L'Autorità ha pertanto invitato la GratisT Italia s.r.l. a modificare i moduli del contratto prima dell'attivazione del servizio e a comunicare ai sottoscrittori che avevano aderito già al servizio le clausole modificate, anche al fine di ottenere nuovamente il consenso dei sottoscrittori alla cessione dei loro dati ad altre società.

Tuttavia, il Garante ha osservato che, anche per quanto riguarda gli abbonati ed utenti chiamati che ascoltano anch'essi messaggi pubblicitari, il servizio *GratisTel* è soggetto alla disciplina in materia di dati personali e di riservatezza nelle telecomunicazioni.

I dati relativi alle utenze chiamate sono, infatti, oggetto di trattamento da parte della società che li raccoglie. Pertanto, anche queste ultime devono essere informate e messe in grado di esprimere consapevolmente le proprie scelte in ordine all'utilizzazione dei loro dati a fini pubblicitari.

L'Autorità non ha ritenuto ammissibile un meccanismo che trasferisca sui sottoscrittori l'obbligo di informare le persone chiamate, il cui onere spetta alla società fornitrice del servizio, la quale è stata invitata a predisporre un messaggio chiaro per permettere al chiamato di non ricevere inconsapevolmente una chiamata con spot o di ascoltare messaggi pubblicitari senza un'informativa anche sintetica e l'espressione di un consenso. La manifestazione di volontà da parte del chiamato, si è rilevato, potrebbe essere espressa anche esercitando, tramite l'apparecchio telefonico, un'opzione per l'instaurazione della chiamata o per l'inserimento dei messaggi pubblicitari, sempre sulla base di una preventiva e idonea informativa.

È rimasto, comunque, aperto il problema più in generale della libertà di comunicazione, che potrebbe essere limitata da un'alternativa circoscritta all'accettazione della pubblicità o all'interruzione della telefonata. Per questo motivo, il Garante ha trasmesso il provvedimento all'Autorità per le garanzie nelle comunicazioni; ciò anche perché quest'ultima potesse valutare, per i profili di sua competenza, la natura del servizio offerto.

Successivamente, a seguito della trasmissione da parte della società degli elementi richiesti con il provvedimento del 13 novembre 1999 circa le misure e gli accorgimenti assunti per rendere conforme il servizio alle norme sulla privacy, nonché per consentirne l'attivazione nel pieno rispetto dei diritti dei cittadini, il Garante ha inviato una nuova segnalazione a GratisT Italia s.r.l. perché, dall'esame della predetta documentazione, in vista dell'annunciato avvio del servizio per il 18 dicembre 1999, era emerso che le modifiche richieste non erano state tutte apportate (v. l'ulteriore segnalazione del 14 dicembre 1999, pubblicata nel Bollettino n. 10/1999, pag. 61).

In particolare, per quanto riguarda i sottoscrittori del contratto, si è ritenuto necessario che la società provvedesse a:

- chiarire quali fossero i dati che i sottoscrittori devono necessariamente fornire nel modulo di iscrizione affinché venga loro erogato il servizio e quali, invece, le informazioni facoltative, anche per quanto riguarda il codice fiscale (la società aveva sino ad allora comunicato ai sottoscrittori di utilizzarlo per imprecisati "scopi interni");
- far presente ai sottoscrittori, dal momento che veniva prevista anche la possibilità per l'utente di ricevere a casa ulteriori informazioni sui prodotti (attraverso i c.d. "spot interattivi"), che è già previsto nel contratto un elenco aggiornato degli inserzionisti dal quale possono essere ricavate le coordinate per esercitare i diritti sanciti dall'art. 13 della legge n. 675 del 1996 (accesso ai dati, loro aggiornamento, rettifica, cancellazione, ecc.);
- specificare meglio, nel modulo di sottoscrizione, le categorie di società e di imprese destinatarie dei dati degli interessati, elencando le principali tipologie di operatori.

Per quanto riguarda invece le persone chiamate attraverso il servizio *GratisTel*, la società aveva previsto, all'inizio della telefonata, un messaggio in base al quale si poteva rifiutare la chiamata interrotta dalla pubblicità. Al riguardo, il Garante ha, però, richiesto che la persona chiamata

fosse messa in grado di esprimere in modo positivo la sua volontà attraverso la digitazione di un tasto, acconsentendo in piena consapevolezza all'instaurazione della telefonata (facendo sì che se il chiamato non accetta la telefonata attraverso la digitazione del tasto indicato, cada la linea).

L'Autorità ha sottolineato inoltre che tale meccanismo serve solo per consentire lo svolgimento della telefonata, ma non per ogni altra utilizzazione dei dati, ad esempio a seguito di "spot interattivi". L'utilizzazione delle informazioni del chiamato a tale scopo può avvenire solo sulla base di una più articolata informativa e dell'acquisizione di un nuovo consenso.

A seguito della seconda segnalazione del Garante, la GratisT Italia s.r.l. ha inviato all'Autorità, prima dell'avvio del servizio, copia dei documenti riformulati secondo le indicazioni fornite dal Garante, impegnandosi a conformare il trattamento dei dati ai princìpi in tema di tutela della riservatezza.

2.10.5 La tutela dei dati nei servizi di accesso gratuito ad Internet

Nel luglio del 1999, il Garante ha avviato un procedimento di indagine nei riguardi del servizio "Libero" di Infostrada, in seguito ad alcune segnalazioni concernenti il lancio di questo nuovo servizio di accesso gratuito ad Internet, che prevede sia l'acquisizione, al momento della sua attivazione, di diverse informazioni personali relative anche ai propri gusti ed interessi, sia il successivo monitoraggio delle connessioni ai siti visitati dagli abbonati, svolto per individuare le loro preferenze (attraverso la determinazione dei loro profili di consumatori, la cosiddetta "profilazione"), nonché per programmare l'invio di messaggi pubblicitari via *e-mail*.

In occasione di tale procedimento, l'Autorità ha così affrontato il tema della raccolta e dell'utilizzazione di dati personali nell'ambito dei servizi di accesso gratuito ad Internet offerti dagli operatori nel settore delle telecomunicazioni, indicando alcune modalità necessarie a garantire la liceità e la correttezza dei loro comportamenti nei confronti degli utenti (provvedimento del 13 gennaio 2000).

Il Garante ha chiarito che, fermo restando il rispetto della volontà dei cittadini e dei consumatori di accettare la cessione di dati identificativi o attinenti a gusti, preferenze ed interessi, per ottenere gratuitamente determinati servizi, gli interessati devono, però, essere messi in grado di esprimere le proprie scelte sull'uso dei dati che li riguardano in maniera consapevole e libera. Per questo è necessario che, anzitutto, ricevano tutte le informazioni necessarie per comprendere appieno le finalità e le modalità del trattamento dei dati, compresi quelli che vengano acquisiti successivamente (tali informazioni ai clienti vanno date sempre, anche quando non venga chiesto loro alcun consenso), verificando con attenzione se alcuni dati, richiesti come "obbligatori" dalle società del settore, siano realmente indispensabili per attivare il servizio.

In particolare, le segnalazioni pervenute all'Autorità hanno prospettato un contrasto con la disciplina sulla privacy, con particolare riguardo all'insufficienza delle informazioni fornite agli interessati, alla possibilità di raccogliere i dati sui siti frequentati (con eventuale conoscenza di informazioni relative, ad es., a salute, vita sessuale, opinioni politiche o sindacali, convinzioni religiose o filosofiche) e di controllare se i messaggi pubblicitari inviati dalla società vengano effettivamente letti dagli abbonati.

