuppone che sia garantito un livello di protezione di dati corrispondente almeno a quello previsto dalla Convenzione n. 108 del Consiglio d'Europa e dalla Raccomandazione N/R(87)15. A tal fine è stata istituita un'Autorità di controllo comune (ACC) incaricata di vigilare sulla corretta applicazione delle disposizioni della Convenzione e, più in particolare, sul rispetto delle disposizioni a tutela del trattamento di dati personali.

La Convenzione prevede che, oltre al Sistema d'informazione comune, vengano istituiti archivi nazionali (N-SIS) per la cui vigilanza sono competenti le autorità nazionali di controllo in materia di prote-

zione dei dati. Agli archivi N-SIS si affiancano gli uffici SIRENE, i quali gestiscono informazioni supplementari relative alle segnalazioni da inserire negli archivi N-SIS e nel SIS.

La legge n. 388/1993 citata e la legge n. 675/1996 individuano il Garante quale autorità nazionale di controllo per l'Italia. Ad esso è demandato il compito "di esercitare un controllo indipendente dell'archivio della sezione nazionale del Sistema d'Informazione Schengen e di verificare che l'elaborazione e l'utilizzazione dei dati inseriti non leda i diritti della persona interessata" (art. 114 della Convenzione). In tale veste, la medesima Autorità è chiamata a far parte dell'Autorità comune di controllo (ACC).

Fra le attività di maggior rilievo dell'ACC, alle cui riunioni il Garante ha partecipato attivamente sin dalla sua costituzione e con continuità, rientra sicuramente quella di "elaborare proposte armonizzate allo scopo di trovare soluzioni comuni ai problemi esistenti" (art. 115, comma 4). In tale cornice, vi rientrano i pareri formulati dall'ACC nel corso del 1997, che si riportano per intero in allegato.

Sino al luglio del 1997, l'Italia ha partecipato ai lavori dell'ACC in veste di osservatore, mentre successivamente ha assunto lo *status* di membro a pieno titolo.

Conformemente agli auspici espressi a Bruxelles, il Garante ha convenuto di allegare alla propria relazione annuale il Primo Rapporto (marzo 1995-marzo 1997).

Si differisce invece la pubblicazione dello schema di relazione annuale relativa al periodo marzo 1997-marzo 1998 (nella quale si prende atto dell'entrata in vigore della legge italiana avvenuta rispetto a Schengen, nel gennaio del 1997), non avendo ancora l'ACC formalizzato la sua approvazione.

L'ACC ha deliberato il 12 dicembre 1997 di curare la pubblicazione di un opuscolo esplicativo del diritto di accesso ai dati da parte delle persone segnalate nel SIS. Il testo, al quale verranno allegati gli estremi delle autorità nazionali, verrà distribuito presso i valichi delle frontiere esterne Schengen, per il tramite delle medesime autorità e, quindi, del Garante.

Giova peraltro aggiungere che nel programma di azione approvato per il primo semestre 1998 è stata ribadita l'intenzione di rafforzare il ruolo dell'ACC nella struttura Schengen, in difesa dei princìpi della protezione dei dati. Particolare attenzione verrà dedicata all'attuazione da parte degli organi esecutivi Schengen delle raccomandazioni formulate dall'ACC, in modo specifico per quanto riguarda la sicurezza del C.SIS (vedi allegato).

**5.4.2. Europol.**

L'istituzione dell'Ufficio europeo di polizia (Europol) — il cui funzionamento è regolato dalla convenzione firmata a Bruxelles nel luglio 1996, la cui legge di ratifica è stata approvata di recente dal Parlamento — mira a favorire la collaborazione fra le forze di polizia nel prevenire e combattere il terrorismo, il traffico illecito di stupefacenti e altre gravi forme di criminalità internazionale.

Il fulcro di questa attività di cooperazione è costituito dallo scambio e dall'elaborazione di informazioni fra gli organi incaricati della tutela della sicurezza e dell'ordine pubblico.

La Convenzione contiene diverse disposizioni a tutela dei dati personali e stabilisce che ciascuno Stato membro istituisca un'autorità di controllo nazionale, incaricata di vigilare sulla liceità delle operazioni di consultazione e trasmissione di dati all'Europol effettuate dallo Stato

stesso (art. 23) nonché un'Autorità di controllo comune, composta dai rappresentanti di tutti i Paesi membri (art. 24), avente il compito di verificare la liceità dei trattamenti effettuati dall'Europol.

Il Garante è intervenuto nella sua qualità di autorità indipendente per il controllo sui trattamenti di dati personali, provvedendo alla realizzazione di tutti gli adempimenti di sua competenza diretti a garantire una pronta applicazione della Convenzione: in particolare, ha partecipato all'elaborazione del regolamento interno dell'autorità di controllo comune — la cui adozione costituisce una precondizione per l'inizio delle attività dell'Europol (art. 45) — e ha preso parte, nel corso del 1997 e dei primi mesi del 1998, all'attività dell'apposito Gruppo di lavoro composto dai rappresentanti degli analoghi organismi della Comunità Europea.

