53 Attività di cooperazione con l'Autorità per le garanzie nelle comunicazioni

Il 20 febbraio 2003 si è tenuta una riunione congiunta tra il collegio del Garante e quello dell'Autorità per le garanzie nelle comunicazioni, nel corso della quale sono state messe a punto alcune linee di intervento comune, anche al fine di intensificare, nell'ambito delle rispettive aree di competenza, le forme di cooperazione istituzionale già avviate in precedenza (v. comunicato stampa del 20 febbraio 2003).

Nel corso dei lavori sono state sottolineate l'importanza e la novità istituzionale rappresentate dalla proficua collaborazione già realizzatasi su questioni di interesse comune (elenchi telefonici, servizi di telecomunicazione non richiesti etc.) e la necessità di procedere a forme ancor più strette di cooperazione.

In vista di questo obiettivo le due Autorità hanno convenuto di rendere sistematico lo scambio di informazioni e di documentazione tra gli uffici, nonché di approfondire, a breve termine, un protocollo che dia attuazione alle linee generali tratteggiate nell'incontro e alle ipotesi di collaborazione proposte.

Nell'ambito di tale collaborazione, l'Ufficio del Garante ha avuto modo di svolgere una prima valutazione, del tutto preliminare, sulla possibile realizzazione in Italia del progetto noto come *"e-number"* o *"Enum"*, con riferimento ad una consultazione pubblica promossa dall'Autorità per le garanzie nelle comunicazioni. Tale sistema permette di creare connessioni fra indirizzi *Internet* e numeri telefonici, al fine di realizzare un numero identificativo universale che consente di instradare il traffico verso i diversi recapiti dell'interessato (telefono fisso, mobile, indirizzo di posta elettronica, ecc.).

Il sistema Enum, già allo studio in altri Paesi europei, ha suscitato notevoli perplessità in ordine alle possibili implicazioni che la sua introduzione potrebbe avere in relazione alla sfera di riservatezza degli interessati.

L'Autorità per le garanzie nelle comunicazioni ha così avviato una consultazione pubblica sull'introduzione del protocollo *Enum* rivolgendo particolare attenzione anche agli aspetti riguardanti la sicurezza e la protezione dei dati personali (v. *Comunicato* pubblicato nella G.U. n. 95 del 24 aprile 2003).

Trattamento di dati personali in Internet

54 Profili generali

Gli sviluppi relativi alla protezione dei dati personali in materia di reti telematiche sono strettamente connessi alla continua evoluzione del settore, come testimoniano le diverse e sempre crescenti segnalazioni, richieste di chiarimenti e quesiti che provengono giornalmente a questa Autorità.

Nel corso del 2002, il Garante ha proseguito nell'opera di costante monitoraggio dell'evoluzione tecnica del settore, stabilendo, in particolare, forme opportune di consultazione con i diversi operatori, in modo da poter promuovere l'adozione di garanzie adeguate sia sul piano della prassi operativa, sia su quello normativo, anche provvedendo a sollecitare l'adozione delle misure necessarie alle autorità pubbliche competenti.

D'altronde, le numerose problematiche esaminate hanno confermato come un'altra caratteristica peculiare della maggior parte dei trattamenti realizzati in tale ambito sia quella di poter prescindere, in larga misura, dai confini nazionali e, quindi, dalla legislazione sulla protezione dei dati applicabile all'interno di essi.

Proprio in ragione di tali peculiarità, sono destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici previsti dal d.lg. n. 467/2001, nonché l'emanando testo unico più volte richiamato.

Sono stati avviati i lavori preliminari per la redazione del codice deontologico relativo ai trattamenti di dati personali *"effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica"*.

In questo quadro, è utile ricordare che la direttiva 2002/58/CE (da recepirsi entro il 31 ottobre p.v.), relativa al *"trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"*, nel modificare la direttiva 97/66/CE, si pone l'obiettivo di adeguare la disciplina sulla tutela dei dati personali agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica. Ciò, adottando un approccio "tecnologicamente neutro", mirante, cioè, a predisporre una normativa valida ed applicabile a tutte le forme di comunicazione elettronica realizzate per via telefonica, su *Internet* o su altri mezzi.

