3) anche al di là di ogni considerazione sui profili inerenti alla protezione dei diritti fondamentali delle persone, le pratiche troppo aggressive di *marketing* via Internet si rivelano inefficaci e controproducenti per chi le attua sul piano della riuscita commerciale (rifiuto generalizzato nei confronti del cosiddetto *spamming*).

4) il conferimento all'utente di un'informativa completa ed esauriente sui trattamenti che verranno svolti sui suoi dati, ed il riconoscimento a questi della facoltà di dare il proprio consenso informato ai trattamenti medesimi costituiscono ormai un presupposto necessario anche per chi intenda perseguire una politica di fidelizzazione dei clienti nel tempo.

53. CASI APPLICATIVI

Il Garante ha concluso nel corso del 2000 un primo monitoraggio di alcuni siti *web* volto ad accertare le modalità di informativa degli utenti e di raccolta del consenso, ove necessario.

Sulla base di una circostanziata segnalazione di un'associazione di consumatori, l'Autorità ha avviato di recente un'ulteriore serie di verifiche con particolare riguardo ai c.d. "trattamenti invisibili" che sarebbero effettuati da altri siti *web*, nonché relativamente all'informativa per finalità di *marketing* e di commercio elettronico, alla c.d. profilazione di clienti anche in relazione a dati sensibili.

Gli accertamenti verranno conclusi – e abbinati ai risultati del predetto monitoraggio – applicando i principi in materia di esauriente informativa e di libero e consapevole consenso richiamati nei par. 51 e 55 della presente Relazione in relazione al *marketing*, al *telemarketing* e alle reti di telecomunicazione e telematiche.

Numerosi altri procedimenti sono in corso per specifiche violazioni segnalate da persone che ricevono *e-mail* indesiderate – a volte, addirittura in presenza di un'espressa opposizione – o fax anche a ripetizione, nell'inosservanza dei principi di cui, in particolare, al d.lg. n. 171/1998 e al d.lg. n. 185/1999.

RETI TELEMATICHE E SERVIZI DI TELECOMUNICAZIONE

54. PROFILI GENERALI

L'universo delle telecomunicazioni e, al suo interno, il settore della telefonia e delle reti informatiche è stato oggetto di particolare attenzione da parte del Garante anche nel corso del 2000: numerose sono state invero le segnalazioni pervenute, a dimostrare la particolare sensibilità dell'opinione pubblica e a testimoniare la crescente familiarità dei cittadini con l'utilizzo delle tecnologie dell'informazione.

L'evoluzione tecnologica in questo settore, notoriamente, mentre rende disponibili nuovi servizi e funzioni di interesse per i cittadini, evidenzia al contempo i rischi collegati ad una pervasiva ed automatica raccolta di dati personali. Laddove, poi, ciò avviene attraverso l'offerta agli utenti di prestazioni gratuite in cambio dell'uso delle informazioni, raccolte senza una esauriente informativa ed impiegate ormai come una vera e propria merce di scambio, è evidente la necessità di assicurare garanzie ancor più adeguate a tutela della sfera privata, dell'identità e della dignità personale.

Emerge, così, il ruolo centrale delle normative a tutela della riservatezza, anche in relazione alla possibilità che i dati raccolti siano utilizzati per operare classificazioni sempre più sofisticate di utenti e consumatori, anche al fine di porre ciascuno in grado di esercitare consapevolmente la propria facoltà di scelta. Occorre infatti considerare che ad una crescente alfabetizzazione degli utenti in riferimento all'uso dei principali servizi di telecomunicazione, non sembra ancora affiancarsi un'adeguata informazione rispetto ai meccanismi di funzionamento ed all'utilizzo delle informazioni trattate da fornitori e gestori nel corso dell'erogazione.

Anche nell'anno trascorso, perciò, l'attività del Garante è stata rivolta soprattutto alla verifica della conformità delle modalità di attivazione ed erogazione dei servizi di telecomunicazione alla normativa sulla protezione dei dati, anche attraverso l'opportuna attività di informazione e di divulgazione generale indirizzata agli operatori e agli utenti, con particolare riguardo ad Internet ed ai servizi di telefonia fissa e mobile.

Nel quadro delle sue competenze nell'ambito del Gruppo europeo delle autorità garanti istituito dall'art. 29 della direttiva n. 95/46/CE, e dei gruppi di lavoro presso il Consiglio dell'Unione europea, il Garante partecipa inoltre attivamente alla rielaborazione del quadro europeo della direttiva in materia di protezione dei dati personali nei servizi di telecomunicazione, attualmente in corso ad opera del Consiglio e del Parlamento europeo.

55. TRASPARENZA E CORRETTEZZA VERSO GLI UTENTI INTERNET

Proprio con riferimento ad Internet si può cogliere con maggiore nettezza il fatto che da strumento di isolamento dagli altri, quale diritto ad essere lasciati soli, la *privacy* si trasforma in strumento di controllo dinamico e di comunicazione. Allo stesso modo, nell'area del commercio elettronico, la riservatezza diventa lo strumento attraverso il quale, con fiducia, l'utente accede all'acquisto di beni o di servizi, con la garanzia che quelle informazioni non verranno impropriamente utilizzate, fatte circolare, elaborate per costruire profili della personalità che potrebbero avere anche effetti discriminatori.

Attualmente è assai difficile utilizzare Internet senza doversi misurare con pratiche invasive della *privacy* individuale ed operazioni di trattamento dei dati personali effettuate con modalità tali da restare invisibili all'interessato. In altre parole, l'utente Internet non sa spesso che i suoi dati personali sono stati raccolti e successivamente elaborati e che potrebbero essere utilizzati per scopi a lui non resi noti. L'interessato per lo più non sa nulla di tale trattamento e non può, di riflesso, assumere decisioni "libere" al riguardo. Il Gruppo europeo dei garanti si è non a caso espresso sulla questione già nel Parere n. 1/1999 del 23 febbraio 1999, incoraggiando l'industria del *software* e dell'*hardware* a lavorare su prodotti Internet rispettosi della *privacy*, fornendo i necessari strumenti per conformarsi alla normativa europea sulla protezione dei dati.

Una prima condizione per un trattamento lecito dei dati personali è che il soggetto dei dati sia informato e messo compiutamente al corrente del trattamento in questione. Il Gruppo si è quindi particolarmente interessato a tutti i tipi di operazioni di trattamento attualmente effettuate da *software* ed *hardware* su Internet privi di queste caratteristiche.

In questa materia anche la CNIL (*Commission nationale pour l'informatique et les libertés*) francese ha svolto una preziosa ricerca, concentrandosi soprattutto sul trattamento automatico ed invisibile dei dati personali attraverso *software* ed *hardware* nel corso della navigazione su Internet. La ricerca è stata presentata al Garante, nello spirito di collaborazione che anima l'operato delle autorità europee, nell'ambito di un seminario svoltosi il 13 novembre 2000 presso la sede dell'Autorità.

Sul versante dell'attività interna, il Garante è intervenuto per valutare le procedure di corretta e trasparente acquisizione e di pertinente trattamento dei dati da parte dei fornitori di servizi di accesso ad Internet. L'Autorità aveva avviato già nel luglio del 1999 un procedimento di indagine nei confronti del servizio di accesso gratuito ad Internet ("*Libero*" di Infostrada), a seguito di diverse segnalazioni concernenti l'acquisizione, al momento dell'attivazione del servizio, di varie informazioni personali, nonché il successivo monitoraggio delle connessioni ai siti visitati dagli abbonati, allo scopo dell'individuazione delle loro preferenze per determinare il profilo dei fruitori del servizio, o per programmare l'invio di messaggi *e-mail* a sfondo pubblicitario (v. Relazione per l'anno 1999, p. 72).

Al termine di un'approfondita istruttoria, nel corso della quale è stato affrontato il tema della raccolta e dell'utilizzazione di dati personali nell'ambito di servizi di accesso gratuito ad Internet offerti dagli operatori nel settore delle telecomunicazioni, il Garante ha indicato alla società titolare del trattamento alcune modalità necessarie ad assicurare la liceità e la correttezza dei comportamenti nei confronti degli utenti (*Provv.* del 13 gennaio 2000).

Il Garante ha chiarito che, fermo restando il rispetto della volontà dei cittadini di consentire alla cessione di dati identificativi o attinenti a gusti, preferenze ed interessi, in particolare per ottenere gratuitamente determinati servizi, gli interessati devono, comunque, essere messi in grado di esprimere le proprie scelte sull'uso dei dati che li riguardano, consapevolmente e liberamente. Per questo è anzitutto necessario che essi ricevano tutte le informazioni necessarie per la piena comprensione delle finalità e delle modalità di trattamento dei dati, compresi quelli acquisiti in un momento successivo – giacché l'obbligo di informazione al cliente permane, anche quando non venga richiesto alcun consenso –, dovendosi verificare attentamente se taluni dati, indicati come asseritamente "obbligatori" dalle società del settore, siano realmente indispensabili per attivare e mantenere il servizio principale offerto.