Durante la fase istruttoria, la società ha eliminato alcune anomalie ed incongruenze presenti nei documenti sottoposti al potenziale cliente al momento dell'iscrizione e ha specificato che l'analisi degli accessi ai siti verrà svolta su un catalogo predefinito dalla stessa società (che non comprenderebbe siti nei quali sono trattati argomenti da cui sono ricavabili dati "sensibili"). Non verrebbe, invece, effettuata alcuna verifica circa il ricevimento e la visualizzazione dei messaggi pubblicitari da parte dei clienti.

Il Garante, tuttavia, ha ritenuto necessario che alcuni profili relativi alle informazioni e ai

documenti, sottoposti al cliente al momento della richiesta del servizio, venissero rivisti e ha fornito, al riguardo, alcune indicazioni da ritenersi valide anche per tutti gli altri operatori che offrono servizi analoghi, in via di rapida espansione.

In particolare, l'Autorità ha sottolineato che l'informativa ai clienti deve essere:

- collocata prima della richiesta di registrazione dei propri dati;
- riferita a tutti gli aspetti del complessivo trattamento svolto dal fornitore nell'ambito del servizio (anziché ai soli profili relativi a finalità commerciali o di marketing), riepilogando in maniera chiara e sintetica le notizie magari disseminate nel contratto;
- integrata con un richiamo, anche sintetico, ai diritti di accesso attribuiti agli interessati dalla legge 675 (art. 13) e con l'indicazione dell'ufficio o servizio presso cui esercitare tali diritti.

Occorre poi precisare meglio tutte le categorie di ulteriori aziende alle quali verranno eventualmente comunicate le informazioni. Tali aziende, a loro volta, dovranno acquisire il consenso degli interessati (oppure la società dovrebbe richiedere il consenso dei clienti anche per conto delle altre aziende, fornendone precisa indicazione, anche in un elenco a parte da rendere agevolmente disponibile agli interessati).

Inoltre, la richiesta del consenso nei confronti degli abbonati che abbiano accettato le condizioni contrattuali e, in particolare, *"autorizzato"* l'invio di messaggi pubblicitari sulla propria casella di posta elettronica, pur potendo essere limitata alle sole operazioni di utilizzazione dei dati per finalità commerciali non collegate al servizio e di loro divulgazione all'esterno, deve essere riferita anche alle disposizioni in tema di pubblicità e di chiamate indesiderate, introdotte dalle recenti normative sulla privacy nelle telecomunicazioni e sui contratti a distanza.

Riguardo all'acquisizione dei dati con i moduli di adesione al servizio, come già detto, vi è poi la necessità di chiarire agli interessati che le informazioni sono raccolte non per specifici obblighi normativi (che non possono essere ravvisati nella mera opportunità di rendere disponibili alcune informazioni sugli abbonati nel caso in cui organi o autorità preposte ad indagini siano interessate in futuro a raccoglierle), ma perché il fornitore intende raccoglierle sulla base di una propria, autonoma, scelta di caratterizzazione del servizio, anche quando l'abbonato non presti il consenso a trattamenti e comunicazioni per finalità commerciali. La valutazione circa le informazioni non essenziali o eccedenti rispetto alle finalità del servizio (il quale si incentra sull'utilizzo dei codici personali d'accesso ad *Internet* e delle caselle di posta elettronica degli interessati) deve essere quindi accompagnata da una migliore specificazione agli interessati delle ragioni della loro raccolta.

In relazione ad altri aspetti, connessi ai dati relativi ai siti consultati dagli abbonati, nel confermare la necessità che la società assuma tutte le misure idonee ad evitare una raccolta di informazioni sensibili, il Garante si è, nel caso concreto, riservato di verificare il catalogo dei siti predisposto dalla società, non appena disponibile, e le attività ad esso collegate, una volta rese operative.

Nel fornire le predette indicazioni, il Garante ha, peraltro, segnalato a Infostrada S.p.a. la necessità di fornire a ciascun utente già abbonato al servizio il nuovo testo di informativa messo a punto per i futuri clienti, assicurando ai vecchi abbonati la possibilità di esprimere nuovamente il consenso e, tramite un meccanismo agevole, revocare le precedenti manifestazioni di volontà.

L'Autorità ha, infine, disposto che copia del provvedimento fosse trasmesso anche ad altri operatori che offrono servizi analoghi, allo scopo di sensibilizzarli ad un maggiore rispetto della normativa sulla protezione dei dati personali.

2.11 Commercio elettronico

2.11.1 Profili generali

Il tema del commercio elettronico è tra i più attuali nel dibattito che concerne, in verità, non solo la tutela della riservatezza dell'individuo di fronte ai trattamenti in rete, ma anche aspetti che potremmo definire prodromici alla stessa promovibilità del commercio on-line quale alternativa ai tradizionali canali di scambio.

Il crescente sviluppo delle attività commerciali in rete potrà realmente incrementarsi solo se, contestualmente, le imprese osserveranno una efficace prassi di tutela dei diritti fondamentali della personalità di utenti e consumatori, adottando politiche e procedure trasparenti nei riguardi dei tipi di dati raccolti, delle modalità della loro concreta elaborazione ed utilizzazione, nonché dell'eventuale comunicazione, così da alimentare la fiducia degli interessati anche in termini di sicurezza dei dati e delle transazioni.

Un'idonea politica di tutela della riservatezza e della sicurezza non è, quindi, un freno *all'e-commerce*, ma, al contrario, un fattore essenziale per la sua crescita, non potendosi del resto concepire il contesto delle reti telematiche come un'area nella quale i diritti della personalità perdono efficacia o divengono puramente "virtuali".

Di fronte alla chiara evidenza che nessun effettivo incremento dell'uso per fini commerciali delle reti, ed in particolare di Internet, si potrà avere, se non sarà offerto un contesto che si presenti al sicuro anche dai pericoli che possono derivare da fronti diversi (come la raccolta occulta o non informata di dati personali, l'uso non garantito di sistemi di pagamento elettronici o, ancora, le possibili vie di elusione della legislazione di tutela della proprietà intellettuale), lo sforzo iniziale dei lavori in atto sul piano internazionale e comunitario e in particolare presso l'Unione Europea, ai quali questa Autorità partecipa attivamente, è stato nel senso di proporre, anche tramite lo strumento della direttiva comunitaria, una sistemazione completa ed organica di tutte le problematiche connesse, e creare un quadro giuridico coerente per lo sviluppo del commercio elettronico sul piano mondiale e nell'ambito del mercato unico europeo.

L'attività complessivamente svolta nel corso del 1999 presso l'OCSE, il Consiglio d'Europa e il Gruppo di lavoro di cui all'art. 29 della direttiva n. 95/46/CE, è sfociata anche in una "posizione comune" comunitaria, destinata a concretarsi a breve in una direttiva del Parlamento europeo e del Consiglio che è sintetizzata nel successivo paragrafo della presente relazione.

Le tematiche di maggior rilievo sul tema privacy-commercio *on line* sono state portate, poi, sempre a livello internazionale, in seno ai lavori dell'OCSE e al forum dell'OCSE che si è svolto a Parigi il 12 e 13 ottobre 1999, dopo la Conferenza di Ottawa dello scorso anno.

Una parallela attività di sensibilizzazione e di intervento è stata inoltre svolta dal Garante anche in seno all'Osservatorio sul commercio elettronico costituito presso il Ministero del Commercio, dell'industria e dell'artigianato, ove è stato dato ampio spazio alla discussione sui temi che più strettamente riguardano l'armonizzazione della disciplina sul commercio con le disposizioni a tutela della privacy.