Nelle more dell'adozione del testo unico e del codice sopra richiamati, nonché della trasposizione in Italia della direttiva citata, l'Autorità ha comunque già fornito alcuni chiarimenti in ordine a diverse problematiche sottese alla materia.

Oltre a offrire alcune prime precisazioni in merito al possibile esercizio, sulla rete *Internet*, dei diritti di cui all'art. 13 della legge 675/1996, il Garante ha concluso l'esame e sta per adottare un provvedimento di carattere generale che fornisce alcuni suggerimenti ed indicazioni agli operatori del settore ed agli utilizzatori della rete in materia di invio di posta elettronica indesiderata (c.d. "*spamming*").

55 Comunicazioni indesiderate

Spamming su Internet

Il Garante si è più volte occupato della problematica relativa all'invio di messaggi di posta elettronica non sollecitati di natura prevalentemente pubblicitaria.

Come già evidenziato in passato (v. *Relazione 2001*, p. 88), la direttiva 2002/58/CE ha recepito, quale sistema di regolamentazione del problema, il principio secondo cui l'invio di messaggi di posta elettronica di carattere pubblicitario è subordinato all'espresso consenso dell'interessato ("*opt-in*").

Il Garante ha espresso un positivo avviso in ordine alla predetta opzione (v. Newsletter, 12 - 18 febbraio 2001). D'altronde, come chiarito dal Garante nel corso del 2002, la legge 675/1996 (art. 11), il d.lg. 171/1998 (art. 10) ed il d.lg. 185/1999 (art. 10, comma 1) già riconducono la fattispecie in esame alla regola del consenso preventivo ed esplicito.

In tal senso, il Garante si è espresso anche in occasione delle decisioni adottate in merito ai ricorsi presentati da alcuni utenti, ai sensi dell'art. 29 della legge 675/1996 (*Provv.* 25 giugno, 25 luglio e 30 settembre 2002). Accertata la fondatezza delle pretese dei ricorrenti, l'Autorità ha provveduto a bloccare le banche dati delle relative società che avevano inviato numerose *e-mail* pubblicitarie e promozionali senza aver acquisito, in via preventiva, il consenso informato degli interessati.

Il blocco dei trattamenti connessi alle predette banche dati si è reso necessario anche per impedire che il trattamento illecito e non corretto dei dati personali potesse estendersi ad un elevato numero di cittadini i cui indirizzi di posta elettronica erano presenti negli archivi delle società medesime.

Svariati altri provvedimenti di blocco sono stati adottati in altre successive circostanze.

In questo quadro, il Garante è altresì in procinto di adottare un provvedimento di carattere generale volto ad offrire altre indicazioni in materia.

L'Autorità ha, già più volte ricordato che nei casi di specie non può essere invocato l'art. 12, comma 1, lett. *c)*, della legge 675/1996, il quale esonera il titolare dal richiedere il consenso dell'interessato ove i dati relativi a quest'ultimo siano provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Infatti, questa disposizione si riferisce esclusivamente agli elenchi o ai registri per i quali è previsto uno specifico regime giuridico di piena conoscibilità da parte di chiunque, e non è, quindi, applicabile ai casi in cui un determinato dato possa essere consultato dal pubblico per mere circostanze di fatto (ad esempio: raccolta su siti *web* o presso *newsgroup* ove erano disponibili per diverse finalità).

Quanto, poi, al consenso all'invio di messaggi pubblicitari e al connesso obbligo di informativa nei confronti dei destinatari, il Garante ha sottolineato che il consenso, oltre a dover essere manifestato liberamente e documentato per iscritto, secondo le previsioni del già citato art. 11 della legge, deve essere preventivo, esplicito ed espresso in forma differenziata rispetto alle varie categorie di prodotti offerti.

La circostanza, poi, che l'indirizzo di posta elettronica sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti, non lo rende liberamente utilizzabile e non autorizza, comunque, l'invio di informazioni di qualunque genere, anche se non specificamente a carattere commerciale o promozionale senza un preventivo consenso.

