

ta, come è argomentabile dall'art. 20, comma 1, lett. g) della legge n. 675/1996, che non prevede la diffusione senza consenso dei dati acquisiti per finalità di difesa. Pertanto, mentre sarebbe stato possibile consegnare la videocassetta all'autorità giudiziaria, non era lecito allegare la stessa ad una rivista. Di qui, la conferma del provvedimento di blocco e l'accoglimento del relativo ricorso.

46. ATTIVITÀ GIORNALISTICA E RISPETTO DEI PRINCIPI
DELLA LEGGE N. 675/1996

In diverse circostanze, il Garante ha dovuto ribadire la necessità di applicare la normativa – in ampia parte di carattere speciale – dettata con riguardo ai trattamenti di dati personali svolti nell'ambito dell'attività giornalistica. Così, ad esempio, nel dichiarare infondato un ricorso presentato contro alcune importanti testate nazionali da parte di una testimone all'interno di un procedimento penale per gravi reati (*Prov. del 3 luglio 2000*), l'Autorità ha chiarito che il trattamento doveva essere valutato alla luce di quanto disposto dall'art. 25 della legge n. 675/1996 e dal codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*Prov. del 29 luglio 1998*, in *G.U.* del 3 agosto 1998).

Pertanto, quando gli articoli o i servizi pubblicati costituiscono una legittima espressione del diritto di cronaca, magari in relazione – come nel caso di specie – a delicate indagini volte ad appurare l'attendibilità di una testimone (l'interessata) e di sue rilevanti dichiarazioni ai fini processuali, e il trattamento è finalizzato ad informare l'opinione pubblica sugli sviluppi di una vicenda che ha richiamato l'attenzione a livello nazionale, nel rispetto dell'essenzialità dell'informazione e della pertinenza dei dati riferiti, lo stesso trattamento deve considerarsi legittimo. In tal caso, quindi, non può invocarsi il mancato conferimento, da parte dell'interessata, del preventivo consenso al trattamento dei dati, essendo questo esplicitamente escluso dalle disposizioni appena richiamate. Ciò, anche quando attraverso gli articoli e le trasmissioni vengano diffusi dati di carattere sensibile, essendo anche in questa ipotesi consentito prescindere dal consenso, naturalmente ove sia rispettato il limite posto al diritto di cronaca dall'essenzialità dell'informazione e si evitino riferimenti a congiunti o ad altri soggetti non interessati ai fatti (art. 5 del citato codice deontologico).

Argomentazioni analoghe hanno fondato la decisione originata da un ricorso – poi dichiarato infondato – presentato da alcuni consiglieri di amministrazione, dirigenti e giornalisti di una delle principali aziende radiotelevisive nazionali che lamentavano l'avvenuta pubblicazione su un quotidiano di una serie di articoli in cui venivano evidenziate asserite appartenenze politiche degli stessi, nonché rapporti e relazioni personali (amichevoli od ostili) esistenti all'interno dell'azienda televisiva medesima (*Prov. del 31 maggio 2000*). Anche in tal caso l'Autorità, applicando la disciplina sopra richiamata, ha ritenuto che gli articoli fossero espressione di una legittima modalità di esercizio del diritto di cronaca – per quanto opinabili potessero essere i toni utilizzati – con riferimento alla personalità, alle esperienze professionali ed agli incarichi ricoperti dalle persone su indicate, le quali occupavano appunto posti di rilievo in un'azienda di primaria rilevanza sociale.

Nel caso di specie, non sussistevano gli estremi per censurare il diritto dei mezzi di informazione di esprimere valutazioni, anche critiche, riferite alle singole persone, atteso che, peraltro, le notizie riportate potevano essere acquisite correttamente dai giornalisti attraverso la consultazione di giornali, interviste, colloqui, dichiarazioni o attingendo alle consuete fonti lecitamente utilizzate nella cronaca giornalistica. Tale pronuncia del Garante, come altre analoghe, non era ovviamente preclusiva per gli interessati della possibilità di adire il giudice ordinario per rivolgere eventuali diverse istanze in sede civile o penale che esulano dall'ambito di competenza del Garante.

In questo contesto, merita infine di essere ricordata la decisione con la quale l'Autorità ha dichiarato non fondato un ricorso presentato dal titolare di una ditta artigiana. Questi aveva infatti lamentato l'avvenuta pubblicazione su un quotidiano locale della notizia secondo la quale alcuni consiglieri comunali avevano segnalato alla Corte dei conti il comportamento di un comune concernente una transazione con il ricorrente, relativamente al versamento di una penale contrattuale legata a "gravi motivi di salute" del ricorrente medesimo (*Prov. del 22 gennaio 2001*, in *Bollettino* n. 16, p. 8). In tale circostanza il Garante ha constatato che l'articolo riguardava una contestata vicenda amministrativo-erariale che traeva spunto da atti e documenti accessibili al pubblico. La vicenda era quindi riferita ad un fatto di interesse generale relativo al corretto svolgimento dell'attività amministrativa comunale e, nel caso di specie, non era stata descritta ricorrendo a particolari o dettagli non pertinenti; il generico riferimento ai "motivi di salute" del ricorrente (origine della controversa riduzione della penale, contestata dai consi-

Al di là dell'esito, tale pronuncia merita di essere ricordata per alcuni chiarimenti di carattere generale offerti dal Garante sulle proprie competenze in relazione ai trattamenti svolti dalla magistratura. Come è noto, infatti, gli uffici giudiziari sono tenuti al rispetto di alcune disposizioni della legge n. 675/1996 che riguardano anche la pertinenza e la non eccedenza dei dati trattati; l'Autorità può accertare la rispondenza dei trattamenti ai requisiti di legge, ove necessario verificando l'attuazione da parte del titolare o del responsabile di modificazioni o integrazioni dirette a rendere il trattamento conforme alle disposizioni vigenti (artt. 4, comma 2; 31, comma 1, lett. b), c), p) e 32, commi 6 e 7, l. n. 675/1996).

A questo riguardo, l'Autorità ha chiarito che tale delicata attività di verifica è stata però inserita dal legislatore - e deve essere conseguentemente esercitata - in un quadro di cooperazione e di rispetto delle reciproche attribuzioni che non permette, ad esempio, di invocare dinanzi al Garante un sindacato sull'ampiezza del materiale probatorio acquisito nel corso delle indagini preliminari o di sollevare davanti all'Autorità questioni attinenti alla validità di atti procedimentali, alla loro riforma o all'utilizzabilità nel processo degli elementi di prova, dovendo tali questioni essere invece esaminate nelle sedi processuali utilizzando gli ordinari strumenti di impugnazione.

Segreto professionale dei giornalisti ed esercizio dei diritti ex art. 13

La tutela del segreto professionale dei giornalisti può venire in considerazione anche con riguardo all'esercizio dei diritti previsti dall'art. 13 della legge n. 675/1996. Infatti, come ha avuto modo di ricordare il Garante anche nel corso del 2000, la possibilità accordata ai giornalisti di opporre il segreto sulle fonti di informazione non li esime dal dare riscontro alle richieste degli interessati.

È stato ad esempio sottoposto all'Autorità un caso di pubblicazione su un quotidiano locale di un articolo in cui il giornalista aveva fatto riferimento all'esistenza di una lettera riservata di un cittadino. Questi aveva chiesto di conoscere in che modo il giornalista fosse entrato in possesso della lettera medesima senza ottenere una risposta soddisfacente e, per tale ragione, ha presentato ricorso al Garante. Seppure parzialmente, il ricorso è stato accolto sulla base del presupposto che, anche nel caso dei giornali, l'interessato ha sempre il diritto di ottenere, a cura del titolare del trattamento, senza ritardo ed in maniera adeguata, la comunicazione dell'esistenza e dell'origine dei dati che lo riguardano, salvo dichiarare che la fonte dalla notizia è coperta dal segreto professionale in ragione del carattere fiduciario del rapporto con il soggetto che la ha fornita (comunicato n. 2 del 10 gennaio 2000, in *Bollettino*, n. 11-12, p. 81).

Liceità delle modalità di raccolta dei dati successivamente diffusi con i mezzi di informazione

Uno dei profili più delicati con riferimento alla disciplina della tutela dei dati personali con riguardo ai mezzi di informazione, attiene alle modalità con cui sono raccolte le informazioni successivamente diffuse. In merito, si deve ricordare il ricorso con cui un avvocato aveva richiesto il blocco della diffusione, tramite una videocassetta allegata ad un giornale, della registrazione di un colloquio fra il ricorrente medesimo ed un suo collega che dichiarava essere avvenuta a sua insaputa mediante una telecamera nascosta.

In tale occasione il Garante, dopo aver disposto il blocco della pubblicazione in via cautelare (*Prov. del 20 settembre 2000*), ha successivamente accolto il ricorso e confermato il blocco, giudicando contraria alla disciplina sui dati personali la diffusione di tale videocassetta attraverso i mezzi di informazione (*Prov. del 30 ottobre 2000*).