Sotto il profilo del tema dei servizi *on line* offerti ai cittadini, e quindi del commercio elettronico inteso quale strumento di attuazione e miglioramento dell'efficacia e produttività dei servizi della pubblica amministrazione, vanno ricordati infine i contributi dell'Autorità in numerosi convegni e seminari e, in particolare, al Forum della p.a. 1999, che si è svolto a Roma dal 4 all'8 maggio 1999, anche sulla tematica "Call center, riconoscimento vocale e servizi ai cittadini", nonché al COMPA tenutosi a Bologna il 15, 16 e 17 settembre 1999.

2.11.2
La posizione comune europea e la direttiva sulle firme elettroniche

Parimenti curata è stata poi la partecipazione di questa Autorità ai lavori che hanno portato all'adozione della direttiva n. 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche, diretta a creare uno standard europeo comune e affidabile quanto alle caratteristiche tecniche e agli effetti giuridici della firma digitale.

La direttiva relativa ad un quadro comune sulle firme elettroniche, è stata adottata il 13 dicembre 1999 ed è stata pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* del 19 gennaio 2000.

Gli Stati membri dovranno attuare i principi della direttiva entro il 19 luglio 2001. La direttiva, come già evidenziato nella precedente relazione, è finalizzata ad introdurre una cornice di regole armonizzate tra gli Stati membri per l'utilizzo delle firme elettroniche.

L'intervento è stato ritenuto necessario per favorire lo sviluppo del commercio elettronico e si riferisce principalmente, anche se non esclusivamente, alle transazioni tra privati. La direttiva prende infatti in considerazione anche l'uso delle firme elettroniche nei rapporti con la pubblica amministrazione o, meglio, nel settore pubblico. Essa, inoltre, detta regole per garantire il riconoscimento giuridico delle firme elettroniche, stabilendone l'equiparazione a quelle autografe. Il principio cardine delle direttiva consiste nell'evitare forme di discriminazione delle firme elettroniche sulla sola base dell'essere espresse sotto forma elettronica, assicurando, in presenza di precisi requisiti di sicurezza, che le stesse siano considerate equivalenti alle firme apposte manualmente.

I principi su cui si basa la direttiva sono, quindi, quelli della neutralità tecnologica, cercando di evitare il collegamento della direttiva ad uno o più prodotti in commercio e tenendo anzi conto del rapido evolversi delle tecnologie, della libertà d'impresa e della libera circolazione. È pertanto escluso che gli Stati membri possano introdurre o mantenere regimi di autorizzazione preventiva, pur avendo la facoltà di conservare o introdurre regimi di accreditamento facoltativi per garantire un più alto livello di sicurezza e di affidabilità dei prestatori di servizi di certificazione e dei certificati da questi emessi.

Durante la discussione i rappresentanti italiani, anche dell'Ufficio del Garante, hanno insistito a lungo per far introdurre nel testo principi di rigore riguardo alla valenza giuridica della firma elettronica, per una identificazione più chiara degli elementi necessari a poter fondare una presunzione di equivalenza con le firme manoscritte e per prevedere specifiche garanzie e sistemi di verifica. Il testo inizialmente proposto dalla Commissione è risultato poi largamente modificato nel corso delle riunioni fino alla posizione comune definita dal Consiglio dei Ministri delle telecomunicazioni dell'Unione europea il 22 aprile 1999, che ha sancito l'ingresso nello stesso di specifici riferimenti, anche nelle definizioni, alle firme elettroniche avanzate ed ai dispositivi "sicuri" di creazione e verifica delle firme stesse.

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

L'art. 8 della direttiva ha previsto infatti una serie di garanzie per la protezione degli aspetti connessi al trattamento dei dati personali, fra cui alcuni obblighi gravanti sul "certificatore" (tra essi, l'obbligo di effettuare la raccolta dei dati direttamente dai soggetti interessati alla certificazione della firma o previo loro esplicito consenso e l'obbligo di rispettare il principio di pertinenza, secondo quanto sostanzialmente disposto all'art. 6 della direttiva comunitaria n. 95/46/CE), nonché facoltà spettanti al soggetto utilizzatore della firma elettronica.

Tra queste ultime, appare rilevante la necessità della prestazione del consenso in merito alla raccolta o all'elaborazione dei dati per fini diversi da quelli necessari per il rilascio e il mantenimento del certificato. Significativo è, anche, il limite posto agli Stati membri ai quali viene preclusa la possibilità di vietare al prestatore di servizi di certificazione di riportare sul certificato uno pseu-

donimo in luogo del nome del firmatario (art. 8, par. 3). L'uso dello pseudonimo, peraltro, è stato disciplinato con l'obiettivo di garantire l'equilibrio tra il rispetto della privacy (e dunque la facoltà di riservarsi l'anonimato nell'ambito degli scambi commerciali) e la possibilità (che rimane aperta per gli Stati membri ai sensi del considerando n. 25 della direttiva), di chiedere l'identificazione delle persone in base alla normativa comunitaria o alla legislazione, fermi restando poi, gli effetti giuridici che la legislazione nazionale attribuisce agli pseudonimi (art. 8, par. 3).

Accanto alla direttiva sinora commentata, per consentire un maggiore sviluppo del commercio elettronico (prevedendo una cornice di regole armonizzate in cui dette attività si svolgano e che serva a dare fiducia ad utenti e consumatori), si colloca la proposta di direttiva del Parlamento europeo e del Consiglio relativa a taluni aspetti del commercio elettronico nel mercato interno.

La proposta, presentata nel novembre del 1998, è stata oggetto di lunga e complessa discussione ed è stata sottoposta al Consiglio Mercato interno il 7 dicembre per la definizione di un accordo politico. Il 28 febbraio 2000 il Consiglio Ecofin ha adottato una posizione comune.

Si tratta di una proposta di tipo orizzontale in quanto si aggiunge alle direttive che già disciplinano i diversi settori interessati, dettando norme solo per la parte che rileva ai fini del commercio elettronico.

La proposta intende armonizzare il quadro di riferimento per evitare che gli Stati membri adottino in materia legislazioni divergenti, creando ostacoli e turbative al mercato interno. Il provvedimento ha però destato varie perplessità sia nelle riunioni di coordinamento interministeriali, sia in seno al gruppo di lavoro del Consiglio dell'Unione che la sta discutendo.

Nelle discussioni è stato possibile superare conflitti e contraddizioni presenti nel testo originario, in particolare riguardo alla definizione del luogo di stabilimento del prestatore di servizi, alla stipulazione di contratti *on-line*; alla responsabilità degli intermediari, alla definizione della nozione di comunicazione commerciale e alle misure per incoraggiarne l'uso; alla previsione di sistemi volti a favorire l'effettiva attuazione delle norme comunitarie; ai principi di mutuo riconoscimento.

I lavori hanno mostrato una certa preferenza della Commissione europea verso la limitazione dell'oggetto della direttiva ad aspetti non specificatamente disciplinati da altre normative di settore, ed in particolare a taluni aspetti giuridici (concernenti specificatamente le comunicazioni commerciali, la conclusione di contratti *on line*, la responsabilità degli intermediari), nel dichiarato intento di rimuovere gli ostacoli risultanti dalla divergenza o dalla sovrapposizione di normative negli Stati membri per garantire, oltre all'*acquis* esistente, la libera circolazione dei servizi *on line* all'interno della Comunità.

L'Autorità è più specificamente interessata alle parti che attengono alla tutela dei dati personali, per le quali ha fornito un contributo attivo partecipando alle riunioni di coordinamento interministeriali e a quelle che si sono tenute nel gruppo di lavoro del Consiglio.