In particolare, le segnalazioni pervenute al Garante avevano prospettato un contrasto con la normativa, sia sotto l'aspetto dell'insufficienza delle informazioni fornite agli interessati, sia riguardo alla possibilità di raccogliere dati sui siti frequentati e di controllare l'effettiva lettura, da parte degli abbonati, dei messaggi pubblicitari inviati dalla società.

Nel corso del procedimento, la società titolare ha peraltro provveduto ad eliminare alcune incongruenze ed anomalie presenti nella documentazione sottoposta al potenziale cliente all'atto dell'iscrizione, specificando che l'analisi degli accessi ai siti *web* sarebbe stata svolta tra quelli presenti in un catalogo predisposto dalla stessa società, in modo da evitare il riferimento a siti dal cui contenuto fosse possibile ricavare il riferimento a dati sensibili, e negandosi, d'altra parte, che fosse effettuata alcuna verifica circa il ricevimento e la visualizzazione dei messaggi pubblicitari da parte degli utenti.

Nel provvedimento finale il Garante ha tuttavia ritenuto necessaria l'ulteriore revisione di alcuni profili relativi alle informazioni e ai documenti sottoposti ai clienti all'atto della richiesta dell'attivazione del servizio, fornendo al riguardo diverse indicazioni che debbono ritenersi estensibili a tutti gli operatori che offrono servizi analoghi.

In particolare si è segnalato che l'informativa, riferita a tutti gli aspetti del complessivo trattamento svolto dal fornitore nell'ambito del servizio (attraverso la riepilogazione chiara delle notizie ad esso attinenti presenti nel contratto, nonché integrata con un richiamo, anche sintetico, ai diritti di accesso attribuiti agli interessati dall'art. 13 della legge n. 675/1996, con l'indicazione dell'ufficio o servizio presso cui esercitare tali diritti), deve essere collocata prima della richiesta di registrazione dei propri dati.

L'obbligo di informazione impone inoltre di precisare tutte le categorie di ulteriori soggetti ai quali potranno essere comunicate le informazioni raccolte e che dovrebbero, a loro volta, acquisire il consenso degli interessati, salvo che sia la prima società titolare del trattamento a richiedere il consenso dei clienti anche per conto delle successive, fornendone una precisa indicazione, anche predisponendo un elenco a parte da rendere agevolmente consultabile per gli interessati.

La richiesta del consenso nei confronti degli abbonati che abbiano accettato le condizioni contrattuali, autorizzando l'invio di messaggi pubblicitari sulla propria casella di posta elettronica, pur potendo essere circoscritta alle sole operazioni di trattamento dei dati per finalità commerciali non collegate al servizio ed alla loro divulgazione all'esterno, dovrebbe essere poi riferita anche alle disposizioni in materia di pubblicità e di chiamate indesiderate, introdotte dalle recenti normative sulla riservatezza delle telecomunicazioni (d.lg. n. 171/1998) e sui contratti a distanza (d.lg. n. 185/1999).

Riguardo ai dati acquisiti con i moduli di adesione al servizio, il Garante ha segnalato la necessità di rendere ben edotti gli interessati che determinate informazioni sono, poi, raccolte non in virtù di specifici obblighi normativi (non ravvisabili nella mera opportunità di rendere accessibili alcune informazioni sugli abbonati ad organi ed autorità preposte ad indagini ipoteticamente interessate in futuro a raccoglierle), quanto in vista dell'intenzione del fornitore di procedere al trattamento sulla base di un'autonoma scelta di caratterizzazione del servizio, anche quando l'abbonato non presti il consenso a trattamenti e comunicazioni per finalità commerciali.

Inoltre, in relazione agli aspetti connessi ai dati relativi ai siti consultati dagli abbonati, il Garante ha confermato la necessità che si assumano tutte le misure idonee ad evitare una raccolta di informazioni sensibili.

Nel fornire tali indicazioni, il Garante ha segnalato la necessità di fornire a ciascun utente già abbonato al servizio il nuovo testo di informativa messo a punto per i nuovi clienti e rispettoso della normativa sulla protezione dei dati personali, assicurando ai vecchi abbonati la possibilità di esprimere nuovamente il consenso o di revocare attraverso un meccanismo agevole le precedenti manifestazioni di volontà.

L'Autorità ha altresì disposto che copia del provvedimento fosse trasmessa anche agli altri operatori che offrono servizi analoghi, allo scopo di sensibilizzarli al maggior rispetto della normativa vigente.

Sotto altro profilo, è emerso che la diffusione crescente delle connessioni onerose o gratuite ad Internet, unitamente alla maggiore attenzione rivolta al potenziale mercato degli utenti telematici da parte delle imprese e delle associazioni, comporta talvolta frizioni tra l'interesse alla comunicazione pubblicitaria, la libertà di manifestazione del pensiero ed il diritto alla riservatezza, che vengono portate all'attenzione dell'Autorità.

Nell'anno trascorso, si è potuto ad esempio assistere ad un incremento dell'utilizzo dei sistemi informatici e di telefonia fissa e mobile per finalità di comunicazione politica e di propaganda elettorale, con l'impiego di metodologie non sempre conformi alla normativa vigente sulla tutela delle informazioni personali. Ci si trova in questi casi, in rete, di fronte all'esigenza di tutelare due diversi interessi: da una parte quello di chi comunica; dall'altra l'interesse di chi, essendo destinatario della comunicazione, ha diritto di preservare la propria sfera privata difesa da ingiustificate invasioni altrui.

Come già riferito in altro paragrafo, in data 15 novembre 2000 il Garante ha avviato accertamenti per verificare la fondatezza di una segnalazione relativa ad un trattamento di dati effettuato dall'Osservatorio sulla legalità e la questione morale, in relazione alla ricezione non gradita di un messaggio di posta elettronica proveniente dal sito dell'associazione.

Sulla base dei riscontri effettuati e degli elementi forniti dall'Osservatorio, la segnalazione non è poi risultata fondata. Si è accertato, infatti, che il messaggio oggetto della segnalazione, non era stato inviato direttamente dall'Osservatorio o dal relativo sito, ma da un privato che aveva ritrasmesso la *newsletter* dell'Osservatorio ad un limitato numero di destinatari, nel quadro di una probabile attività interpersonale di informazione.

Il Garante, constatando che i documenti sottoposti all'utente all'atto dell'adesione non erano pienamente conformi alla normativa, ha però proceduto, sulla base della documentazione acquisita, a segnalare autonomamente all'Osservatorio, ai sensi dell'art. 31, comma 1, lett. c), della legge n. 675/1996, la necessità che l'informativa e la formula di consenso inserite sul sito, in calce al modulo di adesione all'Osservatorio, fossero riformulate in modo da contenere, anche sinteticamente e con eventuale stile colloquiale, tutti gli elementi richiesti dall'art. 10 della legge n. 675/1996.

La Raccomandazione sulla raccolta di dati personali

Il 17 maggio 2001 Il Gruppo delle autorità per la protezione dei dati dell'Unione europea, presieduto da Stefano Rodotà, ha adottato una Raccomandazione (n. 2/2001, riprodotta nella documentazione allegata), indirizzata al Consiglio d'europa, alla Commissione, al Parlamento europeo ed agli Stati membri, che fissa alcuni requisiti minimi per la raccolta di dati personali *on-line*.

La Raccomandazione nasce dall'esigenza di fornire indicazioni concrete sia agli operatori del settore responsabili del trattamento di dati personali nell'ambito di siti *web* (i "titolari", secondo la definizione della direttiva), sia ai singoli cittadini. Essa è rivolta anche agli enti che intendono creare un "bollino di qualità" che certifichi la rispondenza delle procedure di trattamento utilizzate alle direttive dell'Ue in materia.

L'aspetto significativo risiede anzitutto nella distinzione tra un primo gruppo di notizie che ciascun sito deve fornire a tutti i visitatori, in modo snello e visibile, ed un nucleo più articolato di informazioni che il sito può fornire in altre pagine *web* evidenziando l'intera *privacy policy* del sito stesso.

Le indicazioni riguardano, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari devono fornire agli utenti quando questi si collegano a pagine *web*, indipendentemente dagli scopi del collegamento. I Garanti sottolineano che i requisiti indicati rappresentano solo un nucleo "minimo" e che potranno essere integrati, in futuro, da ulteriori raccomandazioni di natura più specifica (ad esempio, per quanto riguarda il trattamento di dati "sensibili" o relativi a minori, oppure i trattamenti per scopi di natura sanitaria).

La Raccomandazione si applica a tutti i trattamenti effettuati da titolari che siano stabiliti in uno degli Stati dell'UE, oppure che non siano stabiliti nell'UE, ma utilizzino, ai fini del trattamento, apparecchiature o dispositivi situati sul territorio di uno Stato membro dell'UE.