In proposito, l'Autorità ha innanzitutto ricordato che la registrazione a fini di difesa giudiziaria da parte di una persona impegnata in una conversazione non richiede il necessario consenso del proprio interlocutore (v. anche *Prov. del 12 luglio 2000*). Infatti, anche nelle ipotesi in cui è stato esplicitamente previsto che tale registrazione è illecita in determinati contesti, come nel caso di riunioni tra avvocati, che possono essere registrate solo con il consenso di tutti i presenti (art. 22, par. 3, codice deontologico approvato dal Consiglio nazionale forense il 17 aprile 1997), si deve ritenere che la registrazione non consensuale da parte di uno dei presenti sia consentita quando avviene per una reale esigenza di tutela di un diritto in sede giudiziaria (art. 12, comma 1, lett. h).

Nel caso di specie non è stata dimostrata l'effettiva esigenza di tutela in sede giudiziaria - e, quindi, della liceità della registrazione - a causa dell'insufficienza degli elementi prodotti nel corso del procedimento, rendendosi pertanto necessario rinviare tale aspetto all'esame delle competenti autorità giudiziarie. Tuttavia, si è potuto chiarire che, anche quando la registrazione è effettuata lecitamente per tutelare un diritto in sede giudiziaria, essa può essere utilizzata senza il consenso dell'interessato solo per le medesime finalità, in particolare dandone comunicazione all'autorità competente. Non è pertanto consentito fare uso dei dati in altro modo, avviandoli ad una diffusione indiscrimina-

glieri comunali) non è stato reputato, proprio in ragione della sua genericità, tale da recare lesione alla dignità dell'interessato: in virtù di ciò l'Autorità ha considerato lecita la pubblicazione dell'articolo, dichiarando pertanto infondato il ricorso.

L'applicazione della normativa ai trattamenti svolti in ambito giornalistico, alle fotografie pubblicate dai giornali ed alle riprese televisive

In altre circostanze l'Autorità ha applicato la normativa a trattamenti di dati personali, realizzati nell'ambito della professione giornalistica, sotto forma di fotografie o di immagini diffuse attraverso i mezzi di informazione.

Anche in tali eventualità all'autore delle fotografie (o delle riprese) si applica la previsione dell'art. 25, comma 4, della legge n. 675/1996; quest'ultima disposizione, infatti, estende le norme relative all'esercizio della professione di giornalista ai "trattamenti temporanei finalizzati esclusivamente alla pubblicazione di articoli, saggi o altre manifestazioni del pensiero" e fra queste, possono essere appunto inserite anche le attività dirette a realizzare un servizio fotografico, atteso che anche le fotografie che ritraggono persone sono trattate dalla legge alla stregua di documenti contenenti dati personali (art. 1, comma 2, lett. c), l. n. 675/1996).

Per tale ragione, colui che scatta fotografie, al pari di chi raccoglie notizie, è tenuto a rendere note la propria identità, la propria professione e le finalità della raccolta, senza ricorrere ad "artifici o pressioni indebite" (art. 2 del codice deontologico dei giornalisti).

Al riguardo, con particolare riferimento all'informativa semplificata prevista per i trattamenti svolti nell'ambito dell'attività giornalistica, il Garante ha chiarito che questa trova applicazione anche nelle ipotesi in cui i dati sono raccolti presso un soggetto diverso dall'interessato (*Prov. del 21 febbraio 2000*).

Nel caso di specie, il Garante era stato investito dell'esame di una vicenda che aveva visto la pubblicazione, da parte di un organo di stampa, delle copie di alcune fotografie relative ad un noto personaggio dello spettacolo conservate presso l'abitazione dei genitori di questo. Poiché, dunque, le fotografie ritraevano una persona diversa rispetto a coloro che vivevano nella casa in cui erano conservate, esse non potevano considerarsi raccolte presso l'interessato, con conseguente inoperatività dell'obbligo di informativa ai sensi dell'art. 10, comma 1, della legge n. 675/1996.

La disciplina sulla riservatezza per i personaggi pubblici e le persone note

Analogamente a quanto accade in altri ordinamenti, anche nel nostro la sfera privata delle persone che ricoprono determinate cariche pubbliche o che hanno acquisito una particolare notorietà risulta essere per certi aspetti più ridotta rispetto a quella delle persone la cui vita privata è protetta maggiormente. Tenendo conto di tale principio, il codice deontologico dei giornalisti ha però previsto che la sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se la notizia o di dati non hanno alcun rilievo sul ruolo o sulla loro vita pubblica (art. 6).

Nel corso del 2000 il Garante si è trovato più volte ad applicare tale disposizione, a fronte di reclami presentati da alcuni personaggi pubblici che denunciavano una lesione della propria vita privata. È questo, ad esempio, il caso di un quesito sottoposto all'Autorità da un noto parlamentare che aveva preso parte ad una cerimonia in cui erano presenti altri personaggi pubblici, e che aveva visto il suo nome riprodotto, insieme a quello di altri, in un articolo di giornale che riferiva della cerimonia medesima. In tale occasione, il Garante ha constatato che non vi era stata alcuna violazione delle disposizioni del codice deontologico appena richiamate e che una parte dell'articolo sembrava anzi scaturire da una precisazione fornita direttamente dall'interessato.

Più in generale, l'Autorità ha ricordato che, con riguardo al principio dell'essenzialità dell'informazione, può considerarsi lecita anche un'informazione molto dettagliata, qualora ricorrano determinati presupposti, tra i quali rileva la qualificazione dei protagonisti come personaggi pubblici (*Prov. del 21 febbraio 2000* e, per un caso analogo, *Prov. del 20 ottobre 2000*).

Fatti resi noti direttamente dagli interessati o attraverso i loro comportamenti in pubblico

Con riguardo alla diffusione operata dai mezzi di informazione, nell'ipotesi in cui gli stessi interessati abbiano in qualche modo reso pubbliche le notizie che li riguardano, viene precluso in alcuni casi un intervento dell'Autorità diretto a ridurre la diffusione delle informazioni medesime (v., in proposito, il comunicato n. 5 del 17 gennaio 2000, in *Bollettino* n. 11-12, p. 83).

La legge n. 675/1996, mentre ha previsto in generale che i giornalisti devono rispettare i limiti del diritto di cronaca, con particolare riferimento a quello dell'essenzialità dell'informazione riguardo a fatti di interesse generale, ha lasciato ferma la possibilità di trattare i dati relativi a circostanze e fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico (art. 25, comma 1). Tale ipotesi ha trovato anche riscontro nel codice di deontologia dei giornalisti che ha fatto salvo il diritto di addurre successivamente motivi legittimi di tutela, ma non ha ribadito il limite dell'essenzialità dell'informazione, richiamato invece con particolare pregnanza per quanto attiene ai dati sensibili (art. 5 del codice di deontologia).

A questo riguardo, si può ricordare un ricorso riguardante le dichiarazioni fatte dal padre naturale di un minore durante alcuni programmi televisivi. Chiarito che in tale ipotesi non sarebbe stato in ogni caso applicabile l'art. 3 della legge n. 675/1996 (in tema di trattamento di dati per fini esclusivamente personali), l'Autorità ha constatato che la vicenda alla quale era stata fatta menzione durante la trasmissione era notoria, in quanto già oggetto di cronaca giornalistica, anche a seguito di dichiarazioni dei relativi protagonisti (v. *Provv.* del 28 febbraio 2000). Di qui l'impossibilità di accogliere la richiesta di opposizione al trattamento formulata dalla ricorrente (in quanto trovava applicazione il già citato art. 5, comma 2, del codice deontologico), che lascia però impregiudicata l'esigenza che giornalisti e conduttori delle trasmissioni televisive operino in modo da evitare o ridurre il rischio di trattare i dati riferiti ai minori in modo da non incidere sul corretto sviluppo della personalità degli stessi (cioè, in particolare, con riferimento all'art. 7 del codice dei giornalisti, sul quale si tornerà fra breve).

Un altro caso che merita di essere menzionato è quello in cui il Garante è stato chiamato a decidere sul ricorso presentato da una madre nei confronti di una televisione a diffusione nazionale, in relazione ad un servizio relativo al rimpatrio in Italia della propria figlia minore a seguito della decisione di una Corte distrettuale statunitense. Anche in tale frangente l'Autorità ha dichiarato infondato il ricorso in quanto, sebbene le fotografie riprodotte nel filmato trasmesso riguardassero un minore, erano state mostrate da uno dei genitori, per di più in un contesto di sentita prospezione di una complessa vicenda familiare che aveva destato in più occasioni il pubblico interesse (*Provv.* del 23 novembre 2000).

Pubblicazione a mezzo stampa dei provvedimenti disciplinari assunti dagli ordini professionali

Come il Garante ha avuto modo di chiarire altre volte, non sempre l'applicazione della normativa sulla tutela dei dati personali porta ad una minore conoscibilità delle informazioni. In alcune circostanze, infatti, quando devono essere tutelati altri diritti e valori, la disciplina sulla riservatezza può farsi veicolo di una maggiore trasparenza. E ciò può riguardare anche trattamenti particolarmente delicati per la protezione dei dati, quali la diffusione attraverso i mezzi di informazione.