Nel corso dei lavori a Bruxelles, l'Autorità si è adoperata al meglio per ridurre il rischio che le problematiche emergenti dal raffronto tra diritti fondamentali e attività commerciali potessero rimanere irrisolte, attraverso una mera formula di deroga quale quella adottata, in quanto la proposta di direttiva reca disposizioni non sempre convergenti con quelle in materia di dati personali. Basti pensare, sotto altri profili, all'art. 7 relativo alle comunicazioni commerciali non sollecitate, agli articoli inerenti alle informazioni da fornire ai fini della conclusione del contratto e alla disciplina della responsabilità degli intermediari, temi che avrebbero richiesto un più preciso chiarimento di raccordo con la disciplina della privacy, sia al fine di dirimere possibili dubbi applicativi, sia per evitare duplicazioni di oneri informativi a carico delle parti, comunque richiesti, su base nazionale, anche ai sensi dell'art. 10 della legge 31 dicembre 1996, n. 675.

Le considerazioni formulate in relazione all'esclusione della protezione dei dati personali

secondo l'originaria previsione dell'articolo 22 della proposta, sono state accolte dal gruppo di lavoro e dalla Commissione ed hanno consentito di modificare parzialmente il testo, inserendo all'articolo 1 (relativo al campo di applicazione) una specifica esclusione per "le questioni relative alla società dell'informazione che sono coperte dalle direttive 95/46/CE e 97/66/CE". È stato del pari introdotto un nuovo considerando che spiega come la protezione dei dati personali sia disciplinata esclusivamente dalle citate direttive, le quali, avendo introdotto una disciplina più armonizzata nella materia, restano pienamente applicabili alla Società dell'Informazione.

Tale soluzione è soddisfacente nella misura in cui demanda alle direttive nn. 95/46/CE e 97/66/CE il compito di continuare a disciplinare il bilanciamento dei diritti coinvolti in materia di tutela della riservatezza. Nonostante i miglioramenti apportati, però, appare ancora non del tutto ottimale, in ragione del fatto che gli operatori a livello comunitario dovranno pur sempre verificare in più fonti normative i parametri per verificare la liceità e la correttezza dei diversi comportamenti in rete, con qualche rischio anche in termini di immediata chiarezza del dettato di varie disposizioni, a volte parzialmente sovrapposte e riportate in più testi comunitari.

2.12 Flussi transfrontalieri di dati

In materia di trasferimento di dati all'estero, non vi sono particolari deliberazioni del Garante di cui dare conto oltre a quelle già riassunte nelle precedenti relazioni (v. Relazione per l'anno 1997, p. 103-105, e Relazione per l'anno 1998, p. 80-82).

Di notevole rilievo è, invece, l'attività svolta dall'Autorità in seno ad organismi comunitari ed internazionali relativamente ai trasferimenti di dati verso Paesi terzi. Per darne conto, sia pur brevemente, è opportuno schematizzare il quadro delle disposizioni rilevanti contenute nella direttiva.

In base all'art. 25 della direttiva n. 95/46/CE è necessario, per trasferire dati in Paese terzo, che questo presenti un livello di protezione "adeguata", da valutarsi con riferimento a tutte le circostanze e, segnatamente, alla natura dei dati. Qualora la Commissione europea constati che un Paese non presenta tale livello di protezione, gli Stati membri adottano tutte le misure per impedire il trasferimento di dati della stessa natura verso tale Paese.

Per constatare su base comunitaria l'adeguatezza della protezione offerta da un Paese terzo possono essere considerati sia la legislazione nazionale, sia, dopo che sia stata accertata la situazione di inadeguatezza, gli impegni internazionali assunti con la Commissione in negoziati volti a porvi rimedio.

L'art. 26 della direttiva prevede inoltre che il trasferimento possa avvenire in determinate circostanze anche verso Paesi la cui legislazione non presenti un livello adeguato di protezione, ad esempio quando l'interessato abbia manifestato il proprio consenso o quando il trasferimento sia accompagnato da clausole contrattuali idonee ad assicurare tale protezione.

Sul piano federale, a differenza di quanto avviene a livello statale, l'ordinamento federale statunitense in materia di protezione della riservatezza non è basato su un organico strumento normativo come invece accade nell'Unione europea, essendo tale protezione affidata, per vari aspetti, ad eventuali sistemi di autoregolamentazione.

Esperti e associazioni di consumatori hanno perciò auspicato l'introduzione di maggiori garanzie, mentre alcuni organismi imprenditoriali hanno manifestato incertezze circa l'impatto che il requisito dell'adeguatezza richiesto dalla disciplina comunitaria potrebbe avere sul flusso di dati tra Europa e Stati Uniti.

Il Governo Usa (e in particolare il Dipartimento del commercio) ha promosso l'elaborazione - ancora in corso - di alcuni *"International Safe Harbor Privacy Principles"* nonché di una guida per la loro attuazione, articolata in una serie di risposte alle domande che più frequentemente si pongono in materia (FAQ).

In sostanza, alla luce di tali principi, come determinati in un negoziato preliminare tra la parte statunitense e la Commissione europea, quest'ultima, con apposita decisione da adottarsi ai sensi dell'art. 25, par. 2, della direttiva (sulla base del parere del Comitato di seguito citato), introdurrebbe la presunzione che i principi (applicati conformemente alla guida) garantiscono un livello adeguato di protezione dei dati trasferiti dalla Comunità ad organizzazioni insediate negli Usa, purché queste si impegnino a rispettare i principi contenuti nel *"Safe Harbor"*.

L'importanza che una simile decisione avrebbe è evidente in riferimento, anzitutto, al principio di non discriminazione nei confronti di altri Paesi terzi presso, alcuni dei quali si registra al riguardo un atteggiamento di attesa.

Da un lato, i Paesi terzi avrebbero interesse ad evitare nei loro riguardi interpretazioni ed applicazioni della normativa comunitaria più rigorose di quelle praticate in seno alla Comunità. Dall'altro, per quanto riguarda i Paesi terzi, definire "adeguato" il livello di protezione adottato negli Usa significa indicare il livello oltre il quale difficilmente la parte europea potrebbe chiedere adeguamenti ad altri Stati.

Inoltre, se si tiene conto dei diritti fondamentali e degli interessi economici in materia, risulta chiaro che una simile decisione sarebbe di rilevante importanza anche per l'attività di revisione della direttiva n. 95/46/CE, prevista dal relativo art. 33 decorsi tre anni dalla scadenza del termine per la sua attuazione.

In questo quadro, la parte europea (e al suo interno diversi Paesi membri ed autorità di garanzia tra cui quella italiana), ha costantemente sottolineato, nel corso del negoziato, l'importanza dell'effettività degli strumenti di tutela posti in essere. Infatti, senza adeguati ed efficaci strumenti di attuazione, volti a consentire l'effettiva realizzazione dei diritti riconosciuti agli interessati, ovvero agevoli e idonee forme di soddisfazione in caso di loro violazione, i diritti sanciti dalle norme comunitarie rimarrebbero solo sulla carta, e il trasferimento dei dati in Paesi terzi diventerebbe in molti casi lo strumento per eludere le norme stesse.

Il negoziato ha avuto però fasi alterne e una bozza completa e consolidata di accordo si è inoltre resa disponibile solo da ultimo.

In questo quadro si colloca l'intensa attività svolta dal Garante, sia in incontri di studio o comunque non ufficiali, sia, soprattutto, in seno agli organismi a livello comunitario previsti dalla citata direttiva n. 95/46/CE. Si allude, in particolare, al Gruppo di lavoro di cui all'art. 29 della medesima direttiva (composto da rappresentanti di ciascuna autorità nazionale e da un rappresentante della Commissione), al quale spetta, tra l'altro, il compito di formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei Paesi terzi; nonché al Comitato di cui all'art. 31 (composto da rappresentanti degli Stati membri e presieduto da un rappresentante della Commissione).

Nell'ambito di quest'ultimo il Garante ha operato in costante e proficuo raccordo con il Ministero della giustizia, che rappresenta il Governo, e ciò ha consentito l'espressione di un orientamento comune.