I Garanti raccomandano pertanto:

– di fornire preventivamente a chiunque si colleghi ad un sito *web* che preveda la raccolta di dati personali le informazioni indicate nella direttiva: identità e indirizzo (elettronico o meno) del titolare; finalità del trattamento; "obbligatorietà" del conferimento delle informazioni richieste all'utente (vi possono essere dati necessari per fornire un servizio richiesto da un utente, mentre altri sono opzionali); modalità per esercitare i diritti di accesso, rettifica, cancellazione, opposizione al trattamento; destinatari eventuali delle informazioni raccolte (e in tal caso l'utente deve avere la possibilità di opporsi alla trasmissione dei suoi dati ad altri soggetti, per scopi diversi da quelli per cui gli vengono richiesti dal sito – ad esempio cliccando su una specifica casella); eventuale utilizzo di procedure automatiche per la raccolta dei dati (è il caso, ad esempio, dei *cookies*); misure di sicurezza adottate per garantire l'integrità e la riservatezza dei dati richiesti;

– di fornire le informazioni sopra elencate direttamente sul *monitor* del singolo utente, prima che avvenga la raccolta dei suoi dati, così da garantire che il trattamento avvenga in modo leale come prescrive la direttiva; per farlo si può ricorrere alle varie possibilità messe a disposizione dalle attuali tecnologie: finestre "a scomparsa", caselle da cliccare, messaggi "*pop-up*". È opportuno inoltre che sulla pagina di accoglienza del sito vi sia un'indicazione chiara e comprensibile dell'esistenza di un'informativa sulla *privacy* (ad esempio: "Questo sito raccoglie e tratta dati personali che la riguardano. Per ulteriori informazioni, clicchi qui");

– di tenere presente che i titolari hanno anche altri obblighi sanciti sempre dalla direttiva, oltre al dovere di informare adeguatamente gli interessati. In particolare, è necessario che la raccolta di dati personali sia necessaria per le finalità specificate: pertanto, se l'obiettivo che il titolare si prefigge (fornire un servizio, un'informazione, ecc.) può essere raggiunto senza elaborare dati personali, questi non devono essere raccolti. Nella stessa ottica, si sottolinea l'opportunità di favorire ed accettare l'impiego di pseudonimi quando questi ultimi permettano comunque di svolgere determinate transazioni. Inoltre, non devono essere raccolti più dati di quelli necessari per lo scopo dichiarato (in base al c.d. principio di "pertinenza"), e i dati raccolti devono essere conservati solo per un periodo giustificato dalle finalità del trattamento;

– di non utilizzare indirizzi di posta elettronica ricavati da "aree pubbliche" di Internet (ad esempio, gruppi di discussione) per attività di *marketing*, nel caso in cui i diretti interessati non sono stati informati; se invece gli interessati sono stati informati della possibilità che i dati forniti in una sede determinata vengono utilizzati per scopi di *marketing* diretto, e hanno avuto la possibilità di esprimere il proprio consenso a questa forma di utilizzazione (magari cliccando *on-line* su una casella apposita), in tal caso l'uso di indirizzi di *e-mail* per fini di *marketing* è da ritenersi lecito. I titolari devono inoltre garantire che l'utente abbia la possibilità di revocare il consenso all'uso dei suoi dati per fini commerciali.

La diffamazione in Internet

Occorre tenere conto che la dimensione della *privacy* non è da considerare soltanto da parte del soggetto attivo in rete, ma deve essere valutata anche dal punto di vista dei soggetti che possono essere a loro volta oggetto della comunicazione in rete.

Come è noto, la libertà di manifestazione del pensiero rimane soggetta, anche quando esplicata su Internet, ai limiti previsti dalle leggi civili e penali e i poteri attribuiti al Garante dalla legge n. 675/1996 devono essere coordinati con le tecniche di tutela ordinariamente previste dal codice civile e dal codice penale, diverse da quelle contenute negli artt. 13 e 29 della legge n. 675/1996, e non invocabili dinanzi all'Autorità perché esorbitanti dalle competenze per essa legislativamente predeterminate.

Il Garante ha precisato questa posizione in un provvedimento del 30 ottobre 2000. Il caso riguarda una persona che aveva lamentato la diffusione, su un sito Internet, di un comunicato dedicatogli, contenente notizie ritenute non veritiere o offensive e riferentesi anche a persone estranee alla sua sfera professionale. L'interessato aveva perciò richiesto all'Autorità di bloccare la diffusione delle informazioni, ma il Garante ha sottolineato che la normativa sulla *privacy* e il codice di deontologia per l'attività giornalistica, nel tutelare la riservatezza, l'identità e la dignità personale, si riferiscono al trattamento illecito e non corretto dei dati e, in particolare, alla diffusione di dati riservati.

Tali disposizioni non possono essere invece invocate rispetto alla diffusione di informazioni denigratorie o diffamatorie, pure altrimenti sanzionata dall'ordinamento in sede civile e penale. Per tale motivo, il Garante non si è avvalso del potere di "blocco" di cui all'articolo 31, comma 1, lettera l), della legge. Tuttavia, l'Autorità ha fatto presente ai ricorrenti che resta in loro disponibilità, ove lo reputino opportuno, l'instaurazione di specifiche controversie a tutela della loro onorabilità presso le competenti autorità giudiziarie.

In un'altra occasione (*Provv.* del 16 gennaio 2001) il Garante è tornato ad occuparsi di una fattispecie di pretesa diffamazione a mezzo Internet.

I ricorrenti hanno chiesto al Garante di disporre la cancellazione o il blocco dei dati personali diffusi tramite alcune pagine *web*: gli autori di tali pagine (identificati in esse con il solo nome di battesimo), nel raccontare la propria esperienza di obiettori di coscienza, avevano divulgato alcune notizie ritenute false e lesive della reputazione di alcune persone e che non sembravano rispettare i limiti posti al diritto di cronaca e di critica (con riferimento ai requisiti di interesse pubblico, verità e correttezza dell'informazione e delle espressioni utilizzate), nonché i principi di protezione dei dati applicabili all'attività giornalistica e ai trattamenti temporanei di dati personali a scopo di pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero.

Chiamato dapprima a pronunciarsi sulla richiesta di adottare in via d'urgenza il blocco dei dati chiesto dalle ricorrenti (ai sensi dell'art. 29, comma 5, l. n. 675/1996), con provvedimento del 6 dicembre 2000 il Garante ha accertato l'insussistenza dei presupposti per adottare il blocco stesso in quanto, anche a seguito della richiesta di informazioni formulata dall'Autorità nei confronti del fornitore del servizio, le pagine *web* accessibili tramite gli indirizzi segnalati erano state disattivate. Da un ulteriore indirizzo risultavano accessibili nuove pagine *web*, che non includevano però dati personali relativi agli interessati; le vicende descritte nell'articolo in contestazione erano state riportate nelle medesime pagine, in un nuovo testo recante una narrazione *impersonale* senza riferimento ad alcun dato *personale*. I resistenti assumevano l'impegno a non divulgare dati delle ricorrenti anche in occasione di eventuali, futuri articoli, pagine e documenti pubblicati tramite Internet.

In sede di valutazione del ricorso il Garante ha dichiarato così non luogo a provvedere, ritenendo accolte le richieste degli interessati formulate ai sensi dell'art. 13 della legge n. 675/1996 e precisando, altresì, che la decisione di non luogo a provvedere non pregiudica il diritto dei ricorrenti di rivolgersi all'autorità giudiziaria in relazione ad altri eventuali profili (come quelli inerenti all'onore e alla reputazione o al risarcimento del danno) per i quali la legge n. 675/1996 non attribuisce competenza all'Autorità.

56. TRATTAMENTO E ACCESSO AI DATI DI TRAFFICO

Le modalità tecniche di erogazione dei servizi di telecomunicazione elettronica, si tratti di quelli Internet o dei servizi di telefonia mobile e fissa, consentono ai fornitori e talora a terzi interessati di accedere alle informazioni sul traffico dell'utenza. Si tratta di dati personali dotati di un notevole valore aggiunto, in quanto idonei anche a rivelare gusti ed interessi del consumatore, come pure a consentire la ricostruzione dell'intera trama delle relazioni private di un soggetto, o addirittura a permettere la rilevazione di informazioni particolarmente "sensibili" senza che l'interessato, avendone conoscenza, sia messo in condizione di esercitare i propri diritti.

Come è noto, peraltro, il d. lg. n. 171/1998 (v. Relazione per l'anno 1998) definisce con precisione quali dati personali (indirizzo, numero dell'abbonato, numero totale degli scatti nel periodo ecc.) possono essere utilizzati per le esigenze di fatturazione, essendo altrimenti obbligatorio cancellare o anonimizzare al termine della chiamata ogni altro dato personale eventualmente memorizzato. Tale trattamento a fini di fatturazione è consentito, peraltro, "sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento" (art. 4, comma 2, d.lg. n. 171/1998). Allo scopo di garantire maggiormente le esigenze di riservatezza degli utenti la normativa impone ai fornitori dei servizi di adottare anche modalità di pagamento alternative alla tradizionale fatturazione, tali da permettere di utilizzare il terminale con altra modalità di pagamento anche anonimo (ad esempio carte di credito, carte telefoniche prepagate ecc.).