Al riguardo, si può ricordare il caso in cui l'Autorità è stata chiamata a decidere sul ricorso presentato da un avvocato per lamentare l'avvenuta pubblicazione - su una rivista dell'ordine di appartenenza - del provvedimento di sospensione dalla professione adottato nei suoi confronti. In tale occasione, il Garante ha avuto modo di ribadire che la legge n. 675/1996 non ha modificato la disciplina legislativa relativa al regime di pubblicità degli albi professionali ed alla conoscibilità degli atti connessi. Per tale ragione, deve ancora ritenersi che tali albi siano destinati per loro natura e funzione ad un regime di piena pubblicità, anche della tutela dei diritti di coloro che a vario titolo hanno rapporti con gli iscritti agli albi (*Provv.* del 29 marzo 2001).

Molte delle disposizioni che regolano tale forma di pubblicità sono spesso risalenti nel tempo e necessitano pertanto di essere aggiornate anche al fine di individuare in modo più preciso le diverse forme di diffusione consentite, secondo la logica sottesa alla legislazione in materia di riservatezza (art. 27, comma 3, l. n. 675/1996). Ciò, tuttavia, non fa venir meno la qualificazione degli albi professionali come atti pubblici non solamente conoscibili da chiunque, ma anche oggetto di doverosa pubblicità.

Più specificamente, il Garante ha chiarito che la *ratio* sottesa alla pubblicità degli albi e dei periodici aggiornamenti relativi a nuove iscrizioni e cancellazioni ricorre anche per i provvedimenti che comportano la sospensione o l'interruzione dell'esercizio della professione. Sebbene l'ordinamento preveda al riguardo specifiche forme di pubblicità (es. comunicazione a tutti i consigli dell'ordine degli avvocati ed alle autorità giudiziarie del distretto al quale il professionista appartiene: art. 46, commi 1 e 3, r.d.l. n. 1578/1933), è chiaro che le stesse consentono a chiunque di venire lecitamente a conoscenza di determinati provvedimenti e di darne legittimamente ulteriore notizia.

Il Garante ha potuto così affermare che i provvedimenti disciplinari dei consigli dell'ordine e del Consiglio nazionale forense devono essere considerati quali atti pubblici soggetti ad un regime di conoscibilità. Ciò, pur in assenza di disposizioni più analitiche di legge o di regolamento in cui siano previste particolari modalità di diffusione a favore di determinati soggetti, ulteriori rispetto a quelli specificamente indicati come destinatari dalle norme vigenti.

L'interesse alla riservatezza del professionista destinatario di una misura disciplinare non può ritenersi quindi prevalente rispetto all'interesse generale alla conoscenza del provvedimento medesimo ed è pertanto lecita la divulgazione della notizia del provvedimento stesso attraverso riviste, notiziari o altre pubblicazioni curate anche dagli ordini interessati. Ciò, ovviamente, nel presupposto che la diffusione del provvedimento avvenga in modo corretto ed in termini esatti e completi, secondo quanto disposto dall'art. 9 della legge n. 675/1996.

Pubblicazione a mezzo stampa dei dati relativi ai redditi dichiarati

Nel corso del 2000 (nonché nei primi mesi del 2001), il Garante è stato chiamato ad occuparsi della diffusione, ad opera dell'Amministrazione finanziaria, dei dati relativi al reddito delle persone fisiche anche con riguardo alla loro pubblicazione da parte degli organi di informazione. Tale tema è stato già affrontato dall'Autorità in diverse occasioni, chiarendo che la disciplina vigente prevede espressamente la pubblicazione di determinati elenchi di taluni contribuenti e del relativo reddito. La stessa normativa dispone inoltre la formazione, da parte di ciascun comune, degli elenchi nominativi di tutti i contribuenti che hanno presentato la dichiarazione dei redditi o che esercitano imprese commerciali, arti e professioni (v. *par. 13* della presente Relazione), elenchi, questi, che devono essere depositati per un anno presso gli uffici delle imposte e i comuni interessati ai fini della consultazione da parte di chiunque (art. 69 d.P.R. n. 600/1973 come successivamente modificato in particolare dall'art. 19 l. n. 413/1991).

L'esistenza di siffatte disposizioni - espressione di una scelta normativa volta ad un'ampia conoscibilità di determinati dati - integra gli estremi richiesti dall'art. 27, comma 3, della legge n. 675/1996 e rende quindi allo stato lecita, salve eventuali modifiche normative, la comunicazione degli elenchi da parte dell'amministrazione finanziaria, anche dal punto di vista della normativa in materia di riservatezza (v. lettera del 13 ottobre 2000, in *Bollettino*, n. 14-15, p. 9).

Sulla base di tali presupposti, l'Autorità ha pertanto dichiarato infondato un ricorso presentato da un imprenditore che aveva chiesto il blocco dei dati relativi al proprio reddito diffusi da un quotidiano locale sulla base di quanto pubblicato dall'amministrazione finanziaria (*Prov. 17* gennaio 2001, in *Bollettino* n. 16, p. 5). Il Garante ha infatti affermato che, essendo le informazioni rese accessibili dall'amministrazione finanziaria destinate ad un'ampia pubblicità, la successiva pubblicazione di dati estratti lecitamente da elenchi accessibili a chiunque è da ritenersi lecita anche senza il consenso degli interessati e senza che sia necessario per la testata che li riproduce dimostrare la sussistenza del requisito dell'essentialità dell'informazione rispetto a fatti di interesse pubblico (art. 20, comma 1, lett. d), l. n. 675/1996).

Decisioni di carattere procedurale e limiti alle competenze del Garante

Non di rado il Garante è stato investito di istanze di tutela che eccedevano le proprie specifiche competenze: si pensi alle ipotesi in cui il suo intervento è stato invocato in relazione alla diffusione di informazioni denigratorie o diffamatorie, oppure al fine di ottenere dall'Autorità il risarcimento di un danno subito in ragione della diffusione di dati personali attraverso i mezzi di informazione (si veda, per tutti, il *Prov. 20* ottobre 2000).

In questi casi l'Autorità ha chiarito ancora una volta l'ambito delle proprie competenze e della tutela amministrativa accordata in relazione al trattamento dei dati personali, ricordando comunque la possibilità di far valere i propri diritti di fronte ad altre autorità (nella specie il giudice ordinario).

In altre circostanze, sono giunte all'Autorità richieste di provvedimenti (ad esempio di blocco della diffusione di talune informazioni) che non potevano essere emanati a causa della mancanza di presupposti procedurali a tal fine necessari (si possono vedere, per tutti, i *Prov. adottati* il 5, il 22 aprile e il 21 settembre 2000; nel terzo di questi casi, l'interessato lamentava di essere stato ripreso durante una trasmissione televisiva a sua insaputa; un altro ricorso è stato dichiarato inammissibile il 30 ottobre 2000, relativamente ad un'intervista dell'ex moglie del ricorrente, mandata in onda durante una nota trasmissione televisiva, nella quale l'intervistata faceva menzione di fatti e circostanze tali da permettere l'identificazione del ricorrente stesso e di suo figlio). Altre volte, invece, sono risultati insufficienti gli elementi di valutazione forniti (*Prov. 21* febbraio 2000).

In molte di tali ipotesi il Garante, oltre ad indicare le procedure di volta in volta necessarie per ottenere il provvedimento richiesto, ha cercato, ove le circostanze lo consentivano e la questione sottoposta lo richiedeva, di offrire comunque una tutela agli interessati, ad esempio considerando anche alla stregua di segnalazioni i ricorsi proposti in maniera non conforme all'art. 29 della legge e al d.P.R. n. 501/1998.

In ogni caso, quando ciò era possibile, il Garante ha sempre tenuto a chiarire che il pronunciamento dell'Autorità, magari riferito ad un particolare aspetto della vicenda, non precludeva a coloro che avessero avuto interesse di instaurare, anche dinanzi alla competente autorità giudiziaria, specifiche controversie dirette ad ottenere giudizi di cui il Garante non poteva farsi carico anche a causa dell'insufficienza degli elementi di valutazione sottoposti al suo vaglio (si veda, per tutti, il *Prov. del 21 febbraio 2000*).

In alcuni casi, infine, l'Autorità ha avviato autonomamente procedimenti distinti da quello aperto su istanza degli interessati, al fine di accertare il rispetto della normativa sulla riservatezza con riguardo a profili in parte diversi da quelli segnalati o che comunque richiedevano di essere autonomamente valutati (si veda, per tutti, la decisione adottata il 27 agosto 2000 su un ricorso presentato dai genitori di una minore, in relazione ad alcuni articoli dedicati ad un procedimento giudiziario, pubblicati da un quotidiano locale).

47. LA TUTELA DEI MINORI

I minori restano tra i soggetti più esposti e indifesi rispetto al rischio di lesione dei propri diritti fondamentali (ed in particolare del diritto alla riservatezza) da parte dei mezzi di informazione.

Indebite ingerenze nella vita privata dei minori possono comportare danni irreparabili nella relativa vita di relazione e nello sviluppo della personalità, derivanti a volte dalla tendenza a spettacolarizzare vicende che meriterebbero invece maggiori cautele da parte dei *media*. Per tale ragione, anche nel corso del 2000 il Garante si è visto più volte obbligato a richiamare al rispetto dei precisi limiti alla diffusione dei dati personali sui minori (si veda, in particolare, il *Prov. del 22 aprile 2000*).