Oggetto della valutazione di tali organismi, con riferimento ad una complessa attività di negoziazione svolta dalla Commissione, è stata principalmente la situazione statunitense.

L'ingente attività dei predetti organismi su tale argomento è diffusamente documentata negli allegati della presente relazione, dai quali si evince l'efficace ruolo di impulso svolto in par-

ticolare dal Gruppo di cui all'art. 29 che, in generale sintonia con il Comitato, ha sollecitato, a più riprese, l'introduzione di un livello più elevato di garanzie rispetto ai diversi principi del *Safe Harbor* (informativa, consenso, diritto di accesso, ulteriori trasferimenti e utilizzazioni di dati, *enforcement*).

Grazie a questa attività, i principi del *Safe Harbor* (inizialmente assai vaghi e vanificati da alcune interpretazioni restrittive inserite nelle *FAQ*) sono stati oggetto di un certo miglioramento, sia pure assai graduale. Il loro adeguamento è tuttora in corso e la posizione definitiva dei medesimi organismi non è ancora definita, essendo prevista nell'ambito delle riunioni che si terranno, in particolare, nel mese di maggio del 2000.

Il proficuo contributo offerto dall'Autorità italiana (che nella persona del prof. Rodotà ha svolto le funzioni di vice presidenza del Gruppo di cui all'art. 29 e, dal marzo del 2000, di presidenza), è testimoniato, tra l'altro, dall'incontro avuto con il sottosegretario di Stato americano Aaron in visita al Garante nel gennaio del 1999, dalla recente audizione del presidente del Garante avvenuta il 22 febbraio 2000 dinanzi al Parlamento europeo, dalla partecipazione alla visita ufficiale a Washington del 18-20 gennaio 2000 del Comitato di cui all'art. 31 (cui ha partecipato, per il Garante, il segretario generale), da alcuni comunicati stampa del Garante, nonché dai diversi contributi, chiarimenti e prese di posizione anche sulla stampa dei rappresentanti del collegio del Garante e del segretario generale.

In proposito il Garante ha segnalato anche l'esigenza di valutare con maggiore attenzione le competenze degli organi statutitensi che dovrebbero svolgere un controllo indipendente, le effettive garanzie di ricorso offerte agli interessati, anche in riferimento alle inibitorie, alla determinazione della legge applicabile e al risarcimento del danno, atteso anche il fatto che l'intervento della *Federal Trade Commission* (il principale organo cui verrebbero presentati i reclami degli interessati), risulta circoscritto negli ultimi due anni ad un numero assai ristretto di casi rispetto alle diverse centinaia di interpelli ricevuti.

Il Garante ha altresì rappresentato che un automatico inserimento nell'elenco delle società aderenti al sistema di autoregolamentazione, non assoggettato al controllo di determinati requisiti, potrebbe favorire l'attività di società di comodo, che potrebbero svanire nel nulla dopo aver trasferito i dati ad un'altra entità, sottraendosi di fatto a qualunque forma di responsabilità. Diverse altre osservazioni sono state formulate per quanto riguarda il livello di garanzie dei principi nonché la loro tutela giurisdizionale e amministrativa.

Sono altresì ancora da approfondire i rapporti tra la decisione della Commissione e i poteri delle autorità nazionali, giudiziarie e di garanzia. Ciò in quanto la base giuridica prospettata per la decisione (l'art. 26, par. 6 della direttiva) conferisce alla Commissione competenze di esecuzione relative alla valutazione di adeguatezza, ma lascia impregiudicati i poteri di tali autorità sui singoli casi.

Il *Safe Harbor* sembra peraltro destinato a coprire soltanto una parte dei flussi verso gli USA, lasciando non regolata un'alta percentuale di trasferimenti che, unitamente a quelli considerati nel negoziato, potrebbero essere con ogni probabilità regolati meglio. Ciò attraverso il ricorso a clausole contrattuali per vincolare sia chi esporta i dati, sia chi li utilizza nel Paese terzo, a condotte regolate più specificamente, anche sotto il profilo della giurisdizione applicabile e del risarcimento del danno, sulla falsariga della proficua esperienza maturata in diversi Paesi membri.

Alcuni schemi di clausole o contratti tipo in materia di protezione dei dati sono peraltro già stati valutati e perfezionati a cura del Consiglio d'Europa, dell'OCSE e dell'*International Chamber of Commerce*, e fanno quindi parte del materiale a disposizione della Commissione per l'elaborazione a livello comunitario. In tal senso, oltre all'attività propulsiva svolta in seno alla

Comunità europea, il Garante ha seguito con attenzione i lavori dell'*International Commerce Exchange* per la definizione di un codice di condotta sulla privacy, nonché di un modello contrattuale da utilizzare per il flusso transfrontaliero di dati, anche al fine di orientare la prassi degli operatori economici coinvolti tramite la formazione di regole condivise e, perciò, rispondenti alle indicate esigenze di effettività.

2.13 Videosorveglianza

L'Italia manca tuttora di una disciplina specifica in materia di video-sorveglianza che pure appare sempre più necessaria ed urgente. Altri Paesi quali Francia, Danimarca, Islanda, Norvegia (e, dal 1999, la Spagna) dispongono invece di un quadro normativo articolato. Nel 1998, il *Data-Protection Registrar* inglese ha predisposto al riguardo un codice di comportamento (*"Code of Practice"*). In Germania, nel marzo dell'anno in corso, la 59.ma Conferenza delle Autorità di protezione dei dati a livello federale e regionale ha approvato una risoluzione che invita il legislatore a introdurre determinati principi di regolamentazione.

La direttiva comunitaria n. 95/46/CE e la Convenzione n. 108/1981 del Consiglio d'Europa vincolano i Paesi membri ad applicare la disciplina sul trattamento dei dati personali anche a dati cifrati o codificati, nonché ai suoni e alle immagini (quali quelle registrate nei controlli video o in altri sistemi di videosorveglianza), qualora permettano di identificare un soggetto anche in via indiretta.

La legge 31 dicembre 1996, n. 675 che - ha attuato la Convenzione n. 108 e ha in buona parte permesso di recepire la direttiva europea - considera anch'essa come "dato personale" qualunque informazione che permetta l'identificazione, anche in via indiretta, dei soggetti interessati, ivi compresi, appunto, i suoni e le immagini (art. 1, comma 1, lett. c), l. n. 675/1996).

Nella perdurante mancanza di una normativa specifica, il Garante ha perciò sollecitato, in sede di verifica dei vari sistemi realizzati o in progetto a cura di enti e di organismi che si sono rivolti all'Autorità, il rispetto di principi desumibili dalla legge n. 675, richiamando l'attenzione sulla necessità che ogni sistema di video-sorveglianza sia attivato e gestito solo in presenza di articolate garanzie che dovrebbero riguardare, in modo particolare, l'eventuale intenzione di conservare le immagini e i suoni in appositi archivi, l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'amministrazione preposta, nonché l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici.

Ad esempio, in merito al parere chiesto al Garante dalla Presidenza del Consiglio dei Ministri e dal Dipartimento della Funzione pubblica sullo schema di regolamento per l'autorizzazione all'installazione ed all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, il Garante (con provvedimento del 24 febbraio 1999, in Bollettino n. 7, pag. 25) ha constatato con soddisfazione la previsione di disposizioni riferite al trattamento dei dati personali.