Ed ancora, con riguardo al diritto degli interessati di richiedere la cessazione dell'invio di messaggi pubblicitari indesiderati, il Garante ha più volte sottolineato che, indipendentemente dal rapporto esistente tra i mittenti ed i destinatari dei messaggi pubblicitari, deve essere data sempre a questi ultimi la possibilità di far valere il proprio diritto di opporsi, in tutto o in parte, al trattamento dei dati medesimi ai fini di informazione commerciale. La richiesta per l'esercizio di tale diritto può essere avanzata senza formalità, ad esempio tramite posta elettronica o anche verbalmente (art. 17, comma 1, d.P.R. n. 501/1998). In ogni caso, tali diritti devono poter essere esercitati gratuitamente ed in maniera agevole.

Nel caso di esercizio dei diritti di cui al richiamato art. 13, i titolari o i responsabili dagli stessi designati, sono tenuti a fornire all'interessato una risposta completa ed esaustiva, con riferimento a tutti gli elementi richiesti.

Nomi a dominio

Durante il periodo di riferimento sono inoltre pervenute a questa Autorità diverse segnalazioni in ordine alla protezione dei nomi a dominio, con specifico riguardo ai dati relativi ai soggetti che registrano siti *web* ("*registrant*") nonché alla pubblicazione di alcuni dati personali sulla rete.

Al riguardo, il Garante ha svolto alcune indagini conoscitive in merito alle modalità ed alle regole di registrazione dei nomi a dominio in Italia, al fine di predisporre un provvedimento generale.

56 Il codice deontologico

Come accennato nel paragrafo relativo ai profili generali, nonché nella *Relazione 2001* (p. 89), è prossima l'adozione del codice sui trattamenti dei dati personali *"effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica"*.

Ed infatti, sulla base di quanto stabilito dal d.lg. 467/2001, il Garante ha promosso, nell'ambito di una generale attività collaborativa con i diversi operatori del settore, la sottoscrizione del predetto codice di deontologia e buona condotta, con il dichiarato scopo di fornire *"i criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di telecomunicazione gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento"*, nell'ottica di *"una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 9 della legge 31 dicembre 1996, n. 675"*.

A tal riguardo, è utile sottolineare che, al pari di quanto previsto per i codici sui trattamenti realizzati a fini storici o statistici, tale codice assumerà il ruolo di fonte dell'ordinamento, come, d'altronde, dispone l'art. 20 del d.lg. 467 cit., il quale testualmente recita: *"il rispetto delle disposizioni in essi contenute costituisce condizione essenziale per la liceità del trattamento dei dati"*.

57 Pubblicazione di fotografie sui siti *web*

Sono pervenute, nel 2002, segnalazioni concernenti la liceità della pubblicazione -anche su siti *web*- di fotografie e immagini che ritraggono persone.

Sul punto merita ricordare un provvedimento del Garante nel quale, tra i vari aspetti esaminati, sono stati forniti chiarimenti in ordine agli adempimenti gravanti sui fotonegozianti e sulle società (che di regola operano sulla base di specifici accordi negoziali con i primi) i quali offrano al cliente, oltre al tradizionale servizio di sviluppo e stampa dei rullini, anche la visione delle proprie fotografie su un apposito sito *web* (*Provv.* 16 maggio 2002, in *Bollettino* n. 28).

In tale occasione il Garante, oltre a ribadire il principio in base al quale le fotografie possono contenere immagini e informazioni qualificabili alla stregua di dati personali (art. 1, comma 2, lett. c), l. n. 675/1996, ha richiamato l'obbligo, per i titolari di siffatto trattamento, di fornire al cliente un'idonea informativa, anche oralmente (art. 10, comma 1, l. n. 675/1996), sin dal momento della richiesta della prestazione e, quindi, della consegna del rullino. Ciò al fine di porre l'interessato in condizione di scegliere in modo consapevole la particolare modalità del servizio di sviluppo desiderato e di conoscere in anticipo le modalità del peculiare trattamento. Tale esigenza non può ritenersi sufficientemente soddisfatta -ha precisato il Garante- tramite la mera esibizione o consegna di materiale promozionale ai clienti. Né l'informativa sui dati personali può considerarsi implicita nel mero pagamento di un prezzo diverso rispetto a servizi tradizionali.