Come è noto, infatti, al fine di tutelarne la personalità, i giornalisti non devono pubblicare i nomi dei minori coinvolti in fatti di cronaca, né fornire particolari in grado di condurre alla loro identificazione. Questo, nella consapevolezza che la tutela della personalità del minore si estende anche ai fatti che non sono specificamente reati, tenuto conto della qualità della notizia e delle sue componenti. Inoltre, per espressa previsione normativa, il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca. Quando, tuttavia, per motivi di rilevante interesse pubblico e fermi restando i limiti di legge, il giornalista decide di diffondere notizie o immagini riguardanti minori, deve farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi ed i limiti stabiliti anche dalla cosiddetta "Carta di Treviso" (art. 7 del codice di deontologia sul trattamento dei dati personali nell'esercizio dell'attività giornalistica).

In applicazione di questi principi, l'Autorità ha disposto il blocco dei dati relativi alle molestie subite da una minore ad opera dei suoi rapitori nei confronti di una serie di testate giornalistiche (*Prov. del 20 giugno 2000*). Alcuni organi di stampa a diffusione nazionale avevano reso note, nei titoli e nel corpo degli articoli, talune circostanze relative alle molestie sessuali che apparivano perpetrate dai rapitori di una minore. Il Garante ha disposto il blocco muovendo dalla considerazione che la possibile ed ulteriore divulgazione dei dati relativi alle molestie, a prescindere dalla loro eventuale rilevanza sotto il profilo penale (profilo per il quale è stata investita la competente autorità giudiziaria in relazione all'art. 734-bis c.p.), avrebbe comportato il concreto rischio di un pregiudizio rilevante per l'interessata. Un provvedimento, dunque, da cui derivava per gli editori titolari del trattamento e per i responsabili del medesimo, un preciso obbligo di sospendere ogni ulteriore operazione di trattamento diversa dalla mera conservazione delle informazioni già raccolte e, in particolare, di astenersi dal diffondere ulteriormente i medesimi dati anche in modo indiretto, attraverso la pubblicazione delle corrispondenti parti dello stesso provvedimento del Garante.

In questo contesto merita di essere infine ricordata anche una decisione assunta dall'Autorità nell'agosto 2000, con riguardo all'avvenuta pubblicazione su taluni organi di informazione di liste di soggetti responsabili di gravi atti di violenza a danno di minori. In merito a tali vicende, il Garante era intervenuto con un comunicato stampa per ricordare che la diffusione indiscriminata di informazioni non trova fondamento nel nostro ordinamento. Tali notizie, infatti, a prescindere dalla loro reale efficacia sul piano della prevenzione e dalla circostanza che i dati possano essere desunti anche da fonti accessibili (quali, ad es. pronunce giudiziarie), sono suscettibili di valutazione critica e fonte di contenzioso potendo anche, a seconda dei casi, oltre che determinare danni agli stessi minori indirettamente identificabili, comportare responsabilità per eventuali inesattezze dei dati, oppure per giudizi indifferenziati su situazioni in realtà difformi o per la lesione del diritto all'oblio di persone interessate rispetto a fatti talvolta assai risalenti nel tempo (comunicato stampa del 23 agosto 2000).

SORVEGLIANZA E SISTEMI BIOMETRICI

48. VIDEOSORVEGLIANZA

Il tema della videosorveglianza è stato nello scorso anno tra quelli con riferimento ai quali il Garante ha profuso un particolare impegno, sia per la diffusione del fenomeno, sia in ragione della particolare sensibilità manifestata al riguardo da parte di numerosi cittadini.

In attesa di una specifica normativa che disciplini l'utilizzo dei sistemi di videosorveglianza, le regole previste in via generale dalla disciplina sul trattamento dei dati personali risultano (anche sulla scorta delle indicazioni comunitarie contenute nella direttiva n. 95/46/CE) già applicabili alle immagini ed ai suoni, nel caso in cui le apparecchiature che li rilevano permettano di identificare, in modo diretto o indiretto, un determinato soggetto.

In questo quadro, anche in uno spirito di collaborazione che molte amministrazioni hanno sino ad oggi dimostrato, taluni enti locali hanno ritenuto di interpellare preventivamente il Garante con riferimento ad iniziative di controllo del territorio da realizzare attraverso l'impiego di dispositivi elettronici.

In particolare, il Comune di Mantova ha sottoposto al Garante un progetto di installazione di un sistema di tele-sorveglianza in alcune zone della città, basato su dodici telecamere, in parte destinate ad effettuare rilevazioni a fini statistici e di studio degli accessi dei veicoli al centro storico e nelle zone a traffico limitato, in parte utilizzate per finalità di controllo a distanza "con funzioni di prevenzione e repressione di attività illecite".

Nella specie, il Garante, con provvedimento del 7 marzo 2000, ha fatto presente che per gli aspetti concernenti l'installazione e l'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, occorreva tener conto della nuova disciplina introdotta dal d.P.R. n. 250/1999, il quale prevede, tra l'altro, per i comuni interessati, l'obbligo di munirsi di un'autorizzazione rilasciata dal Ministero dei lavori pubblici, nonché il vincolo di utilizzazione degli impianti per raccogliere dati riguardanti il luogo, il tempo e l'identificazione dei veicoli che accedono al centro storico o nelle zone a traffico limitato, rilevando immagini solamente in caso di infrazione. Alla luce di ciò, il Garante ha chiesto di rivedere l'impostazione del progetto, nella parte in cui ipotizzava una rilevazione sistematica di tutte le targhe dei veicoli transitati, con la previsione di una verifica a posteriori al fine di redigere una lista dei soggetti "sanzionabili" e una rilevazione anonima prevista solo in una fase successiva, per fini statistici e di studio.

La vicenda ha offerto l'occasione all'Autorità per ribadire che la legge n. 675/1996 è applicabile anche ai trattamenti di immagini effettuati attraverso i sistemi di videosorveglianza, a prescindere dalla circostanza che le informazioni siano registrate in un archivio elettronico o eventualmente comunicate a terzi dopo la loro temporanea raccolta e conservazione attraverso circuiti di controllo.

Benché sia vero che le registrazioni effettuate mediante l'uso di telecamere non contengono sempre e necessariamente dati di carattere personale, in quanto la distanza, l'ampiezza dell'angolo visuale e la qualità degli strumenti possono rendere non identificabili le persone inquadrare, la c.d. legge sulla *privacy* considera "dato personale" qualunque informazione relativa a persone anche non identificate, ma identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione. Sicché, ai fini dell'applicazione della legge n. 675/1996, non è necessario che le persone vengano identificate in maniera chiara ed univoca, essendo al contrario sufficiente che i soggetti risultino identificabili attraverso, ad esempio, il collegamento con altre fonti conoscitive, quali foto segnaletiche, *identikit* o archivi di polizia contenenti immagini.

L'Autorità ha quindi invitato il Comune di Mantova a compiere un'attenta verifica, in riferimento alle finalità indicate nel progetto (in particolare con riguardo a quelle di "prevenzione e repressione di attività illecite criminali"), al fine di accertare quali di esse rientrassero effettivamente tra le funzioni istituzionali demandate all'ente stesso, alla luce dell'ordinamento degli enti locali all'epoca dei fatti vigenti, dell'ordinamento della polizia municipale, nonché dagli statuti e dai regolamenti comunali (v. art. 27, comma 1, l. n. 675/1996), sollecitando altresì l'ente locale ad individuare misure di sicurezza idonee ad assicurare un uso corretto dei dati da parte dei soggetti legittimati (art. 15, l. n. 675/1996 e d.P.R. n. 318/1999), nonché di modalità volte a fornire agli interessati, in modo efficace, l'informativa prevista dall'art. 10 della legge n. 675/1996.

In relazione alla prevista installazione degli impianti di tele-sorveglianza nel Comune di Mantova, il Garante ha in conclusione segnalato la necessità di apportare talune modifiche al progetto, al fine di renderlo conforme a quanto rilevato in sede di esame preventivo, evidenziando in particolare:

a) la necessità di introdurre una limitazione delle modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine), anche al fine di assicurare il rispetto 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;

b) la necessità di istituire una correlazione tra liceità e pertinenza della raccolta di informazioni e il previsto livello elevato di precisione e di dettaglio della ripresa dei tratti somatici delle persone (si parlava infatti di *"zoom e/o brandeggio motorizzato, con la conseguente possibilità di gestire al meglio l'inquadratura"*), nonché di tener conto dei precisi limiti posti all'installazione di impianti audiovisivi dall'art. 4 della legge n. 300/1970 (c.d. Statuto dei lavoratori), evitando altresì la ripresa sistematica di luoghi privati;

c) la necessità di individuare i soggetti legittimati all'accesso, alla custodia ed all'utilizzazione alle registrazioni anche all'interno dell'ente, escludendo persone diverse dai responsabili e dagli incaricati;

d) la necessità di precisare 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.

Diversamente dal Comune di Mantova, che si era limitato a predisporre un progetto (sul quale ci si è soffermati in questa sede anche perché presenta profili poi risultati comuni ad altre iniziative), quello di Portici ha trasmesso al Garante la delibera della Giunta comunale con la quale era stato approvato uno schema di regolamento per l'installazione e l'utilizzo di impianti di videosorveglianza del territorio, di telecontrollo ambientale e di pannelli a messaggi variabili.