In particolare, detto regolamento prevede che gli impianti rilevino immagini solo in caso di infrazione e, per il resto, effettuino il monitoraggio del traffico, attraverso dati anonimi. Sono altresì prevista l'utilizzazione dei dati per le sole finalità di applicazione del regolamento medesimo, salva la possibilità di uso dei dati per fini di giustizia e la disponibilità di dati anonimi per studi e statistiche; la conservazione delle immagini per il solo periodo necessario all'applicazione delle infrazioni e alla definizione dell'eventuale contenzioso; l'esclusione di interconnessioni con altri archivi o base dati; nonché il tracciamento delle consultazioni della banca dati che custodisce le immagini. Nell'ambito di una collaborazione istituzionale proficuamente instaurata, i suggerimen-

ti di modifica dello schema formulati dal Garante sono stati accolti pressoché interamente in sede di emanazione del d.P.R. 22 giugno 1999, n. 250.

In una successiva occasione il Garante ha invece esaminato l'ipotesi che il Comune di Torino ha formulato per installare nonché d'intesa con le forze di polizia, un sistema di video-sorveglianza sui mezzi di trasporto pubblico urbano dell'ATM (Azienda torinese mobilità), presso alcune fermate, nel quadro di un'azione mirante a contenere il fenomeno della criminalità e a diminuire la pericolosità di ambiti cittadini particolarmente insicuri.

Con provvedimento del 23 marzo 1999 (in Bollettino n. 8, p. 57), l'Autorità ha in primo luogo osservato come in tale progetto le finalità fossero da una parte ispirate alla prevenzione e alla repressione dei reati e, dall'altra, basate su una connessa tutela del patrimonio pubblico (mezzi di trasporto, impianti fissi ecc.), oltre che dettate da un intento di generale cura del benessere cittadino.

Alla luce di tali finalità, il Garante ha inteso verificare la posizione dei soggetti coinvolti nell'iniziativa, identificando il "titolare del trattamento" nel Comune di Torino, quale centro di imputazione e riferimento degli interessi coinvolti e ravvisando nell'Azienda il possibile ruolo del responsabile del trattamento. Il Garante ha poi indicato la necessità di regolare i seguenti profili prima dell'avvio del progetto:

a) verificare la posizione dei soggetti coinvolti nell'iniziativa e procedere alla formale identificazione del titolare e del responsabile del trattamento;

b) determinare con precisione la localizzazione delle telecamere e le modalità di ripresa in aderenza alle finalità che avevano suggerito l'installazione del sistema, tenendo conto dei principi fondamentali fissati dall'art. 9 della legge n. 675/1996, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti. Al riguardo, si è suggerito di predisporre modalità di ripresa che permettano, per quanto tecnicamente possibile, di evitare riprese particolareggiate tali da risultare eccessivamente intrusive della riservatezza delle persone o da permettere la rilevazione di particolari non rilevanti;

c) evitare che le telecamere riprendano in modo stabile le postazioni di guida dei conducenti, anche in considerazione dei limiti posti all'installazione di impianti audiovisivi dall'art. 4 della legge 20 maggio 1970, n. 300 (cd. Statuto dei lavoratori);

d) evidenziare che le immagini visionate per finalità di polizia giudiziaria possano essere utilizzate per controlli, anche indiretti, sull'attività lavorativa dei dipendenti ATM;

e) delimitare puntualmente i soggetti legittimati a trattare i dati personali, individuando con precisione, così come richiesto dall'art. 19 della legge n. 675, gli incaricati del trattamento;

f) prevedere tutte le misure di sicurezza idonee per evitare fenomeni di dispersione dei dati o di accessi non autorizzati, ecc.;

g) garantire in modo costante l'impossibilità di accesso diretto alle immagini registrate, specie presso i terminali "locali" a bordo dei mezzi o presso le fermate; la regolare distruzione delle immagini non oggetto di segnalazione; il rigoroso controllo di sicurezza sui dati registrati che, a seguito di denuncia, vengono esaminati dall'autorità di polizia;

h) consentire l'accesso alla cd. "stazione di lettura" mediante il sistema della "doppia chiave" congiunta (una in possesso del personale preposto ATM e una in possesso dell'autorità di polizia), essendo la visione "in chiaro" delle immagini registrate strettamente connessa alla commissione di atti criminosi ed alla previa denuncia degli stessi all'autorità di polizia;

i) fornire agli interessati, da parte del titolare del trattamento, le informazioni previste dall'art. 10 della legge n. 675/1996, segnalando in maniera idonea agli utenti del servizio di trasporto l'esistenza del sistema di video-sorveglianza.

Inoltre, in risposta alle informazioni fornite dal Comune di Riomaggiore in ordine alla realizzazione di un sistema di video-sorveglianza nella zona B di Punta Montenegro della Riserva Marina delle Cinque Terre, d'intesa con la Capitaneria di Porto della Spezia, il Garante (con provvedimento del 21/10/1999, in Bollettino n. 10, pag. 80) ha sollecitato un'attenta riflessione volta ad appurare:

j) l'esistenza di una fonte normativa che legittimi l'installazione di tali sistemi di video-sorveglianza e che ne indichi le relative finalità, e cioè se tale iniziativa risponda alle funzioni istituzionali demandate all'ente. A tal fine, è apparso altresì necessario che fosse precisato come si configurano dal punto di vista della legge n. 31 dicembre 1996, n. 675, le posizioni dei soggetti coinvolti nell'iniziativa (Capitaneria di Porto di La Spezia e Comune di Riomaggiore), anche alla luce degli scopi dagli stessi perseguiti;

k) la precisa localizzazione delle telecamere e le modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limite della possibilità di avvicinamento dell'immagine), anche al fine di assicurare il rispetto dei principi fondamentali fissati dall'art. 9 della legge, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;

l) l'individuazione di idonee ed appropriate misure per assicurare un utilizzo corretto dei dati da parte dei soggetti legittimati (art. 15 della l. n. 675/1996);

m) le procedure e le modalità volte a fornire agli interessati le informazioni previste dall'art. 10 della legge.

In questo quadro, il Garante ha perciò manifestato perplessità per l'attivazione di un sistema di video-sorveglianza privo di un insieme articolato di garanzie, che dovevano riguardare, in modo particolare, l'eventuale intenzione di conservare le immagini in un apposito archivio, l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'ente e l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti.

Riguardo a quest'ultimo aspetto, l'Autorità ha fatto inoltre presente che la divulgazione di dati tra soggetti pubblici richiede l'esistenza di una puntuale norma di legge o di regolamento ed è possibile, in via del tutto residuale, anche quando non sia prevista da una norma, purché sia necessaria per lo svolgimento di alcune funzioni istituzionali e sia effettuata una comunicazione preventiva al Garante (il quale potrebbe vietarla in caso di violazione di legge: art. 27, comma 2).

In seguito, fornendo riscontro a una richiesta di parere in ordine alla delibera della Giunta comunale di Portici con la quale è stato approvato un regolamento per l'installazione e l'utilizzo di impianti di videosorveglianza del territorio, di telecontrollo ambientale e di pannelli a messaggi variabili, il Garante (con provvedimento del 17 febbraio 2000) ha ricordato che, per i soli aspetti riguardanti l'installazione e l' esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici o nelle zone a traffico limitato, è stato introdotto, mediante apposito regolamento (d.P.R. 22 giugno 1999, n. 250), l'obbligo per i comuni di richiedere un'autorizzazione rilasciata dal Ministero dei lavori pubblici-Ispettorato generale per la circolazione e la sicurezza stradale. Il Garante ha altresì rilevato che il progetto tiene conto di alcune indicazioni formulate dall'Autorità in relazione ad analoghe iniziative di enti locali e di amministrazioni centrali. Il Garante ha ribadito, ad ogni modo che, tra le finalità elencate dal provvedimento della Giunta, possono essere perseguite solo quelle che rispondono alle funzioni istituzionali demandate all'ente, come già indicato nel caso del Comune di Riomaggiore. Analogamente ai casi già illustrati, il Garante ha reputato inoltre necessarie:

a) una localizzazione più precisa delle telecamere e una limitazione delle modalità di ripresa delle immagini, con particolare riguardo al livello di dettaglio della ripresa dei tratti somatici delle persone presso gli impianti volti unicamente a prevenire le violazioni al codice di strada;

b) l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'ente e la precisazione delle finalità per le quali potranno essere autorizzati eventuali accessi di persone diverse dai responsabili e dagli incaricati;

c) una puntuale verifica, per quanto riguarda l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici;

d) l'indicazione del soggetto o della struttura cui il cittadino può rivolgersi per esercitare i diritti di cui all'art. 13 della legge;

e) le modalità dell'eventuale riutilizzazione dei supporti magnetici una volta cancellati;

f) la precisazione che, ai fini dell'analisi dei flussi di traffico, il trattamento è effettuato con modalità volte a salvaguardare l'anonimato, ma solo successivamente alla fase della raccolta, giacché le immagini registrate possono contenere dati di carattere personale.