Per quanto concerne l'invio della fattura ordinaria, il d.lg. n. 171/1998 prevede invece il diritto di ricevere, gratuitamente e dietro richiesta, l'indicazione dettagliata degli elementi dimostrativi degli oneri addebitati. Però, se ci si avvale di questo servizio, a garanzia soprattutto della riservatezza dei diversi utenti, devono essere mascherate le ultime tre cifre del numero chiamato. Quest'ultima prescrizione ha tenuto presente sia le indicazioni provenienti dal confronto in ambito europeo, sia il rapporto fra cifre mascherate e lunghezza totale dei numeri delle utenze telefoniche.

Diversi cittadini, liberi professionisti, imprenditori, associazioni, enti ed altri organismi (pubblici e privati) abbonati al servizio telefonico, tuttavia, continuano a lamentare gli ostacoli frapposti dai fornitori di servizi di telefonia all'accesso ai dati concernenti le chiamate addebitate nella bolletta, non in linea con le indicazioni dell'Autorità.

Proprio in risposta alla segnalazione di un cittadino che, dovendo tutelare un suo diritto in sede giudiziaria, aveva chiesto invano ad un gestore telefonico il rilascio della documentazione del traffico in entrata e in uscita relativamente ad un'utenza a lui intestata, il Garante ha rilevato che la legge sulla *privacy* permette all'abbonato di accedere ai dati di traffico sia in entrata, sia in uscita dalle proprie utenze telefoniche, senza necessità di un'autorizzazione o di altro provvedimento giudiziario.

In tale occasione il Garante, ribadendo quanto stabilito in diversi provvedimenti in materia di telecomunicazioni, ha specificato che rientra nella nozione di dato personale "qualunque informazione relativa all'interessato" (art. 1, l. n. 675/1996) e, come tale, se richiesta, essa deve essere messa a disposizione. Il diritto di accesso deve essere esercitato dall'interessato direttamente nei confronti del titolare o del responsabile del trattamento, personalmente o tramite un terzo cui sia stata conferita delega o procura per iscritto.

Nel caso in cui il gestore telefonico non dia soddisfazione alla richiesta ci si può rivolgere all'autorità giudiziaria o al Garante che ha ritenuto illegittimo, invece, l'accesso diretto a dati relativi a utenze intestate a terzi, i quali restano conoscibili esclusivamente tramite provvedimento giudiziario.

In un provvedimento adottato l'8 giugno 2000 a seguito di un ricorso, il Garante ha nuovamente affrontato tale questione, in riferimento alla comunicazione di alcuni dati di traffico telefonico in entrata e in uscita relativi ad alcune utenze fisse, chiesta dal difensore con un'istanza, formulata ai sensi dell'art. 38 disp. att. c.p.p., in materia di indagini difensive per l'esercizio del diritto alla prova, nonché con una successiva nota sottoscritta dallo stesso difensore. A seguito dell'invito ad aderire formulato dall'Autorità, la società ha comunicato agli interessati l'intendimento di non voler aderire alla richiesta formulata ai sensi del citato art. 38 disp. att. c.p.p. Con successiva memoria, la società resistente ha poi evidenziato, in particolare, che:

– la richiesta di acquisizione dei dati sarebbe stata volta all'esercizio di un eventuale diritto di difesa da parte di uno dei ricorrenti, che non sarebbe risultato, però, intestatario delle utenze telefoniche e non aveva, quindi, il diritto di accedere ai dati dell'abbonato (il quale, a sua volta, pur avendo sottoscritto le richieste e il ricorso, non sarebbe risultato titolare di alcun diritto nella sede processuale penale alla quale si è fatto riferimento);

– relativamente ai dati delle chiamate in entrata, vi era un'esigenza di tutelare la riservatezza degli abbonati chiamanti, per cui tali dati potevano essere comunicati "previo ordine del giudice" e, comunque, essere ricavati dal fornitore del servizio telefonico "a seguito di una procedura di elaborazione tecnicamente complessa ed onerosa, nell'ordine di centinaia di milioni" (di cui si sono illustrate, in termini generali, le modalità);

– le norme della legge n. 675/1996 sui presupposti di liceità del trattamento e della comunicazione dei dati personali non farebbero sorgere in capo al titolare del trattamento "alcun obbligo giuridico di adempimento". Tale obbligo, considerato quanto illustrato nella memoria della società, non poteva derivare neanche dall'art. 38 disp. att. c.p.p., che non attribuirebbe al difensore "alcun potere idoneo a costringere terzi a fornire le informazioni che vengono richieste".

Il Garante ha dichiarato il ricorso inammissibile, per difetto dei presupposti di cui all'art. 29 della legge n. 675/1996 (richiesta di esercitare il diritto di accesso ai dati che riguardano le proprie utenze telefoniche ai sensi dell'art. 13, l. n. 675/1996, e proposizione del ricorso solo in caso di inerzia o rigetto di tale specifica richiesta), atteso che il difensore si era limitato a chiedere l'accesso ai dati relativi al traffico di alcune utenze telefoniche intestate ad un altro ricorrente, con specifico riferimento, però, alla facoltà di raccogliere elementi di prova a fini investigativi ai sensi dell'art. 38 disp. att. c.p.p.

Il Garante ha precisato che una richiesta ai sensi del citato art. 38 disp. att. c.p.p. può permettere di ottenere la comunicazione "in chiaro" dell'intera sequenza dei numeri telefonici composti, senza il mascheramento delle ultime cifre (art. 20, comma 1, lett. g), l. n. 675/1996: cfr. *Provv.* del Garante del 5 ottobre 1998 e 5 ottobre 1999, in *Bollettino*, 1998, n. 6, p. 101 ss. e n. 10, p. 51 ss.), ma non crea nel titolare del trattamento destinatario della richiesta un obbligo di adempiere ed è, comunque, inidonea a giustificare un ricorso ai sensi dell'art. 29.

L'inammissibilità del ricorso, però, come ha tenuto a chiarire l'Autorità, ha lasciato impregiudicato il diritto di far valere in altra sede ulteriori istanze, in merito alle quali la legge n. 675/1996 non ha attribuito competenze al Garante, e non ha precluso inoltre all'abbonato di esercitare i diritti di cui all'art. 13 nei termini sopra indicati.

A tale riguardo, in riferimento alla particolare categoria di dati oggetto della controversia (dati relativi al traffico telefonico in entrata), il Garante ha osservato che la legge garantisce il diritto di accedere anche ai dati personali non ancora registrati (art. 13, comma 1, lett. c), n. 1), l. n. 675/1996) oltre che, ovviamente, ai dati disseminati in più luoghi o archivi, ovvero conservati in modo disorganico (casi in riferimento ai quali l'art. 17, comma 9, d.P.R. n. 501/1998 impone al titolare del trattamento di adottare opportune misure per agevolare l'accesso, tenendo presente la definizione di "dato personale" contenuta nell'art. 1 della legge).

L'accesso non può, invece, riguardare dati personali non ancora raccolti o che divengono materialmente esistenti solo a seguito di una specifica attività creativa notevolmente complessa e che potrebbe essere realizzata solo con la collaborazione di altri soggetti. Tali valutazioni vanno ovviamente condotte caso per caso, nel quadro delle condizioni tecniche del settore interessato.

Da ultimo, è intervenuto in materia il regolamento emanato con d.P.R. n. 77 dell'11 gennaio 2001 (in *G. U.* 29 marzo 2001). Fatte salve le disposizioni della normativa in materia di protezione dei dati personali e della vita privata, ai sensi della legge n. 675/1996 e del d.lg. n. 171/1998, tale regolamento ha disposto che le fatture debbono contenere dati particolareggiati, in modo da permettere la verifica e il controllo dei costi inerenti all'uso della rete telefonica pubblica fissa e dei servizi telefonici pubblici fissi.

Nella sua versione di base (definita con delibera dell'Autorità per le garanzie nelle comunicazioni) la fattura dettagliata deve essere fornita senza costi supplementari per l'utente, cui può eventualmente essere proposta una fattura ancora più particolareggiata a condizioni economiche ragionevoli o a titolo gratuito. Le chiamate gratuite per l'abbonato, comprese quelle dirette a numeri di emergenza, non sono indicate nella fattura dettagliata dell'abbonato (art. 28 d.P.R. n. 77/2001).

Constatato che il regolamento in questione interessa aspetti riguardanti la *privacy* e il trattamento dei dati personali nell'ambito delle telecomunicazioni, l'Autorità ha rilevato che tale decreto è affetto da un vizio che lo rende annullabile perché adottato senza che sia stato rispettato, come già avvenuto in altri casi segnalati, l'obbligo di consultazione del Garante previsto dalla legge sulla *privacy*. Al tempo stesso, il Garante ha interessato l'Autorità per le garanzie nelle comunicazioni per una valutazione comune sulla questione della formazione degli elenchi di telefonia mobile, al fine di prevenire incertezze operative e un diffuso contenzioso riguardo ai diritti degli interessati.