Dall'esame di tale provvedimento è emerso che con tali impianti il Comune intendeva monitorare le zone nevralgiche del traffico cittadino ed i punti di maggiore concentrazione abitativa, per una pluralità di finalità, tra le quali: a) dotarsi di uno strumento attivo di protezione civile; b) identificare, in tempo reale, luoghi e ragioni di ingorghi per consentire, fra l'altro, il pronto intervento della polizia municipale; c) rilevare infrazioni al codice della strada; d) rilevare situazioni di pericolo per la sicurezza pubblica, consentendo l'intervento degli operatori. Anche in tal caso, l'Autorità, con provvedimento del 17 febbraio 2000, ha segnalato la necessità di apportare talune modificazioni allo schema di regolamento, al fine di renderlo armonico con le previsioni della legge n. 675/1996.

Queste vicende, che hanno offerto un'ulteriore attestazione dell'interesse sviluppatosi attorno al tema della videosorveglianza, hanno stimolato altresì una valutazione istituzionale delle dimensioni e delle caratteristiche del fenomeno, basata anche sull'ausilio di esperti esterni. È stata curata, così, un'importante esperienza di ricerca "sul campo", condotta con la collaborazione della società Ipermedia. La ricerca, condotta tra il 20 marzo e il 20 maggio 2000, ha avuto lo scopo di fornire una valutazione preliminare circa la presenza dei sistemi di videosorveglianza visibile esterna nei luoghi pubblici di alcune città italiane: Milano, Verona, Roma, Napoli. Più specificatamente, si è trattato di uno studio pilota volto a fornire, attraverso i dati raccolti, alcune indicazioni sulla presenza di tali strumenti nel nostro Paese e porre, quindi, le basi per un eventuale studio di più ampio respiro, destinato alla misurazione esaustiva del fenomeno ed alla valutazione del suo "impatto ambientale".

Il campo d'indagine è stato individuato nelle zone centrali e semicentrali di Milano, Roma, Napoli e Verona.

Data la dimensione esplorativa della ricerca, nell'ambito di ciascuna città si è optato per un campionamento a scelta ragionata: sono stati selezionati alcuni itinerari, assunti in qualità di casi-campione, con riferimento al centro commerciale, storico, politico (nel caso di Roma) e residenziale di ciascun ambito cittadino, all'interno dei quali è stato rilevato il numero di videocamere presenti, poi assunte ad unità di analisi. Sono state oggetto d'indagine tutte le videocamere esterne e visibili che riprendevano le strade e le piazze campionate, sicché la ricerca tiene conto anche dei casi di videocamere interne a recinzioni, ma rivolte verso l'esterno, o presenti nelle strade adiacenti a quelle percorse, ma rivolte verso queste ultime.

L'obiettivo principale della ricerca, consistente nel fornire una valutazione preliminare circa la presenza dei sistemi di controllo video visibili ed esterni nelle quattro città italiane indicate, scontava evidentemente la carenza, creatasi per effetto dell'interazione negativa di molti fattori, di uno dei presupposti necessari all'identificazione dell'universo di riferimento: la possibilità di delimitare le unità che lo compongono. In concreto, ci si è trovati di fronte ad un universo "sconosciuto", non essendo note, oltre

al numero delle unità che lo costituiscono, anche la loro localizzazione e le loro caratteristiche. Ciò nonostante, i campioni relativi alle quattro città oggetto di rilevazione possono considerarsi sufficientemente validi (considerando anche la dimensione esplorativa della ricerca) per fornire dati utili ad elaborare (ancorché su un piano certamente non scientifico, ma congetturale) una prima stima riguardo alla diffusione di tali sistemi.

I dati sono stati raccolti tramite una scheda di rilevazione composta da otto variabili relative alla città, zona, ubicazione, collocazione, identificabilità, posizione, visibilità e tipologia della videocamera. Per mezzo di essa è stato possibile raccogliere informazioni non solo sull'affollamento, ma anche sul grado di percettibilità degli strumenti di videosorveglianza, specie attraverso l'analisi della posizione e della visibilità degli apparecchi.

Le videocamere individuate sono complessivamente 1095: 726 a Roma, 213 a Milano, 89 a Napoli e 67 a Verona. Considerando il carattere campionario dell'indagine, questi numeri consentono di stimare, a livello di attendibile proiezione statistica, la presenza in Italia di circa un milione di impianti di videosorveglianza.

Non si sono peraltro evidenziate significative differenze tra le quattro città (pur trattandosi di tre grandi capoluoghi e una città di minori proporzioni). In ciascun ambito cittadino, invero, i sistemi di videosorveglianza risultano collocati principalmente a vigilanza di sportelli bancari, sono posti ad altezza portone, facilmente individuabili e di grandi dimensioni. Inoltre, fatta eccezione per Milano, dove le telecamere sono equamente distribuite tra zone centrali e semicentrali, si è riscontrata una maggiore concentrazione di meccanismi di controllo video nelle aree poste al centro delle città.

I risultati della ricerca sono stati presentati ai rappresentanti delle istituzioni e alla stampa in occasione di un apposito incontro promosso dal Garante presso la Camera dei deputati nel luglio 2000, che ha visto la partecipazione anche di rappresentanti di governo, di gruppi parlamentari, del mondo accademico e della cultura.

L'iniziativa ha avuto risalto sulla stampa quotidiana, periodica e radiotelevisiva che, sull'esempio dell'Autorità, ha promosso specifiche ricerche a campione sottoposte all'attenzione dell'opinione pubblica, che hanno altresì riscosso l'interesse delle istituzioni.

Ad essa hanno fatto seguito da un lato alcuni progetti di legge coerenti con l'impostazione data dal Garante; dall'altro, talune linee-guida che, su richiesta del Consiglio d'Europa, sono state predisposte dal segretario generale del Garante unitamente ad un rapporto, che il Consiglio stesso si accinge ad approvare definitivamente (v. www.coe.fr).

Anche in considerazione dei riscontri ottenuti, e per venire incontro alla forte domanda di informazione sul tema, il Garante ha quindi provveduto a stilare una sorta di "decalogo" valevole per tutti coloro che intendono installare impianti stabili (o comunque non occasionali), cioè sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini, in particolare a fini di sicurezza, di tutela del patrimonio, di controllo di determinate aree e di monitoraggio del traffico o degli accessi di veicoli nei centri storici. In sintesi, fermo restando innanzitutto il principio di proporzionalità tra mezzi impiegati e fini perseguiti, anche per evitare l'applicazione delle sanzioni previste dalle norme vigenti, sono state indicate ai titolari del trattamento le seguenti cautele:

a) occorre chiarire gli scopi che si intendono perseguire e verificare se sono leciti in base alle norme vigenti. Se l'attività è svolta, ad esempio, per prevenire pericoli concreti o specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche;

b) il trattamento dei dati deve avvenire per scopi determinati, espliciti e legittimi;

c) i titolari del trattamento tenuti a notificare al Garante l'esistenza di trattamenti devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza;

d) i cittadini devono essere informati, in maniera chiara anche se sintetica, della presenza di telecamere e dei diritti che possono esercitare sui propri dati, tanto più se le apparecchiature non sono immediatamente visibili;

e) per il controllo a distanza dei lavoratori rimangono comunque validi i divieti e le garanzie previsti dallo Statuto dei lavoratori;

f) i dati raccolti devono essere quelli strettamente necessari agli scopi perseguiti: vanno pertanto registrate solo le immagini indispensabili, va limitato l'angolo visuale delle riprese, vanno evitate immagini

dettagliate o ingrandite e, di conseguenza, vanno stabilite in maniera adeguata la localizzazione delle telecamere e le modalità di ripresa;

g) va stabilito con precisione entro quanto tempo le immagini devono essere cancellate e occorre prevedere la loro conservazione solo in relazione ad illeciti che si siano verificati o a indagini giudiziarie o di polizia;

h) vanno individuate, con designazione scritta, le persone che possono utilizzare gli impianti e prendere visione delle registrazioni; deve essere vietato l'accesso alle immagini ad altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia;

i) i dati raccolti per determinati fini (ad esempio sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio per pubblicità o analisi dei comportamenti di consumo), fatte salve le esigenze di polizia o di giustizia e non possono essere diffusi o comunicati a terzi;

l) le immagini registrate per la rilevazione degli accessi dei veicoli ai centri storici devono rispettare l'apposito regolamento (d.P.R. 250/1999) ed essere conservate per il solo periodo necessario alla contestazione delle infrazioni.

Nel caso, invece, di impianti di videosorveglianza finalizzati esclusivamente alla sicurezza individuale (si pensi, ad esempio, al controllo dell'accesso alla propria abitazione), questi, ove perseguano effettivamente solo tale scopo, non rientrano nell'ambito di applicazione della legge sulla riservatezza, essendo il trattamento effettuato a fini personali. Le persone che possono divenire oggetto di indebiti controlli possono comunque tutelare i propri diritti dinanzi all'autorità giudiziaria. Anche in queste ipotesi vanno quindi rispettati alcuni obblighi: le riprese devono essere limitate al solo spazio antistante tali accessi, evitando forme di videosorveglianza su aree circostanti che potrebbero limitare la libertà altrui; le informazioni raccolte, inoltre, non devono essere comunicate o diffuse ad altri.