Analoghe indicazioni sulla necessità di apportare le opportune modificazioni sono state formulate dal Garante (con provvedimento del 7 marzo 2000) riguardo al progetto di installazione di un sistema di video-sorveglianza ipotizzato dal Comune di Mantova con finalità di rilevazioni a fini statistici e di studio degli accessi dei veicoli al centro storico e alle zone al traffico limitato, nonché per finalità di controllo a distanza con funzione di prevenzione e repressione di attività illecite.

Il Garante aveva potuto già evidenziare positivi elementi di collaborazione con il Ministero dell'interno, in merito all'attività del Comitato di sorveglianza del Programma operativo "Sicurezza per lo Sviluppo del Mezzogiorno d'Italia" con riguardo agli interventi di innalzamento dello standard di sicurezza lungo l'asse autostradale Salerno-Reggio Calabria, attraverso un sistema integrato di video-sorveglianza e di comunicazione satellitare. Va sottolineato in proposito che tale sistema prevede, tra l'altro, il controllo degli accessi autostradali e delle aree di servizio e di parcheggio tramite telecamere "intelligenti" per la lettura delle targhe delle autovetture in transito; dette telecamere avrebbero in dotazione un software che, programmato con liste di targhe "sensibili", effettuerebbe una comparazione in tempo reale con l'immagine ripresa, fornendo, in caso di rilevazione positiva, segnali di allerta al centro di controllo.

L'Autorità ha apprezzato l'attenzione dimostrata dal Ministero dell'interno nella predisposizione del progetto, ai fini dell'adozione di misure organizzative e di sicurezza volte a garantire il rispetto della normativa in materia di protezione dei dati personali. In particolare, su richiesta del Garante (con nota del 15 dicembre 1998), sono stati forniti elementi più dettagliati circa:

a) le diverse modalità di gestione delle immagini riprese dalle videocamere utilizzate dal sistema di controllo, anche in riferimento alle aree di servizio lungo l'asse autostradale e al monitoraggio del traffico sospetto;

b) le misure di sicurezza adottate anche in riferimento alla codifica dei segnali e delle immagini;

c) i meccanismi per fornire un'adeguata informazione agli interessati sulla viabilità e nelle aree di servizio;

d) la non previsione di rilevazioni di tipo acustico integrati al sistema di video-sorveglianza.

Il Garante, circa la conservazione delle informazioni e l'accesso alla consultazione, ha poi rilevato (con nota dell' 8 giugno 1999) l'opportunità che:

a) i dati relativi alle immagini o alle targhe automobilistiche non confluiscano in altri archivi o banche dati o, comunque, non siano intrecciati con altre informazioni diverse da quelle strettamente necessarie per l'espletamento dei controlli o delle indagini;

b) si predisponga, ove non previsto, un sistema di tracciamento delle consultazioni degli archivi.

Principi analoghi potranno essere formulati dal Garante in riferimento ad altri interventi progettuali previsti nel Mezzogiorno presso altri percorsi autostradali e tratte viarie.

In sintesi, la differenza che il Garante ha riscontrato nello svolgimento della propria attività rispetto al precedente anno è stata la moltiplicazione dei progetti di installazione di sistemi vasti e articolati di video-sorveglianza dentro e fuori gli spazi urbani. I sistemi di monitoraggio visivo, dapprima circoscrivibili ad una piazza o a una strada, si estendono a percorsi tramviari cittadini, poi alla superficie urbana in porzione più o meno estesa, successivamente ad aree comunali con l'inclusione di spazi naturali e, infine, tendono a coprire settori sempre più estesi del territorio.

Allo scopo di avere un quadro dettagliato e capillare di questo fenomeno il Garante ha deciso - senza precedenti in Italia, ma con numerosi riscontri in altri Paesi industriali avanzati- di conferire un incarico di consulenza sulla diffusione e sulla consistenza delle diverse forme di video-sorveglianza utilizzate in luoghi pubblici, esercizi commerciali, supermercati, banche, ecc. La ricerca, necessariamente di tipo preliminare, è in via di espletamento in alcune città campione del Nord, del Centro e del Sud, sulla base di schede analitiche di rilevamento. La decisione è stata presa in attesa della complessiva regolamentazione della materia attraverso uno dei decreti legislativi che il Governo era stato delegato ad emanare (in base all'art. 1, comma 1, lettera i) l. n. 676/1996) e che, se verrà nuovamente conferita tale delega attualmente scaduta, dovrà fissare le norme per un giusto equilibrio tra il diritto alla riservatezza dei cittadini e le esigenze di pubblica sicurezza e della prevenzione dei reati.

Il Garante ha inoltre avviato una ricerca interna su vari aspetti specie giuridici, culturali e sociali del fenomeno della video-sorveglianza, in Italia e all'estero. La ricerca prevede la raccolta e la classificazione di articoli di stampa da quotidiani, periodici italiani e internazionali e riviste specializzate, nonché di saggi, monografie, repertori bibliografici e materiali riversati anche da siti Internet a partire dal 1 gennaio 1997.

2.14 La disciplina della sicurezza nel trattamento dei dati

L'attenzione della legge al tema della sicurezza non è episodica, essendo maturata in un contesto di iniziative nazionali ed internazionali che hanno inteso riempire un vuoto legislativo sulla materia evidenziato da tempo e in varie sedi.

A partire dalla fine degli anni ottanta, vari organismi e sedi internazionali quali l'OCSE, il G 7, il G 10, il GAFI, EUROPOL e il Consiglio d'Europa, ognuno per quanto di competenza ed in base alle tematiche in agenda, hanno richiamato l'attenzione sulla sicurezza informatica e telematica. Dal lungo e complesso dibattito internazionale sono derivate indicazioni utili, raccomandazioni, risoluzioni, direttive, convenzioni ed accordi.

Il riflesso di tale attività nell'ordinamento interno è stato, al contempo, intenso e significativo. Dalla legge n. 518/1992 sulla tutela giuridica dei programmi per elaboratore al successivo decreto n. 205 del 15 marzo 1996, nonché alla legge n. 547/1993 sui crimini informatici (che ha esteso, tra l'altro, l'operatività di determinate disposizioni incriminatrici ai soli sistemi informatici "protetti"). Sono intervenute inoltre alcune discipline particolari che, direttamente o indirettamente, riguardano il tema della sicurezza. Si allude, ad esempio, all'obbligo di misure di sicurezza nei centri edp tenuti al rispetto del segreto d'ufficio (d.P.C.M. del 15 febbraio 1989), al d.P.R. 5 luglio 1995, n. 417, riguardante le biblioteche pubbliche statali, così come alla legge n. 59/1997 sulla riforma della p.a. (art. 15, comma 2) e al d.lg. n. 115/1995 (che prevede precisi obblighi per produttori, distributori e detentori riguardo all'immissione di prodotti sicuri sul mercato).