I dati sul traffico nel progetto di convenzione europea sulla cybercriminalità

La cybercriminalità è il rovescio della medaglia della Società dell'informazione. L'utilizzo di nuove tecnologie, infatti, mentre reca enormi benefici, offre la possibilità di perpetrare nuovi tipi di reati, ovvero di rendere più insidiosi i reati tradizionali sfruttando i nuovi strumenti disponibili. Il Consiglio d'Europa è impegnato dal 1997 nella stesura di un progetto di Convenzione internazionale sul *cybercrime*, che potrà essere sottoscritto anche da Paesi che non sono membri del Consiglio d'Europa. Sul progetto di Convenzione il Gruppo europeo dei Garanti si è espresso da ultimo con il Parere n. 4/2001, del 22 marzo 2001, che ha fatto seguito all'intervento del 7 settembre 1999 (Raccomandazione n. 3/1999), relativo alla conservazione dei dati sulle comunicazioni a fini giudiziari da parte dei fornitori di servizi Internet.

Nella sua più recente versione, il progetto di convenzione non contiene più, a differenza che in precedenza, un obbligo generale di sorveglianza consistente nella conservazione sistematica di tutti i dati relativi al traffico. Tuttavia, i Garanti europei hanno manifestato preoccupazione in riferimento alle disposizioni contenute nel progetto di Convenzione in merito ai dati di traffico, laddove, riferendosi alla conservazione e diffusione rapide di dati di traffico e di altra natura, non contemplano la possibilità, per la parte contraente cui sia presentata la richiesta di assistenza, di rifiutarsi di fornirla per motivi legati alla tutela dei dati (es.: inadeguatezza della tutela nel Paese di provenienza della richiesta), bensì soltanto per ragioni di ordine generale (ordine pubblico).

Allo stesso modo, l'imposizione dell'obbligo di conservare per almeno 60 giorni, su richiesta, dati informatici archiviati e dati relativi al traffico, al fine di consentire l'adozione di un provvedimento motivato delle autorità giudiziarie in ordine alla necessità dell'acquisizione ed alle modalità del loro utilizzo, comportano un onere per le imprese e per i privati cittadini interessati non coordinato con le disposizioni della direttiva 97/66/CE; preoccupazioni analoghe sono sollevate dalla disposizione che obbliga i fornitori di servizi a raccogliere o registrare, in tempo reale, nei limiti delle condizioni tecniche, dati relativi al traffico.

È evidente, in merito, che i consumatori non potranno nutrire una sufficiente fiducia nei servizi offerti dai fornitori, qualora non sia chiaro l'ambito dei soggetti legittimati ad accedere a dati e comunicazioni riservate, come e quando ciò sia possibile. Il Gruppo europeo ha espresso in merito l'auspicio, alla luce del forte impatto di tali disposizioni sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, che il Consiglio d'Europa consulti i propri esperti nel campo della tutela dei dati prima di definire la propria posizione sul progetto di Convenzione.

57. ELENCHI PUBBLICI E DIRITTI DEGLI INTERESSATI

In data 15 novembre 2000 il Garante ha avviato accertamenti nei confronti dell'Associazione politica nazionale Lista Marco Pannella, per verificare la liceità e la correttezza di alcuni trattamenti di dati relativi ad indirizzi di posta elettronica, in relazione a numerose segnalazioni che lamentavano la ricezione non gradita di messaggi per via telematica per finalità di comunicazione politica. Molti cittadini hanno fatto inoltre presente che non è stato loro possibile cancellarsi dagli elenchi dei destinatari secondo le modalità indicate nelle *e-mail* non gradite, o di essere stati costretti a reiterare invano più richieste di cancellazione.

All'esito dell'istruttoria, il Garante ha riscontrato che le segnalazioni pervenute erano fondate (Provv. 11 gennaio 2001).

L'Associazione ha fatto presente di aver reperito oltre 390.000 indirizzi di posta elettronica a scopo di comunicazione politica, utilizzando un software il quale archivierebbe indirizzi *e-mail* visualizzati su pagine *web* con suffissi ".it", ".org", ".com" e ".net" accessibili a chiunque in rete senza l'uso di *password* o di altri sistemi di protezione. La circostanza, peraltro, non ha trovato pieno riscontro in quanto, da accertamenti tecnici effettuati, in diversi casi non è stato possibile reperire in rete gli indirizzi di posta elettronica dei cittadini che hanno inviato una segnalazione.

A prescindere da tale aspetto, tuttavia, l'Autorità ha ritenuto che l'utilizzazione per finalità di comunicazione politica di tali indirizzi non fosse comunque lecita e corretta. Gli indirizzi di posta elettronica dei segnalanti non provenivano da "pubblici registri, elenchi, atti o documenti conoscibili da chiunque" (art. 12, comma 1, lett. c), l. n. 675/1996) e la loro utilizzazione nel caso in esame non poteva ritenersi consentita in mancanza di una previa manifestazione positiva di consenso da parte degli interessati (essendo altresì inoperanti gli ulteriori presupposti elencati nell'art. 12 della medesima legge).

Il Garante ha precisato che la previsione contenuta nella citata lettera c) si riferisce non a qualunque dato personale che sia di fatto consultabile da una pluralità di persone, ma ai soli dati personali che, oltre ad essere desunti da registri, elenchi, atti o documenti "pubblici" (in particolare in quanto formati o tenuti da uno o più soggetti pubblici), siano sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque, regime che può peraltro prevedere modalità o limiti temporali per il trattamento, da rispettare anche in caso di comunicazione o diffusione dei dati.

Le disposizioni richiamate, ha osservato il Garante, possono semmai trovare applicazione in altri casi – di stretta analogia – in cui un determinato registro, elenco, atto o documento sia reso ad esempio accessibile a chiunque sulla base della determinazione di un soggetto pubblico adottata in base ad una norma

(come avviene per l'elenco degli abbonati al servizio di telefonia vocale, per il quale l'Autorità per le garanzie nelle comunicazioni provvede affinché sia reso disponibile agli utenti: art. 17, comma 1, d.P.R. 19 settembre 1997, n. 318).

Una legittimazione all'utilizzazione pubblica di determinati dati può derivare anche dal consenso espresso degli interessati, manifestato in modo specifico ed informato.

Al contrario, le citate disposizioni non possono essere applicate in modo da poter trattare liberamente qualsiasi dato personale di natura non sensibile in base alla sola circostanza che il dato sia stato conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti.

L'utilizzazione per finalità di comunicazione politica degli indirizzi di posta elettronica dei segnalanti non poteva pertanto avvenire senza un preventivo consenso manifestato dagli interessati eventualmente anche nei confronti di più soggetti. Non era pertanto corretto gravare l'utente dell'onere di chiedere all'Associazione di interrompere l'invio dei messaggi non richiesti.

Parimenti, la conoscenza di fatto degli indirizzi che si realizza attraverso la partecipazione a *newsgroup* e *forum*, allo stesso modo, non poteva essere disgiunta dalla finalità per cui essa è stata resa possibile.

Contrastava, pertanto, con i principi di correttezza e finalità del trattamento raccogliere i dati che singoli utenti "lasciano" in un newgroup, forum, ecc. solo per le finalità di specifica discussione su determinati temi, hobbies, ecc., ed utilizzarli per altri scopi che nulla hanno a che vedere – anche indirettamente – con l'argomento per il quale l'utente partecipa ad una discussione più o meno "pubblica" ed indica il proprio recapito e le proprie generalità (art. 9, comma 1, lett. b), l. n. 675/1996).

Ad una conclusione analoga il Garante è giunto per i casi nei quali gli indirizzi di posta elettronica risultavano acquisiti dall'Associazione in quanto pubblicati su alcuni siti *web* per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale ed associativa.

La pubblicità di alcuni indirizzi resi conoscibili attraverso tali siti doveva essere collegata anch'essa, infatti, agli scopi per cui essa si verifica, non potendosi sostenere, anche in tali casi, che i dati posti a disposizione del pubblico per circoscritte finalità siano liberamente utilizzabili per l'invio generalizzato di *e-mail* anche quando queste non abbiano un contenuto commerciale o pubblicitario.

Il Garante ha poi rilevato che, a prescindere dalla liceità o meno dell'utilizzazione dei dati, l'Associazione era comunque tenuta a soddisfare senza ritardo le richieste di cancellazione ai sensi dell'art. 13 della legge n. 675/1996, curando un servizio attivo ed efficace di eliminazione degli indirizzi dei reclamanti.