Il Garante ha altresì richiamato l'attenzione sulla necessità che in tali casi siano adottate le specifiche misure di sicurezza volte a prevenire taluni rischi, tra i quali quelli di distruzione o perdita dei dati personali trattati o di accesso non autorizzato (art. 15 l. n. 675/1996 e d.P.R. 28 luglio 1999, n. 318); obblighi che, con riferimento al peculiare trattamento in questione, assumono rilievo in relazione alle diverse fasi del processo di realizzazione del servizio, nonché ai diversi soggetti in esso coinvolti (i negozianti e gli altri addetti allo sviluppo delle fotografie; il gestore del *server* nel quale viene conservato il *file* contenente le fotografie; la società titolare del sito su cui queste ultime vengono pubblicate).

58 Fotografie e immagini su cataloghi pubblicitari, giornali, riviste o altri strumenti di diffusione

I principi sopra ricordati sono stati riaffermati dall'Autorità in risposta ai numerosi quesiti concernenti, più in generale, la possibilità di pubblicare fotografie o immagini costituenti dati personali su cataloghi, giornali, riviste o altri analoghi strumenti di diffusione, ivi compresa la rete *Internet*.

In varie occasioni, pertanto, l'Autorità ha ricordato che le suddette immagini possono essere trattate solo con il consenso espresso, specifico e documentato per iscritto (art.11, l. n. 675/1996). Ciò, fatta salva l'eventuale sussistenza degli altri presupposti equipollenti del consenso indicati agli artt. 12 e 20 della legge citata.

Tra i casi in cui è consentito ad un soggetto privato trattare fotografie e immagini prescindendo dal consenso dell'interessato -ma non dalla previa informativa, ai sensi dell'art.10 della legge n. 675/1996- rileva, in particolare, l'ipotesi in cui la raccolta e la diffusione dei predetti dati siano necessarie per l'esecuzione degli obblighi derivanti da un contratto del quale è parte la persona ritratta (ad esempio, come nel caso evidenziato nel paragrafo precedente nel contesto di un servizio fotografico richiesto dall'interessato), ovvero per l'esecuzione di misure precontrattuali adottate su richiesta della stessa (artt. 12 lett. *b)*, e 20 lett. *a-bis)*, l. n. 675/1996).

Analogamente, è possibile prescindere dal consenso nel caso in cui il trattamento sia effettuato nell'esercizio del diritto di cronaca e, in generale, della libertà di manifestare il proprio pensiero (artt. 12, lett. *e)* 20, lett. *d)* e 25). In tale caso trovano applicazione le disposizioni contenute nel codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica.

Il Garante ha inoltre precisato che la legge n. 675/1996 non ha inciso sulle garanzie contenute nella legge sul diritto d'autore (artt. da 87 a 97 l. 22 aprile 1941, n. 633) le quali prevedono, fra l'altro, che l'esposizione, la riproduzione e la messa in commercio del ritratto di una persona presuppongono il consenso della persona ritrattata, a meno che la riproduzione dell'immagine sia giustificata *"dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico"* e che vietano, comunque, l'esposizione o la messa in commercio qualora rechi *"pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata"* (v. art.10 c.c.).

L'Autorità ha infine ricordato che -fermo restando quanto previsto per i trattamenti effettuati nell'esercizio del diritto di cronaca e di libera manifestazione del pensiero (art. 25, l. n. 675/1996 citata)- le specifiche disposizioni concernenti i dati c.d. "sensibili" (in particolare gli artt. 22 e 24 e le autorizzazioni generali per il 2002) trovano applicazione anche con riferimento alle immagini idonee a rivelare tale tipo di informazione.

Sicurezza dei dati e dei sistemi

59 Misure di sicurezza: novità normative e casi applicativi

La sicurezza costituisce una priorità nella normativa concernente la protezione dei dati personali e pertanto specifiche norme si rinvengono sia in atti sopranazionali, sia nella normativa nazionale.

Importanza primaria riveste la direttiva 95/46/CE che, come è noto, è stata recepita in Italia in larga misura con la legge n. 675/1996. In particolare, l'art. 15 si occupa della sicurezza dei dati, prevedendo due livelli di misure di sicurezza: le misure idonee e le misure minime.