Come è noto, anche la legge del 31 dicembre 1996, n. 675, attribuisce al tema della sicurez-

za dei dati grande importanza e rilievo, facendone scaturire obbligazioni di carattere "trasversale" riferibili ad ogni tipo di trattamento.

Tale esigenza ha trovato attuazione nella Sezione III del Capo III della legge n. 675/1996, significativamente intitolata *"Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento del danno"*.

L'articolo 15 della legge può essere considerato una norma "aperta", che si limita a fissare le finalità e gli "obiettivi di sicurezza" che devono essere perseguiti dal titolare, con modalità e strumenti destinati a essere dettagliati con diversi strumenti.

L'intervenuta emanazione del regolamento con il D.P.R. n. 318/1999, che va ad aggiungersi alle norme sopra richiamate, ha gettato quindi le basi per una disciplina "generale" della sicurezza, la cui importanza emerge anche dalla circostanza che le disposizioni previste al citato articolo 15 interessa anche a trattamenti pubblici in materia di polizia, giustizia, difesa e sicurezza dello Stato ai quali la legge n. 675, com'è noto, si applica solo in parte (v. art. 4 l. n. 675). Inoltre, nel corpo del testo del d. lg. n. 135/1999 recante *"Disposizioni integrative della legge 31 dicembre 1996 n. 675, sul trattamento dei dati sensibili da parte dei soggetti pubblici"*, segnatamente all'articolo 17, comma 4, è contenuto un esplicito richiamo al dettato dell'articolo 15, commi 2 e 3.

Ponendo attenzione al complessivo impianto normativo, emerge con evidenza la finalità di ridurre al minimo i predetti rischi mediante l'utilizzazione di sistemi di sicurezza costantemente adeguati nel tempo

Ciò, per due diverse necessità: da un lato, l'articolo 18 della legge n. 675/1996, prevede che il titolare ed il responsabile (se designato) debbano risarcire gli eventuali danni ai sensi dell'articolo 2050 del codice civile. Dall'altro, la legge prevede l'individuazione di misure di sicurezza minime, la cui mancata adozione comporta l'irrogazione di una sanzione penale. L'art. 36 della legge stabilisce infatti che la responsabilità sussista qualora non siano rispettati, o lo siano stati solo parzialmente, gli standard "minimi" di sicurezza prescritti dall'apposito regolamento governativo.

L'art. 15 della legge n. 675/1996 disciplina due tipi differenti di misure: da un lato, il comma 1, che prescrive misure di sicurezza tali da ridurre al minimo il rischio, non individuate ma individuabili sulla base di soluzioni tecniche concretamente disponibili (la loro mancata predisposizione comporta responsabilità civile in caso di danno). Dall'altro, e al loro interno, le misure "minime" previste al comma 2, specificatamente individuate all'interno di un ulteriore atto (il regolamento), che contiene i vari precetti della norma contenuta nell'articolo 36, la cui violazione comporta anche una sanzione di carattere penale.

Pertanto, il regolamento non è destinato a contenere tutte le regole tecniche da adottare in ogni caso per la sicurezza dei dati personali, in riferimento alle diverse modalità di trattamento utilizzate, ma individua unicamente quei requisiti volti ad introdurre un livello *minimo* di protezione, il cui mancato rispetto comporta una maggiore esposizione a rischio del bene giuridico tutelato dalla norma.

La particolarità di tale strumento consiste poi in una impostazione di tipo flessibile, essendo destinato ad un aggiornamento avente cadenza almeno biennale, all'evidente fine di evitare una sua oggettiva "staticità" a fronte di un'evoluzione tecnologica sicuramente "dinamica". Il regolamento non intende quindi individuare le migliori misure evidenziate dalla scienza tecnica in un dato momento, mirando più semplicemente ad enucleare un minimo denominatore comune delle misure di sicurezza disponibili, tale da poter definire le stesse "minime".

In coerenza con la legge da cui promana, il regolamento previsto dalla legge n. 675 si rivolge a tutti i soggetti – pubblici e privati – che nell'ambito delle loro attività pongono in essere un trattamento di dati personali.

Con il regolamento si sono individuate categorie omogenee di modalità di trattamento di dati, al fine di correlare la soglia minima, da un lato, alla tipologia del dato e, dall'altro, allo strumento tecnico utilizzato per il trattamento, tenendo conto della distinzione già operata dalla legge tra dati "comuni" e "sensibili" (dovendosi considerare anche la loro diversa valenza nel quadro di una differente intensità del livello di garanzie per essi previsto).

Nel d.P.R. n. 318 una prima, grande distinzione ha avuto riguardo alle modalità delle operazioni svolte per effettuare il trattamento. Da una parte, quelle effettuate in sostanza con l'esclusivo ausilio di supporti cartacei; dall'altra, quelle poste in essere anche in parte mediante strumenti elettronici o comunque automatizzati.

L'ottica in cui sono state previste le misure di sicurezza è insita non solo nella protezione dei sistemi o delle trasmissioni in quanto tali, ma, più direttamente, nella protezione dei dati personali: il livello di sicurezza si modifica di conseguenza in relazione alla presenza o meno dei dati stessi. Così pure, nel caso siano contestualmente presenti dati "comuni" e "sensibili", è necessario osservare le misure previste per la categoria più elevata).

Va evidenziato, inoltre, come nel regolamento si sia preferito non individuare per ogni singola misura di sicurezza i soggetti tenuti ad adottarla. Tale individuazione dipenderà dalle attribuzioni del titolare del trattamento e dai ruoli ed incarichi conferiti in concreto all'interno della struttura.

Quanto alle definizioni, il regolamento, oltre ad utilizzare quelle già contenute dalla legge 675, prevede quelle di:

- "misure minime", intendendo per esse il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto, in relazione ai rischi a cui fa riferimento l'articolo 15, comma 1, della legge (misure, che possono ad esempio comportare, nei casi previsti nei successivi articoli: l'identificazione dell'utente, l'autorizzazione all'accesso alle funzioni, ai servizi, ai locali, ai dati, la registrazione degli ingressi e i limiti al riutilizzo di supporti per l'archiviazione elettronica o automatizzata o cartacea);
- "strumenti", intendendo per essi i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
- "amministratori di sistema", riferendosi ai soggetti cui è conferito il compito di sovraintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne la utilizzazione.

Quanto agli effetti che il regolamento spiega sui trattamenti effettuati a fini esclusivamente personali, - eccettuati in generale dall'osservanza dei diversi obblighi nomativi fissati dalla medesima legge (a condizione che i *"dati non siano destinati ad una comunicazione sistematica o alla diffusione"*), ma comunque sottoposti agli obblighi di sicurezza -, il regolamento ha previsto misure di sicurezza tali da tener conto in modo adeguato del possibile, minore rischio insito in tale attività.

Considerato che anche alcune osservazioni formulate nella fase di predisposizione del regolamento sia dal Consiglio di Stato, sia dal Garante andavano nella direzione di limitare, per quanto possibile, l'ambito di applicazione della norma penale in materia di sicurezza, con l'intuibile intento di evitare un'applicazione irragionevole e diffusa della sanzione, si è prevista la sua applicazione soltanto ai trattamenti dei dati di cui agli artt. 22 e 24 della legge organizzati in archivi ed effettuati mediante elaboratori stabilmente accessibili da altri elaboratori, escludendo in tal modo i computer *"stand alone"*. Per quelli caratterizzati invece dalla predetta accessibilità, la misura minima di sicurezza è stata individuata nel solo obbligo, per il soggetto titolare, dell'utilizzo di una parola chiave che inibisca l'accesso al sistema o anche solamente ai dati.