Elenchi di abbonati ai servizi di telefonia mobile

Nell'ambito dei servizi di telefonia vocale, analogamente a quanto disposto dal d.P.R n. 318/1997, il recente regolamento emanato con d.P.R. n. 77 dell'11 gennaio 2001 (in *G.U.* 29 marzo 2001) ha previsto la possibilità di pubblicazione degli elenchi degli abbonati ai servizi di telefonia mobile. Il decreto prevede la possibilità per tali abbonati di decidere se e come (ad esempio, con il solo cognome, con l'indicazione dell'iniziale del nome proprio) comparire negli elenchi, escludendo altresì l'utilizzo delle stesse informazioni per fini pubblicitari (art. 20). È inoltre prevista la possibilità di verificare ed eventualmente di correggere i dati o di chiedere di essere radiati dagli elenchi.

Gli elenchi di tutti gli abbonati che non si siano espressamente opposti al fatto di esservi inseriti, con i numeri dei telefoni fissi e mobili e i numeri personali, dovrebbero essere messi a disposizione del pubblico su supporto cartaceo o elettronico, o su entrambi, in una forma approvata dall'Autorità per le garanzie nelle comunicazioni, e aggiornati periodicamente.

In proposito, il Garante ha richiesto immediatamente notizie ai fornitori di telefonia mobile sulle iniziative intraprese in ordine alla predisposizione di tali elenchi, alle modalità ipotizzate o utilizzate per informare le persone interessate e per garantire alle stesse un efficace esercizio dei diritti previsti dalla normativa sulla protezione dei dati personali, nonché dallo stesso regolamento che introduce la pubblicazione degli elenchi.

Constatato che il regolamento in questione interessa aspetti riguardanti la *privacy* e il trattamento dei dati personali nell'ambito delle telecomunicazioni, l'Autorità ha poi rilevato che tale decreto è affetto da un vizio che lo rende annullabile perché adottato senza che sia stato rispettato, come già avvenuto in altri casi segnalati, l'obbligo di consultazione del Garante previsto dalla legge sulla *privacy*.

Il Garante ha rilevato il rischio che il regolamento venga applicato, riguardo alla formazione degli elenchi, con modalità non idonee ad una piena protezione dei diritti degli interessati; al tempo stesso, ha interessato l'Autorità per le garanzie nelle comunicazioni per una valutazione comune al fine di prevenire incertezze operative e un diffuso contenzioso riguardo ai diritti degli interessati.

In particolare, come osservato dal Gruppo dei garanti europei nel Parere n. 7/2000, adottato il 2 novembre 2000, occorre rendere effettiva la possibilità per gli abbonati di decidere se essere inclusi o meno negli elenchi cartacei o elettronici; inoltre, vista la portata degli elenchi elettronici, gli abbonati dovranno essere informati sul loro eventuale uso ulteriore, ed i dati trattati dovranno essere limitati allo stretto necessario per identificare l'utente, senza rivelare informazioni strettamente "private".

Il Garante, come altre autorità per la protezione dei dati, si sta occupando anche di casi di "ricerche inverse" negli elenchi. Si tratta di nuovi servizi del mercato liberalizzato che offrono, con facilità e a basso costo, capacità estesa per il trattamento di tutte le informazioni contenute negli elenchi telefonici, anche attraverso l'associazione delle metodologie di ricerca a criteri multipli. Si rende, così, possibile risalire al nome e all'indirizzo dell'abbonato da un determinato numero, ovvero ai nomi e numeri telefonici degli abitanti in uno stesso quartiere, e così via.

L'orientamento del Gruppo europeo è quello di considerare tale nuova finalità degli elenchi come non compatibile con la finalità iniziale, considerando il trattamento illecito a meno che l'interessato non abbia manifestato un proprio specifico consenso al trattamento dei dati personali per tali nuove finalità. Il Gruppo ha adottato una posizione comune in merito, nel Parere n. 5/2000, approvato il 13 luglio 2000.

Un altro aspetto rischioso è legato alla possibilità per chiunque di modificare gli elenchi su supporto elettronico: si rende pertanto necessario garantire che le trasmissioni di elenchi rispettino le scelte espresse gratuitamente dagli utenti e dagli abbonati presso il fornitore iniziale. Inoltre, la possibile cessione dei dati sotto forma di CD ROM solleva ulteriori problemi legati alla durata dell'autorizzazione al trattamento, che deve essere determinata in modo da non consentire l'uso di dati non più utilizzabili in relazione alle scelte espresse dagli interessati.

La stessa proposta di revisione della direttiva 97/66/CE, partendo dall'implicito presupposto che non è opportuno l'inserimento in via automatica degli utenti dei servizi di telefonia mobile o dei servizi di comunicazione elettronica (posta elettronica) in elenchi pubblici, prevede che siano gli abbonati a decidere se vogliono figurare in un elenco pubblico e specificare quali dei loro dati personali debbano esservi riportati. Per tener conto delle varie possibilità di utilizzo degli elenchi pubblici, in particolare di quelli elettronici, è necessario informare gli abbonati circa gli scopi per i quali gli elenchi sono stati predisposti e garantire che il consenso ad essere inclusi venga prestato sulla base di un'accurata ed esauriente informazione circa le modalità di utilizzo dei propri dati personali.

58. SERVIZI DI LOCALIZZAZIONE

Nelle reti di comunicazioni mobili odierne, i dati relativi alla localizzazione dell'utente sono già disponibili. Questo tipo di informazione è necessaria per consentire la trasmissione di comunicazioni che sono originate e destinate ad un utente che non ha una postazione fissa. Si tratta di un informazione "grezza" sulla localizzazione, che è in realtà un sottoprodotto del servizio di trasmissione delle comunicazioni, e deve ritenersi disciplinato dalla vigente direttiva 97/66/CE e dal d.lg. n. 171/1998, nella parte riguardante i dati sul traffico.

Esiste tuttavia un nuovo tipo di servizi forniti dalle reti cellulari e satellitari che consentono di individuare esattamente l'ubicazione dell'apparecchiatura terminale dell'utente mobile. In questo caso i dati relativi alla localizzazione sono molto più precisi e vengono specificamente sottoposti a trattamento da parte dei fornitori della rete allo scopo di fornire servizi a valore aggiunto agli utenti e agli abbonati.

Nel corso del 1999, il Garante ha avviato le procedure di accertamento relative al delicato problema della "localizzazione" degli apparecchi di telefonia mobile, con la richiesta indirizzata ai gestori italiani di servizi di telecomunicazioni mobili di dettagliate informazioni (v. Relazione per l'anno 1999, p. 66).

L'Autorità si è riservata di effettuare una valutazione complessiva del problema alla luce dei chiarimenti, anche tecnici, forniti dai gestori, in modo da verificare la presenza di eventuali irregolarità rispet-

to alla normativa sulla protezione dei dati personali e prospettare misure idonee ed accorgimenti per la tutela dei diritti degli interessati.

Nel maggio 2000, con riferimento alle notizie apparse sui principali organi di informazione concernenti l'avvio di programmi di localizzazione per telefoni mobili, resi disponibili in Internet e via rete mobile, sulla base della tecnologia *CellPoint Finder* (che consentirebbe di localizzare con precisione i detentori degli apparecchi di telefonia cellulare), il Garante, in collaborazione con i fornitori/gestori, ha avviato un'ulteriore procedura di accertamento, chiedendo alla società interessata particolareggiate informazioni riguardo alle caratteristiche del programma in questione, ai fornitori di servizi ai quali esso sia stato già fornito sul territorio nazionale, alle modalità di conservazione dei dati, in ordine agli strumenti a disposizione dell'utente per disattivare il programma, nonché alle tecniche ideate per informare i singoli abbonati ed utenti interessati al servizio ed acquisirne il consenso.

Nell'ambito del procedimento, inoltre, il Garante ha richiesto ai principali gestori di telefonia mobile di fornire elementi circa: la tipologia dei dati veicolati sulle infrastrutture di rete dai quali è possibile individuare, direttamente o tramite ulteriori elaborazioni, la posizione geografica delle apparecchiature terminali mobili; le precise modalità di acquisizione, registrazione ed elaborazione dei dati, con particolare riferimento al grado di precisione della localizzazione spaziale delle apparecchiature terminali e alla persistenza in qualunque modo nel sistema informativo dei dati grezzi o dell'elaborazione su di essi svolta; l'esistenza o la previsione di accordi con altre società per la fornitura di servizi di localizzazione delle apparecchiature terminali, anche attraverso la predisposizione di idonei programmi informatici. L'Autorità ha inoltre convocato per un'audizione le società interessate ed altri qualificati rappresentanti del settore per procedere ad un approfondito esame congiunto degli elementi forniti.

In merito, la Commissione europea, nel preambolo alla proposta di revisione della direttiva n. 97/66/CE, ha espresso la preoccupazione che la capacità di trattare dati estremamente precisi in ordine all'ubicazione dell'utente nelle reti di comunicazione mobili porti ad una situazione in cui questi resti sotto sorveglianza permanente, al punto da trovarsi costretto a non utilizzare affatto detti servizi di comunicazione pur di tutelare la propria vita privata. La proposta precisa che i dati relativi alla localizzazione dell'utente possono essere utilizzati esclusivamente con il consenso informato dell'abbonato, prescrivendo che l'utente deve anche disporre di uno strumento semplice per rifiutare temporaneamente il trattamento dei dati relativi alla localizzazione, analogamente a quanto previsto per l'identificazione della linea chiamante. Le uniche deroghe a tale principio generale sono l'utilizzo dei dati relativi alla localizzazione dell'utente da parte dei servizi di emergenza e le deroghe vigenti ai fini della sicurezza pubblica e delle indagini di natura penale.