49. IMPRONTE DIGITALI E RILEVAZIONI BIOMETRICHE

Attraverso l'analisi delle caratteristiche biometriche (geometria del volto, della mano, dell'iride, etc.), è possibile, a distanza, acconsentire all'esecuzione di operazioni o confrontare le informazioni rilevate con quelle memorizzate in apposite banche di dati, al fine di attivare gli opportuni rimedi.

La questione tocca anche il tema della sicurezza di operazioni e transazioni e della sicurezza in determinati ambienti, avvertito soprattutto da talune categorie di aziende, in ragione della particolare natura dell'attività da esse svolta.

Anche per questi motivi l'introduzione di sistemi di lettura e/o raccolta di impronte digitali (che di regola operano contestualmente ad altre apparecchiature di rilevazione di informazioni personali, specie in forma di controllo video) è fenomeno che ha interessato, sino ad oggi, soprattutto gli istituti di credito.

Nel corso del 2000, anche su segnalazione dell'utenza (il cui grado di attenzione si dimostra crescente di fronte al diffondersi dell'uso di tecnologie sofisticate), il Garante si è occupato del problema in alcune occasioni (provvedimenti dell'11 dicembre 2000, del 7 marzo 2001 e del 28 febbraio 2001). In relazione alle modalità con le quali si sono sviluppate le prime esperienze applicative, sono emersi anzitutto tre profili:

a) un problema di rispetto del principio di proporzionalità sancito dall'art. 9 della legge n. 675/1996, tra almeno uno dei sistemi in concreto impiegati (quello di rilevazione delle impronte digitali, a volte associate ad immagini) e le finalità perseguite, essendo apparse esorbitanti, nei pochi casi esaminati, le intraprese attività indifferenziate di raccolta di dati significativi - quali le impronte associate alle immagini - imposte a tutti coloro che entrano nella banca, ivi compresi i soggetti diversi dai clienti in senso proprio, di per sé non legittimate da generiche esigenze di sicurezza non accompagnate da elementi che evidenzino una concreta situazione di rischio;

b) la tendenziale insufficienza, quando non addirittura la carenza, dell'informativa prescritta dall'art. 10 della legge n. 675/1996, tanto più vistosa se si considera la particolare natura delle informazioni personali che vengono raccolte, anche grazie a recenti acquisizioni scientifiche che in linea astratta potreb-

bero consentire di ricavare elementi conoscitivi di sicura "sensibilità" relativamente alla persona cui i dati si riferiscono. Le informative sono risultate inidonee ad avvertire gli interessati della presenza di dispositivi elettronici di rilevazione dell'impronta e dell'immagine dei clienti, come della loro eventuale associazione (effettuata contemporaneamente o successivamente all'ingresso nei locali della banca), nonché carenti delle indicazioni concernenti l'esercizio dei diritti di cui all'art. 13 della legge n. 675/1996;

c) il complessivo profilo relativo alle modalità di rilevazione e all'eventuale classificazione dei dati, al tempo di conservazione, alle misure di sicurezza, all'accesso da parte del personale interno e/o del personale di polizia.

In considerazione di ciò, il Garante ha vietato con alcuni primi provvedimenti, con effetto immediato, l'ulteriore utilizzazione dei dispositivi di rilevazione delle impronte digitali utilizzati dagli istituti di credito interessati dalle verifiche dell'Autorità, determinandone la disattivazione. Altre disattivazioni sono state comunicate da taluni istituti richiesti di fornire elementi di valutazione.

Resta da completare l'esame del delicato problema dell'individuazione di un ragionevole punto di equilibrio che salvaguardi - segnatamente dal punto di vista delle modalità da seguire in concreto - anche le istanze di sicurezza rappresentate in casi particolari da alcuni soggetti.

Il Garante ha pertanto ripreso di recente la valutazione complessiva del problema e si riserva di formulare a breve alcune ulteriori indicazioni a completamento, sviluppo ed arricchimento di quanto già affermato in precedenza.

50. BRACCIALETTO ELETTRONICO

Particolare interesse ha destato, in un momento che ha fatto registrare un picco di crescita della domanda di sicurezza da parte dei cittadini, la controversa introduzione di forme di controllo a distanza - che comportano una massiccia attività di raccolta e trattamento di dati personali - di soggetti sottoposti alla misura cautelare degli arresti domiciliari o alla detenzione domiciliare, in attuazione di quanto disposto a seguito delle modifiche al c.p.p. e all'ordinamento penitenziario operate con d.l. 24 gennaio 2000, n. 341, emanate al dichiarato scopo di decongestionare l'apparato di vigilanza, alle prese con l'esigenza di dislocare ad altri servizi di controllo del territorio risorse umane impegnate nella sorveglianza a domicilio.

Le nuove disposizioni sono state rese operative con il già menzionato (v. par. 2) d.m. 2 febbraio 2001, adottato dal Ministro dell'interno di concerto con il Ministro della giustizia e pubblicato sulla *G.U.* del 15 febbraio 2001, recante "modalità di installazione ed uso e descrizione dei tipi e delle caratteristiche dei mezzi elettronici e degli altri strumenti tecnici destinati al controllo delle persone sottoposte alla misura cautelare degli arresti domiciliari nei casi previsti dall'art. 275-bis del codice di procedura penale e dei condannati nel caso previsto dall'art. 47-ter, comma 4-bis, l. 26 luglio 1975, n. 354".

Il decreto rappresenta un'importante testimonianza del positivo rapporto di collaborazione instauratosi tra il Garante ed altri soggetti istituzionali, che nella specie non si sono limitati a dare formale attuazione all'art. 31, comma 2, della legge n. 675/1996 (ove è stabilito che "il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla presente legge"), ma hanno recepito diverse indicazioni formulate dall'Autorità. Indicazioni ispirate alla necessità di contemperare le perseguite necessità di controllo con l'esigenza di evitare forme di vigilanza inutilmente oppressive, in particolare per quanto concerne il rispetto dei principi sanciti nell'art. 9 della legge n. 675/1996, con specifico riguardo alle modalità di raccolta e trattamento, alle finalità e alla durata della conservazione dei dati raccolti, nonché agli aspetti attinenti alla sicurezza delle informazioni personali, ai sensi dell'art. 15 della medesima legge e del d.P.R. n. 318/1999.

MARKETING

51. INFORMATIVA E SPECIFICITÀ DEL CONSENSO

L'innovazione introdotta dall'erompere delle tecnologie dell'informazione e della comunicazione, determinando tempi e modalità di trattamento delle informazioni una volta impensabili, ha coinvolto ormai la società nella sua interezza, con rilevanti implicazioni in relazione allo svolgimento delle attività economiche in generale e del *marketing* in particolare. Per esso, a ben vedere, si sono schiuse nuove prospettive; non solo, infatti, è ormai agevole l'elaborazione di volumi di dati personali prima difficilmente gestibili (se non a costi elevati), ma è altresì possibile rendere destinatari di flussi informativi non più una generalità indistinta di potenziali acquirenti, quanto *target* sempre più mirati di potenziale clientela, sino a giungere a forme di comunicazione individualizzata.

La rilevanza, quindi, della raccolta e dell'utilizzo dei dati personali è di tutta evidenza nel *marketing* moderno, la cui attività è tesa appunto ad offrire alle imprese informazioni, possibilmente sempre più complete, afferenti a soggetti che si ritengono compatibili, in relazione alle relative caratteristiche personali, con i beni e servizi prodotti ed offerti.

Con l'introduzione nell'ordinamento nazionale della disciplina sul trattamento dei dati personali, da un lato, i destinatari dell'attività di *marketing* (che dei loro stessi dati personali in larga misura si alimenta) hanno preso coscienza di disporre di nuovi strumenti di difesa nei confronti dei trattamenti caratterizzati da finalità pubblicitarie, promozionali e commerciali (avendo oggi il diritto di consentire in modo libero e consapevole all'uso di detti dati per tali fini, come anche di opporvisi). Dall'altro lato, anche le imprese acquisiscono sempre più coscienza del valore aggiunto che può rappresentare una banca dati di qualità e selettiva in cui siano inseriti specifici e "mirati" dati personali di coloro i quali hanno liberamente ed espressamente manifestato un consenso al trattamento, compilando questionari articolati.

Sul fenomeno, in particolare in relazione alla raccolta dei dati effettuata attraverso questionari e *coupon* mediante i quali vengono richiesti dati anagrafici, recapiti telefonici e telematici, informazioni sulle attività professionali svolte, redditi, composizione del nucleo familiare, gusti e preferenze, l'Autorità era già intervenuta alla fine del 1999 (v. Relazione per il 1999). Si è reso così evidente un ricorso crescente a tali tecniche in numerosi settori merceologici e si è constatato che detta raccolta non è sempre svolta conformemente alla normativa sulla protezione dei dati personali.

I rilievi critici riguardano soprattutto l'informativa all'interessato, spesso mancante o inidonea (per incompletezza o inesattezza) a rendere conto compiutamente delle modalità e delle finalità del trattamento effettuato, riflettendosi così sulla validità delle dichiarazioni di consenso rilasciate.

In un provvedimento a carattere generale emesso il 13 gennaio 2000, trasmesso anche ad organismi, istituzioni ed organizzazioni dei settori interessati, sono state pertanto fornite precise indicazioni alle quali si è conformata nel corso dell'anno l'attività di verifica del Garante.