**5.4.3. Sistema Informativo Doganale.**

Il 26 luglio 1995 è stata firmata la Convenzione fra gli Stati membri dell'Unione Europea relativa all'utilizzazione di tecnologie per scopi doganali (sistema informativo doganale - SID), la cui ratifica è attualmente all'esame del Parlamento. Il SID intende essere uno strumento per la lotta contro le frodi comunitarie e un ausilio alla prevenzione e alla repressione di reati in materia di circolazione delle merci e di traffico di stupefacenti, consentendo maggiore rapidità nello scambio delle informazioni utili al riguardo.

Particolare rilevanza è stata data al rispetto dei princìpi sanciti dalla Convenzione n. 108 di Strasburgo e alla Raccomandazione N. R(87)15 sui dati di polizia.

Come per la Convenzione Europol, le norme nazionali volte a definire il quadro interno di protezione dei dati saranno previste dai decreti delegati di cui dalla legge n. 676/1996, il che dovrebbe favorire un'elaborazione organica anche attraverso l'inclusione in un unico veicolo normativo volto a semplificare la consultazione delle future regole.

**5.4.4. Eurodac.**

Un recente progetto di Convenzione, basato sull'articolo 15 della Convenzione di Dublino relativa alla determinazione dello Stato competente per l'esame delle richieste d'asilo, è in corso di elaborazione presso l'apposito gruppo di lavoro del Consiglio dell'Unione europea. La Convenzione contempla l'istituzione di un sistema per la raccolta, la memorizzazione, il confronto e lo scambio di dati relativi alle impronte digitali di soggetti che presentino richiesta di asilo in uno degli Stati membri (EURODAC).

Il sistema prevede una banca dati centralizzata contenente tutte le impronte digitali dei richiedenti, con una serie di garanzie relative, ad esempio, alla cancellazione di tali dati una volta trascorso un periodo di 10 anni (o nel momento in cui un soggetto divenga cittadino di uno degli Stati membri), nonché al diritto di accesso da parte degli interessati.

Anche in questo caso si fa riferimento al rispetto dei princìpi sanciti dalla più volte citata Convenzione n. 108, sul quale dovranno vigilare le autorità nazionali competenti per la protezione dei dati personali. Il controllo esercitato da tali autorità si applicherà in modo particolare alla legittimità della memorizzazione e della trasmissione dei dati.

Nell'ambito delle riflessioni avviate dalla citata iniziativa in atto presso il Consiglio GAI (v. par. 5.4.), il Garante si è interrogato circa il rischio che su questo, e sugli altri strumenti sopra ricordati, in corso di

adozione o comunque di applicazione, si creino distinti "corpi normativi" della protezione dei dati, e conseguentemente regole diverse per la tutela sostanziale e procedimentale dei diritti della personalità.

A questo proposito, è stata richiamata l'attenzione — da ultimo nell'audizione svoltasi davanti al Comitato parlamentare di controllo sull'attuazione e il funzionamento di Schengen tenutasi il 12 marzo c.a. — sull'opportunità di assicurare un maggiore coordinamento nelle predette iniziative, come del resto auspicato dal Parlamento europeo nella risoluzione sul funzionamento e sull'avvenire di Schengen n. A4-0014/97 (punto 16).

## 5.5. Consiglio d'Europa.

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. Al suo interno, infatti, dopo l'adozione di una serie di provvedimenti di carattere settoriale, nel 1981 si è giunti 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 la base su cui sono state costruite le successive regolamentazioni in ambito comunitario e nazionale. In seguito all'approvazione della legge n. 675/1996 è stato possibile depositare lo strumento di ratifica il 29 marzo 1997, il che ha permesso di far entrare in vigore la Convenzione per l'Italia lo scorso 1 luglio.

L'attività del Consiglio d'Europa in materia non si è però esaurita con l'approvazione della Convenzione, ed è proseguita in un'intensa attività di elaborazione della normativa di settore nonché nell'aggiornamento di quella preesistente.

Il Garante, sin dalla sua costituzione, ha preso parte alle diverse attività del Consiglio d'Europa, dando un contributo significativo all'elaborazione dei diversi testi attualmente in discussione. In particolare, ha rappresentato l'Italia in seno al Comitato consultivo della convenzione n. 108 (T-PD), al Gruppo di progetto sulla protezione dati (CJ-PD) e al Gruppo di lavoro sulle nuove tecnologie (GT-15).

Il T-PD ha il compito di proporre e discutere eventuali modifiche alla Convenzione n. 108, e di pronunciarsi sui problemi applicativi. Attualmente, al suo interno sono in discussione l'adesione della Comunità europea alla Convenzione n. 108, alcune modifiche della Convenzione concernenti l'estensione dell'applicabilità agli archivi cartacei, alle persone giuridiche nonché la previsione obbligatoria di un'Autorità indipendente di controllo.

Il CJ-PD si occupa dell'elaborazione dei progetti di raccomandazioni in materia di trattamento di dati personali. Durante il 1997, è stato impegnato nella predisposizione di una raccomandazione sui trattamenti di dati personali a fini assicurativi, nell'elaborazione di un codice di condotta per gli utilizzatori di *Internet*, e nella collaborazione con altri comitati costituiti all'interno del Consiglio d'Europa impegnati nell'elaborazione di raccomandazioni che hanno riflessi sul trattamento dei dati personali.