Sul punto si è recentemente pronunciato anche il Gruppo dei Garanti europei, nel Parere n. 7/2000 del 2 novembre 2000, rilevando che in linea di principio i dati relativi all'ubicazione non devono essere sottoposti a trattamento per la fornitura di servizi a valore aggiunto, ma eccezionalmente possono essere sottoposti a trattamento per finalità chiaramente specificate che richiedano tecnicamente l'uso dei dati relativi all'ubicazione e sempre che vengano messi in atto controlli di sicurezza consoni ai rischi per la vita privata. In considerazione del carattere "sensibile" dei dati in relazione alla libertà di movimento del cittadino e del fatto che non si tratta di dati necessari per stabilire la comunicazione, l'utente/abbonato deve avere il pieno controllo sulle finalità e modalità del trattamento cui essi vengono sottoposti con la possibilità, qualora sia interessato, di consentire liberamente al trattamento dei dati sull'ubicazione in relazione ad ogni fornitura di un servizio a valore aggiunto e con necessità di integrare l'attuazione tecnica di tale diritto nell'apparecchiatura dell'abbonato e non nella rete, come avviene invece nel caso dell'identificazione della linea chiamante.

SICUREZZA DEI DATI E DEI SISTEMI

59. LO STATO DELL'ARTE NELL'APPLICAZIONE DELLE MISURE DI SICUREZZA

La legge del 31 dicembre 1996, n. 675 ha assegnato una precisa base giuridica agli obblighi relativi alle misure di sicurezza che riguardano il trattamento automatizzato e non automatizzato di dati.

La disciplina prevede il dovere di custodire e controllare i dati trattati mediante l'adozione di idonee e preventive misure di sicurezza tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 15, comma 1, l. n. 675/1996); la mancata predisposizione di tali misure comporta la responsabilità per danni eventualmente cagionati (art. 18, l. n. 675/1996). Lo stesso art. 15, inoltre, ai commi 2 e 3, individua tramite un apposito regolamento le *"misure minime di sicurezza"* la cui violazione costituisce sicura esposizione al rischio di lesione del diritto alla tutela dei dati personali e comporta l'applicazione di sanzioni di carattere penale (art. 36, l. n. 675/1996).

Il previsto regolamento, emanato con il d.P.R. 28 luglio 1999, n. 318, entrato in vigore il 29 marzo 2000, comporta per il titolare del trattamento non solo l'obbligo di adottare le misure minime previste al comma 2 dell'art. 15 della legge n. 675/1996, ma anche di custodire e controllare i dati adottando le idonee e preventive misure di sicurezza di cui all'art. 15, comma 1.

L'Autorità, con deliberazione del 29 maggio 2000 (in *Bollettino* n. 13, p. 30), ha chiarito che nei confronti dei soggetti interessati non sussiste alcun obbligo di comunicare sistematicamente al Garante le determinazioni eventualmente adottate in attuazione del regolamento ed ha precisato che gli atti previsti dal regolamento, come il documento programmatico sulla sicurezza o la designazione dei responsabili e degli incaricati del trattamento, devono essere esibiti all'Autorità solo a seguito di un'eventuale e specifica richiesta in sede di ispezione o di controllo.

Successivamente, la legge 3 novembre 2000, n. 325 recante: *"Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste all'art. 15 della legge 31 dicembre 1996, n. 675"*, ha consentito a coloro i quali non avevano adottato le misure minime entro il predetto termine del 29 marzo 2000 di beneficiare, seppure non in modo automatico, ma adempiendo a determinate prescrizioni, di un differimento del termine fino al 31 dicembre 2000. Tale differimento, non direttamente rilevante ai fini della responsabilità civile per danno derivante da mancata o inidonea adozione di misure di sicurezza, ha permesso di prorogare al 31 dicembre 2000 l'applicabilità delle previste sanzioni penali (art. 36, l. n. 675/1996). Per contribuire alla corretta applicazione della legge il Garante è intervenuto, con un provvedimento del 5 dicembre 2000 (in *Bollettino* n. 14/15, p. 19), precisando le modalità applicative per l'adozione del documento previsto dall'art. 1 della legge n. 325/2000 con un atto avente data certa.

60. PRIMI CASI APPLICATIVI

Il Garante nel corso dell'anno 2000 ha affrontato l'argomento delle misure minime di sicurezza in varie occasioni, sia rispondendo a quesiti, sia formulando pareri su gli atti cui è richiesta la consultazione dell'Autorità.

In un parere pronunciato su richiesta della Lega italiana per la lotta all'AIDS (LILA) (in *Bollettino*, n. 11/12, p. 7) ha ricordato che gli organismi sanitari sono tenuti al rispetto dei principi di correttezza e di pertinenza richiesti per il trattamento di dati sensibili da parte dei soggetti pubblici, e devono adottare specifiche cautele a tutela della riservatezza degli interessati. Tra queste assume carattere di priorità la separazione dei dati anagrafici da quelli sanitari e la cifratura delle informazioni contenute in elenchi o banche dati. Per quanto riguarda, invece, il regolamento sulle misure minime di sicurezza, l'Autorità ha precisato che esso impone l'adozione, da parte di chi utilizza i dati, di idonee cautele e

accorgimenti di tipo organizzativo e tecnico, allo scopo di evitare la distruzione, la perdita e l'uso illecito delle informazioni raccolte, elaborate e conservate. Il Garante ha richiamato, infine, l'attenzione sull'accesso ai dati "*particolari*" (sensibili e giudiziari) che richiede al titolare o, se designato, al responsabile del trattamento l'obbligo di rilasciare specifiche autorizzazioni agli incaricati del trattamento o della manutenzione dei dati sensibili o di carattere giudiziario. Il rispetto di questi principi dovrà essere ancora più accurato quando si trattano informazioni inerenti all'AIDS o all'infezione da HIV, dalla cui circolazione può derivare un grave pregiudizio per la vita privata e la dignità personale degli interessati.

L'Autorità garante, in un provvedimento del 28 febbraio 2000 (in *Bollettino*, n. 11/12, p. 9), ha fornito analoghe raccomandazioni agli uffici giudiziari, richiamando il rispetto dei principi di correttezza e di pertinenza in base ai quali possono essere trattati e diffusi i soli dati necessari al perseguimento delle finalità istituzionali, precisando altresì che, al fine di tutelare la sicurezza dei dati raccolti, ciascun ufficio giudiziario, come ogni altra amministrazione, è tenuto al rispetto del regolamento in materia di misure minime di sicurezza e all'adozione delle idonee cautele organizzative e tecniche in modo da ridurre al minimo i rischi di distruzione dei dati e di accessi non autorizzati.

Il Garante, inoltre, nell'esprimere il prescritto parere allo schema di d.P.R. concernente "*Disposizioni relative all'uso di strumenti informatici e telematici nel processo civile*" (v. *Provv.* del 4 ottobre 2000, in *Bollettino*, n. 14/15, p. 13) ha ravvisato la necessità che nello stesso venisse effettuato un espresso richiamo all'art. 15 della legge n. 675/1996 e al connesso d.P.R. n. 318/1999, in quanto il suddetto provvedimento è applicabile ai trattamenti di dati personali effettuati per ragioni di giustizia presso uffici giudiziari (art. 4, comma 2, l. n. 675/1996). Nel medesimo provvedimento il Garante ha richiamato la necessità di precisare che i dati personali acquisiti presso i difensori delle parti a seguito di accesso al sistema informatico civile o, comunque, di ricezione di atti e documenti per via telematica, siano utilizzati in modo lecito e corretto da parte dei vari soggetti che vi possono accedere (sostituti ausiliari, tirocinanti, praticanti, colleghi operanti presso studi associati, associazioni di professionisti; personale amministrativo, ecc.). In tale occasione il Garante ha ricordato di aver impartito in proposito alcune prescrizioni nell'autorizzazione generale n. 4/2000, rilasciata ai sensi dell'art. 22, l. n. 675/1996 in tema di trattamento dei dati sensibili da parte di liberi professionisti. Nuove regole potrebbero essere adottate in materia in occasione del varo del codice di deontologia per il trattamento di tutti i dati personali trattati a fini di indagine difensiva e di difesa di un diritto in sede giudiziaria, promosso dal Garante con provvedimento del 10 febbraio 2000 e attualmente in fase di predisposizione.