In ordine a ciò sono stati altresì emessi provvedimenti *ad hoc* nei quali si è di volta in volta segnalata la necessità di: a) apportare modifiche alla clausola di informativa e consenso presente nei modelli utilizzati; b) correggere l'impostazione seguita da società che esercitano, in particolare, attività di *telemarketing* (Prov. 14 settembre 2000) e che non forniscono l'informativa agli interessati contattati telefonicamente neppure al momento della promozione, pur essendo tenute ad indicare le principali caratteristiche del trattamento dei dati, anche se temporaneo (si è evidenziato in tal caso che il mancato rispetto delle disposizioni sull'informativa agli interessati, di cui all'art. 10 della legge n. 675/1996, comporta l'illiceità del trattamento e, tra l'altro, la violazione amministrativa prevista dall'art. 39, comma 2, della legge medesima); c) richiedere il consenso all'interessato rispetto ad ulteriori ed eventuali trattamenti promozionali ed alla comunicazione a terzi dei dati con una formula "in positivo", anziché "in negativo", ovvero dando per presupposto il consenso salvo eventuale diniego.

Gli stessi principi sono stati poi estesi a società che effettuano selezione del personale e che, nello svolgimento della propria attività, raccolgono *curricula* anche tramite annunci riportati su quotidiani o periodici, realizzando in tal modo una raccolta di dati personali; pure in questa evenienza si rende infat-

ti necessario assolvere all'obbligo di informativa nei termini più volte indicati dal Garante, considerando che, in caso di inottemperanza, le dichiarazioni di consenso spesso richieste (e rese) per i *curricula* sono da ritenersi invalide.

Nel giugno del 2000 il Garante, sempre al fine di fornire indicazioni riguardo all'esatto adempimento della normativa sulla protezione dei dati personali, ha svolto due audizioni con operatori direttamente interessati ai provvedimenti sopra richiamati e con organismi ed associazioni operanti nei settori maggiormente coinvolti.

Nella prima audizione, gli operatori hanno formulato un giudizio positivo e di condivisione delle indicazioni fornite dal Garante in ordine al contenuto e alle modalità di predisposizione dell'informativa, soprattutto per quanto concerne l'esigenza di completezza, semplificazione, sintesi e chiarezza delle informazioni. In tale sede, sono stati forniti ulteriori chiarimenti, in particolare sui seguenti aspetti:

- elementi essenziali da riportare nell'informativa, contemperando le esigenze di sintesi e di semplicità;
- indicazione delle categorie dei soggetti a cui i dati sono comunicati, evitando la generica formula "*aziende di nostra fiducia*";
- eliminazione della richiesta di consenso per i trattamenti derivanti dall'esecuzione di obblighi di natura contrattuale o dall'acquisizione di informative precontrattuali su richiesta degli interessati;
- inidoneità di alcune correnti formule di consenso con riferimento ai trattamenti svolti da altre società destinatarie dei dati.

In particolare il Garante ha ribadito l'esigenza che il consenso degli interessati, per essere validamente manifestato, deve essere espresso, libero e specifico. Le disposizioni vigenti, infatti, richiedono l'acquisizione e la documentazione per iscritto dell'atto di assenso al trattamento dei dati da parte dell'interessato.

Nella seconda audizione, le associazioni di categoria hanno manifestato la propria disponibilità a costituire un gruppo di lavoro sulle problematiche applicative della legge n. 675/1996 nel settore del *direct marketing*, che potrebbe curare anche la predisposizione di linee-guida e modelli semplificati utilizzabili dalle società associate. In particolare, una di queste ha segnalato l'esigenza di distinguere tra le vere e proprie ricerche di mercato, svolte dai propri associati (i quali acquisirebbero dati personali solo nella fase iniziale, mediante interviste effettuate previo consenso degli interessati, con una loro successiva analisi o divulgazione in forma anonima ed aggregata secondo metodi statistici e scientifici), e le indagini di *marketing* eseguite tramite modulistica analoga a quella esaminata dal Garante, che avrebbero invece la finalità di "profilazione" dei comportamenti delle persone, ricerca di clientela e gestione delle relative banche dati.

In materia, quindi, l'Autorità persevera nella propria opera volta, da un lato, a sensibilizzare gli operatori di settore e, dall'altro, a vigilare per assicurare il rispetto delle disposizioni sulla tutela del trattamento dei dati personali.

Il Garante apprende poi con soddisfazione che emerge progressivamente un moderno concetto di *marketing*, finalizzato a prestare al consumatore un servizio attraverso forme selettive di consenso, più rispettose della personalità degli interessati, nelle quali l'elemento di adeguata informativa è prevalente rispetto al mero profilo promozionale e pubblicitario.

COMMERCIO ELETTRONICO

52. PROFILI GENERALI E LINEE DI TENDENZA

Dei vari argomenti coinvolti dalla problematica riguardante la tutela dei dati personali, due presentano particolari aspetti di ampiezza e di costante mutevolezza: l'incidenza nei confronti del commercio elettronico e del *direct marketing* ⁽¹⁾.

La globalizzazione dei mercati coincide con quella delle reti telematiche di comunicazione anche interattiva. Assistiamo a modifiche di tecniche contrattuali per la vendita dei prodotti, nonché all'evoluzione di tecniche informative e promozionali degli stessi prodotti, in forme sempre più personalizzate.

Da un lato emerge la necessità di standardizzare le tecniche contrattuali al fine di automatizzare un numero crescente di affari e dall'altra preme la contemporanea esigenza di personalizzare gli approcci promozionali dell'offerta. Ciò comporta una costante attenzione da parte di autorità garanti come il Garante italiano, che assumono una caratteristica peculiare: di essere, nel medesimo tempo, applicatrici del diritto e creatrici di "giurisprudenza", ma anche sollecitatrici di tempestivi adeguamenti legislativi a causa dell'incalzare delle innovazioni di prodotto e di processo.

In un mondo sempre più interconnesso e quindi globalizzato dalla velocità delle conoscenze e dal movimento degli uomini, capitali, merci e servizi, l'aumento globale del valore aggiunto è direttamente proporzionale all'aumento della velocità e della quantità degli scambi. Tutto ciò si riflette nell'aumento della quantità dei beni prodotti e, quindi, nella riduzione dei costi di produzione, nonché nella dilatazione delle utilità - e conseguentemente di rischi - per utenti e consumatori.

Le problematiche relative alla tutela dei dati personali e riguardanti la trasparenza e correttezza del loro uso sia in sede di offerta di prodotti, sia in sede di conclusione ed esecuzione contrattuale nelle compravendite, sono destinate ad incidere sempre più nell'immediato futuro e ciò è legato anzitutto alla diffusione dei *personal computer* ed ai collegamenti Internet.

Dall'indagine pubblicata di recente dalla X Commissione attività produttive della Camera dei deputati sul commercio elettronico, si apprende che gli utenti Internet a livello mondiale nel luglio del 2000 erano già 360 milioni ⁽²⁾. Per quanto riguarda l'Europa, alla stessa data il numero degli utenti era di 95 milioni ed è previsto che salirà a 140 milioni nel 2003.

Già ora in Italia il 32% delle famiglie possiede un *personal computer* e si stima che circa 14 milioni di individui, pari al 25% della popolazione, abbia navigato in Internet nell'ultimo trimestre del 2000. Si prevede che tale numero raddoppierà nel 2003.

Da questi dati ci rendiamo facilmente conto come, nel prossimo futuro, l'incidenza della problematica riguardante la tutela della *privacy* aumenterà ancora, impegnando da un lato l'adeguamento legislativo e, dall'altro, l'attività giurisprudenziale e di indirizzo del Garante italiano.

Il problema che si pone è quello di garantire libertà di sviluppo ai mercati riducendo al minimo i vincoli e gli adempimenti e garantendo, dall'altro, la necessaria tutela ai diritti fondamentali dell'individuo. Si tratta dunque di una vera e propria navigazione tra Scilla e Cariddi, tra la libertà di intraprendere e i diritti di riservatezza del singolo.

Per quanto riguarda il valore del commercio elettronico in Europa si stima che nei prossimi quattro anni passerà da 25 a 510 miliardi di euro, cioè dagli attuali 50 mila miliardi di lire ad oltre un milione di miliardi di lire.

⁽¹⁾ Il presente paragrafo riproduce ampi brani dell'intervento del prof. Gaetano Rasi, componente del Garante, al convegno su "Diffusione dell'e-commerce, tecniche di direct marketing e protezione dei dati", tenutosi a Roma in occasione del Forum P.A. del 7-11 maggio 2001.

⁽²⁾ Camera dei Deputati, Servizio Commissioni indagini conoscitive e doc. leg.va, n. 40, "Il commercio elettronico", X Commissione, Atti parlamentari, XIII Legislatura. All'indagine ha preso parte anche il prof. Rasi prima della elezione quale componente del Garante.

aumento del 42% sullo stesso dato mensile dell'anno precedente. Tutto ciò sembra dunque dare adito a considerazioni riguardanti una espansione del sistema purché, naturalmente, vi siano condizioni favorevoli e non ostative.

Un recente studio curato dal Gruppo dei Garanti europei (*Privacy on the Internet, An integrated approach to on-line data protection*, menzionato nella documentazione allegata alla presente Relazione), relativo anche al fenomeno dello *spamming* (ossia dei messaggi di posta elettronica contenenti comunicazioni pubblicitarie indesiderate), ha posto in luce dati secondo cui il fenomeno stesso negli USA sarebbe in declino perché gli stessi operatori preferiscono ricorrere ad attività di *marketing* più corrette anche in termini di protezione dei dati. Si allude all'introduzione del concetto di *marketing* su autorizzazione, ossia l'istituzione di canali di comunicazione con i consumatori su base volontaria passando per gradi da un rapporto fondato sull'interesse ad un rapporto basato sulla fiducia.

Con il crescere della fiducia, il consumatore viene convinto ad autorizzare una gamma sempre più ampia di attività di *marketing*, raccolta di dati sulle abitudini di vita, su *hobbies* e interessi, invio di messaggi pubblicitari relativi a nuovi prodotti e servizi, ecc. Questo tipo di *marketing* basato su un approccio di "*opt-in*" (ossia, sulla possibilità per il cliente di scegliere se aderire o meno) è espressione di una parola d'ordine crescente fra gli operatori del settore negli USA (che permette probabilmente di superare le conclusioni dell'ultimo rapporto su Internet redatto dall'*USIC-United States Internet Council*, contenente una serie di raccomandazioni ai Governi, tra cui quella secondo cui una rete soggetta ad eccessive restrizioni - anche in materia di *privacy* - renderebbe impossibile il commercio elettronico).

Il *marketing* basato su un approccio di "*opt-in*", dopo essere stato la parola d'ordine degli operatori americani può diventare anche l'approccio più adatto ad una prassi europea, conformemente alle norme giuridiche che vanno già in questa direzione in diversi Stati membri tra cui l'Italia.

Quattro sono attualmente gli strumenti comunitari rilevanti: a) la direttiva generale sulla protezione dei dati (95/46/CE); b) la direttiva sulle telecomunicazioni (97/66/CE); c) la direttiva sulle vendite a distanza (97/7/CE) e d) la direttiva sul commercio elettronico (2000/31/CE).

Le direttive non sono pienamente armonizzate tra loro (le prime due, ed in parte anche la terza, adottano un approccio sostanzialmente basato sull'*opt-in*, mentre quella sul commercio elettronico sembra favorire un approccio di tipo *opt-out*). Si è creata così una qualche ambiguità di fondo, posta in evidenza anche dagli estensori dello studio da ultimo citato, che non facilita l'individuazione di condotte chiare ed univoche da parte delle imprese che operano in questo settore. Alcune disposizioni riguardano poi solo la legittimità dell'invio di comunicazioni commerciali indesiderate nell'ambito di determinate relazioni *business-to-consumer* o *business-to-business*, e non disciplinano a monte la più complessa questione della raccolta e del trattamento dei dati personali.

Non vi sono, tuttavia, rilevanti conflitti di tipo giuridico, giacché la direttiva n. 2000/31/CE (e tale aspetto dovrà essere tenuto presente all'atto del suo recepimento in Italia) non si applica nei settori disciplinati dalle due citate direttive sulla protezione dei dati.

Occorrerà però grande attenzione nell'interpretare ed armonizzare sul piano applicativo questo complesso di regole.

Per eliminare le menzionate ambiguità occorre anche che il dibattito si sposti dalla mera correttezza dell'invio di messaggi pubblicitari alla liceità e correttezza della raccolta di dati.

Esplicitando le circostanze in cui è possibile raccogliere legittimamente dati personali (come l'indirizzo di *e-mail*), l'operatore commerciale ed il destinatario dell'*e-mail* possono già scegliere in modo trasparente la natura e gli sviluppi futuri del rapporto instauratosi.

Appare poi naturale estendere su scala europea al *marketing* diretto via *e-mail* le stesse regole valide per il *marketing* diretto effettuato attraverso dispositivi automatici di chiamata o *fax* - poiché in entrambi i casi si tratta di attività di natura invasiva che non possono essere interrotte dai destinatari.

Alcune prime considerazioni conclusive e riassuntive sembrano quindi possibili:

1) la tutela della riservatezza non solo non contrasta, ma costituisce il necessario presupposto per lo sviluppo del commercio elettronico.

2) sempre più spesso gli utenti ed i consumatori scelgono l'operatore o il fornitore di servizi a cui si rivolgono tenendo conto della politica in materia di *privacy* da questo adottata. Ciò fa sì che oggi l'adozione di pratiche rispettose dei diritti delle persone sia divenuta un fattore stesso - importante - di concorrenza fra gli operatori del settore.

Sempre nella stessa indagine della X Commissione della Camera dei Deputati, si prevede che per l'Italia, nel periodo 1999-2004 le vendite *on-line* passeranno da 1,8 a 53 miliardi di euro, ossia da 3.600 miliardi di lire a oltre 110 mila miliardi di lire.

In cifre individuali gli acquirenti via Internet dovrebbero passare da meno di 1 milione di fine 1999 a circa 10 milioni dell'inizio del 2004.

Attualmente il 65% delle transazioni elettroniche riguarda il *business to business* ed il 35% del *business to consumer*. Si prevede che alla fine del 2003 il *business to business* raggiungerà un peso percentuale pari al 77%. In altre parole sono soprattutto le aziende ad usarlo fra loro, piuttosto che il cliente finale.

Questi dati corrispondono con altro recente studio - curato dall'IPSOS - il quale indica addirittura che vi sarebbe una generale tendenza da parte del pubblico dei consumatori a non sviluppare il commercio elettronico. Nel 1999 a livello europeo infatti il 27% degli intervistati dichiarava di voler fare a breve un acquisto via Internet mentre, alla distanza di un anno, la percentuale è scesa al 20% (i francesi dal 48% delle intenzioni di acquisto sono passati al 16%; gli inglesi dal 24% al 16%; i portoghesi dal 42% al 31%; gli italiani dal 31% al 25%).

Comunque, si tratti di commercio tra imprese o di vendite ai consumatori, il problema riguarda non solo i dati relativi ai mezzi di pagamento utilizzati (carta di credito), ma anche le altre informazioni personali quali, per esempio, i gusti presumibili dai consumi abituali. E ciò non direttamente nei confronti dei consumatori, ma attraverso i loro fornitori che acquistano i dati elaborati da terzi. Sono tutti dati utilizzati per definire il profilo dei clienti ai fini del *marketing*.

Mentre inizialmente - da parte di coloro che si pongono come ditte fornitrici - si era registrato un atteggiamento di diffidenza nei confronti delle disposizioni poste a tutela della riservatezza, successivamente si è potuto riscontrare un progressivo mutamento di posizioni.

Oggi sono sempre più gli operatori che comprendono l'importanza di instaurare con gli utilizzatori - ossia con altre imprese e pure con i consumatori - un rapporto impostato in termini di lealtà e trasparenza nell'uso dei loro dati personali.

Dobbiamo constatare che progressivamente si avverte la necessità di passare da sistemi di raccolta occulta dei dati ad altri che prevedono l'informazione preventiva del consumatore sui trattamenti, consentendogli di prestare, al riguardo, forme differenziate di consenso.

Si realizza così un sistema per il quale il destinatario dei prodotti e dei servizi è in grado di valutare esplicitamente i vantaggi, in termini di informazione, assistenza, servizi aggiuntivi che possono derivare all'interessato proprio da un corretto utilizzo dei suoi dati.

Tutto questo non costituisce solamente un modo per attrarre più consumatori, evitando di "spaventarli" attraverso pratiche eccessivamente aggressive di raccolta dei dati e successivo trattamento ai fini di *marketing*. Ma anche la sola via per ottenere dagli stessi consumatori informazioni attendibili, evitando che essi - secondo quanto a volte accade - ricorrano a forme di "difesa" basate sul conferimento di dati errati. Col risultato di vanificare le strategie di *marketing* adottate.

Le considerazioni fatte spiegano anche perché le politiche della *privacy* in materia di commercio elettronico siano oggi divenute uno strumento di competizione fra i diversi operatori. Ossia un elemento ulteriore per caratterizzarsi di fronte ai consumatori, conquistandone la fiducia e mantenendola nel tempo.

Una prima soluzione proposta è già sul tappeto e riguarda l'adozione del marchio internazionale di garanzia a tutela dei consumatori *on-line* e rientra nelle iniziative riguardanti il commercio elettronico della Commissione dell'Unione Europea. La *Better Business Bureau on-line (BBB on-line)* ed *Eurochambres (Association of european chambers of commerce and industry)*, come molti altri soggetti, hanno ad esempio proposto un primo marchio di fiducia internazionale, che dovrebbe attestare che l'impresa che lo espone *on-line* aderisce a specifici standard commerciali e garantisce il rispetto di un codice di condotta nella risoluzione di eventuali controversie.

La correttezza e riuscita di queste iniziative dipende tra l'altro dalla scelta dei parametri per il rilascio del "marchio": assai utile, in tal senso, è la serie di prescrizioni contenute nella recente Raccomandazione sui requisiti minimi per la raccolta di dati attraverso siti *web*, approvata dai Garanti europei e riportata nella documentazione allegata alla presente Relazione.

Passando al *direct marketing* va osservato che l'andamento della pubblicità via Internet e la collaterale attività di vendita *on-line* ha subito negli USA una crescita: a febbraio di quest'anno si è avuto un