Da ultimo l'Autorità, in data 23 febbraio 2001 (v. parere, in *Bollettino*, n. 17, p. 32), nel rispondere ad un quesito posto da dipendenti di una società, ha chiarito che, ai sensi del regolamento sulle misure minime di sicurezza, non è possibile vietare ai propri dipendenti che devono utilizzare gli strumenti informatici servendosi di *password* loro singolarmente assegnate, l'autonoma modifica delle stesse. Il Garante ha infatti ricordato che la parola chiave per l'accesso ai dati personali deve essere autonomamente sostituibile ed ha suggerito anche modalità per la prevista comunicazione della sostituzione al soggetto preposto alla sua custodia.

I TRASFERIMENTI ALL'ESTERO DI DATI

61. PAESI CHE OFFRONO UNA PROTEZIONE ADEGUATA

La Commissione europea ha constatato con due decisioni che alcuni Paesi terzi garantiscono un livello di protezione adeguato. A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

Queste decisioni non eliminano però la rilevanza dell'attività delle autorità di garanzia dei Paesi membri, poiché queste possono esercitare i loro poteri per sospendere il trasferimento verso l'estero nel caso in cui, ad esempio, la competente autorità del Paese terzo abbia accertato che il destinatario dei dati viola le norme vigenti in materia di protezione dei dati, ovvero in altre ipotesi assai complesse, nelle quali, tra l'altro, una violazione sia molto probabile, si possano ritenere inadeguate e non tempestive le misure che la competente autorità del Paese terzo intenda adottare e il trasferimento comporti il rischio imminente di gravi danni per gli interessati.

Il 26 luglio 2000 la Commissione ha adottato la decisione 2000/519/CE, riguardante l'adeguatezza della protezione dei dati personali in Ungheria (*G.U.C.E.* n. L 215 del 25 agosto 2000), sulla base del parere espresso nel 1999 dal Gruppo di lavoro previsto dall'art. 29.

La Commissione ha considerato in particolare che il principio della tutela della vita privata è contemplato dalla costituzione ungherese; che l'Ungheria ha ratificato la Convenzione del Consiglio d'Europa sulla protezione delle persone riguardo al trattamento automatizzato di dati di carattere personale (Convenzione n. 108/1981 del Consiglio d'Europa), volta a rafforzare la tutela dei dati personali e ad assicurare la libera circolazione tra le parti contraenti; che le norme vigenti in quel Paese incorporano i principi fondamentali necessari per assicurare un adeguato livello di protezione delle persone fisiche; che l'applicazione di tali norme è garantita dai ricorsi giurisdizionali, nonché dal controllo indipendente esercitato dal commissario nominato dal Parlamento.

Da notare che nei confronti dell'Ungheria la decisione riguarda tutti i trasferimenti di atti personali, mentre la decisione di seguito menzionata nei confronti degli Usa è relativa ai trasferimenti verso imprese ed organizzazioni aderenti al *"Safe Harbor"*.

Per vari aspetti simile è la decisione n. 2000/518/CE relativa alla Svizzera, resa in pari data (26 luglio 2000, in *G.U.C.E.* n. *L 215* del 25 agosto 2000) dalla Commissione: anche in questo caso la Commissione, conformemente al parere del Gruppo di lavoro previsto dall'art. 29, ha ritenuto adeguato il livello di protezione offerto da quell'ordinamento per tutte le attività rientranti nel campo di applicazione della direttiva, dopo aver considerato la costituzione, l'adesione alla Convenzione n. 108/1981 sopra menzionata, le norme federali e quelle cantonali e l'indipendenza dell'autorità di controllo competente in materia.

Non ancora a livello di Commissione, bensì di Gruppo di lavoro previsto dall'art. 29, sono invece le valutazioni relative a Canada ed Australia.

La prima, del 26 gennaio 2001 (parere n. 2/2001), in qualche misura interlocutoria, nella sostanza segnala alla Commissione alcuni aspetti essenziali dell'ordinamento canadese in materia di protezione di dati personali. Anzitutto si fa presente che le norme relative al trattamento effettuato da privati, contenute nel *Personal Information and Electronic Documents Act*, saranno pienamente in vigore nel 2004 e che il loro ambito di applicazione è relativo solo a soggetti privati che trattano dati personali nel corso di attività a scopo di lucro.

Si è poi richiamata l'attenzione sul rapporto tra norme federali e norme delle diverse province, attesa la non omogeneità della disciplina, occorrendo pertanto verificare l'opportunità di una valutazione dell'adeguatezza con riferimento ai singoli ordinamenti; si è poi sottolineata l'esigenza di monitorare l'evoluzione normativa riguardante i dati sensibili, valutando favorevolmente iniziative volte ad assicurare una più organica tutela degli stessi, anche con riferimento al loro trasferimento dal Canada ad altro Paese.

Il medesimo gruppo di lavoro, col parere 3/2001 del 26 gennaio 2001, ha invece ritenuto non ancora adeguata la protezione offerta dall'ordinamento australiano, o, più precisamente, ha indicato alcuni punti critici da superare per giungere ad una valutazione di adeguatezza.

Tra i punti va ricordata la non applicazione ad alcune materie, segnatamente alle piccole imprese ed ai dati dei dipendenti, degli strumenti normativi di protezione dei dati (*Privacy Act, Privacy Amendment*), ancorché questi possano essere di natura sensibile. In particolare non è chiara la definizione australiana di "piccola impresa", che diventa quindi potenzialmente di vastissima applicazione. È inoltre consentito in termini piuttosto ampi che l'informativa agli interessati sia fornita successivamente alla raccolta dei dati medesimi e per i dati sensibili le limitazioni relative alla raccolta non escludono che possa farsene un uso ulteriore, per scopi diversi da quelli originari. Gli strumenti di tutela, inoltre, non risultano applicabili a soggetti che non siano cittadini australiani o che non risiedano in Australia.

Questa valutazione non favorevole risulta ovviamente modificabile in futuro ma, al di là delle specifiche considerazioni sulle quali si basa, appare senz'altro significativa della complessità e delicatezza delle analisi richieste.

62. "*SAFE HARBOR*"

Di rilievo, anche nel corso del 1999 e del 2000, è stata l'attività svolta dal Garante in seno ad organismi comunitari ed internazionali, relativamente ai trasferimenti di dati verso Paesi terzi.

È nota, al riguardo, la disciplina contenuta nell'art. 25 della direttiva 95/46/CE secondo la quale lo stato di destinazione deve presentare un livello di protezione "adeguata", da valutarsi con riferimento a tutte le circostanze, segnatamente alla natura dei dati, protezione in mancanza della quale gli Stati membri devono adottare tutte le misure per impedire il trasferimento di dati della stessa natura verso tale Paese, a meno che ricorrano altri presupposti che permettano di trasferire comunque i dati (l'art. 26 prevede ad esempio che il trasferimento possa avvenire anche verso Paesi la cui legislazione non presenti un adeguato livello di protezione, in particolare quando l'interessato abbia manifestato il suo consenso, o quando il trasferimento sia accompagnato da clausole contrattuali idonee ad assicurare tale protezione).

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

In questo quadro si è collocata l'attività del Garante in seno agli organismi comuni previsti dalla citata direttiva 95/46: il Gruppo consultivo di cui all'art. 29 (composto da un rappresentante di ciascuna autorità nazionale e da un rappresentante della Commissione, e presieduto nel periodo considerato dal Presidente del Garante italiano), al quale, tra l'altro, spetta formulare un parere sul livello di tutela nella Comunità e nei Paesi terzi; il comitato di cui all'art. 31, composto da rappresentanti degli Stati membri, è presieduto da un rappresentante della Commissione.

La presente esposizione sintetizza ed in parte rielabora il materiale disponibile sul sito Internet della competente Direzione generale della Commissione (*http://europa.eu.int/comm/internal-market*), cui si fa doveroso rinvio per ogni dettaglio.

Anche quest'anno, nell'ambito di quest'ultimo gruppo il Garante ha operato in continuo raccordo con il Ministero della giustizia, che rappresenta il Governo, nell'espressione di un orientamento comune al Governo ed all'Autorità di garanzia.

Si riassumono di seguito i momenti essenziali di tale attività, con costante riferimento ad alcuni atti di particolare importanza, che in qualche misura indicano la rilevanza non solo comunitaria della disciplina sulla protezione dei dati personali e quindi chiamano le autorità garanti, dopo un'impegnativa fase di elaborazione, ad una non meno rilevante funzione di verifica nell'applicazione di tali strumenti, volti ad assicurare un più ampio ambito di applicazione dei principi e delle regole fondamentali contenuti nella normativa comunitaria in materia.

Per quanto riguarda il trasferimento di dati negli U.S.A., il 26 luglio 2000 la Commissione europea ha adottato una decisione (n. 2000/520/CE in *G.U.C.E. n. L 215* del 25 agosto 2000) che constata che il dispositivo di *"Safe Harbor"* approntato dalla Commissione federale per il commercio degli Stati Uniti assicura un adeguato livello di protezione dei dati personali trasferiti dall'Unione europea.

Il *"Safe Harbor"* costituisce un insieme di principi a garanzia del trattamento dei dati personali uniti alla previsione di alcuni sistemi per assicurare il rispetto di tali principi. L'adesione al *"Safe Harbor"* è