Le prime sono rivolte a ridurre al minimo il rischio di distruzione, di perdita accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme, mentre le seconde sono quelle indicate nel regolamento emanato ai sensi dell'art. 15, comma 2, della legge n. 675/1996 (d.P.R. n. 318/1999). Questo regolamento doveva essere già adeguato in passato, essendo previsto al comma 3 che l'aggiornamento avvenga con cadenza almeno biennale.

La mancata adozione delle misure adeguate espone il destinatario della norma ad una responsabilità di tipo civile ai sensi dell'art. 18 della legge n. 675, mentre all'inosservanza delle prescrizioni indicate nel d.P.R. n. 318/1999 sono collegate le sanzioni penali previste all'art. 36 della medesima legge n. 675/1996, come modificato dal decreto legislativo n. 467/2001.

Le modifiche operate sugli aspetti sanzionatori penali per la mancata osservanza delle misure minime, entrate in vigore il 1° febbraio 2002, operano principalmente su due versanti: da un lato l'esclusione dal penale del trattamento effettuato per fini personali (art. 2, d.lg. n. 467/2001), dall'altro la rivisitazione della fattispecie criminosa (art. 14, d.lg. n. 467/2001).

In merito al primo punto l'esclusione della sanzione penale indicata all'art. 36 della legge n. 675/1996 non esonera le persone fisiche che trattano i dati per fini esclusivamente personali dall'adottare le misure di sicurezza di cui all'art. 15 comma 1, restando pertanto operanti le conseguenze civili previste al successivo articolo 18, e il conseguente obbligo al risarcimento dei danni cagionati ai sensi dell'art. 2050 del codice civile.

Con riguardo invece al secondo profilo il legislatore ha mantenuto, anche nella nuova formulazione dell'art. 36, la figura del reato, seppure diversamente configurato da delitto in contravvenzione e punito, pertanto, con l'arresto o con l'ammenda.

La novità più rilevante è data tuttavia dall'introduzione di una procedura estintiva del reato (cd. ravvedimento operoso) espressamente mutuata dalla normativa in materia di sicurezza e igiene sul lavoro prevista nel decreto legislativo n. 758/1994 (art. 20, d.lg. n. 467/2001).

Il tema della sicurezza ha un carattere poliedrico e si riverbera su numerosi settori di intervento della normativa sulla riservatezza.

È utile ricordare anche in questo paragrafo che nel 2002 è stato adottato il codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (cfr. paragrafo 25), pubblicato nella *Gazzetta Ufficiale* n. 230 del 1 ottobre 2002. Il codice contiene specifiche indicazioni in ordine all'adozione delle misure di sicurezza. Sono previste numerose misure volte a proteggere i dati. I rilevatori devono garantire la sicurezza delle informazioni e rispettare le norme poste dal codice a tutela dei cittadini. La comunicazione dei dati tra soggetti del Sistema statistico nazionale deve avvenire nel rispetto delle misure di sicurezza previste dall'art. 15 della legge. E' necessario determinare differenti livelli di accesso ai dati personali con riferimento alla natura dei dati e alle funzioni dei soggetti coinvolti nei trattamenti, nonché adottare le cautele previste dagli articoli 3 e 4 del d. lg. n. 135/1999 in riferimento ai dati sensibili.

Tra gli atti normativi del 2002 che contengono apposite previsioni in ordine alle misure di sicurezza, assume particolare rilievo la direttiva 2002/58/CE sulla tutela della vita privata nelle comunicazioni elettroniche. L'importanza di tale direttiva è evidenziata dal fatto che il legislatore, per consentire il suo recepimento con lo strumento della legge comunitaria (legge 3 febbraio 2003, n.14), ha disposto uno slittamento di sei mesi del termine entro cui adottare il previsto testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

La direttiva prevede l'obbligo per il fornitore del servizio di predisporre appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi congiuntamente con il fornitore della rete pubblica di comunicazione.

La nuova direttiva fa gravare in capo al fornitore del servizio l'obbligo di informare gli abbonati quando sussiste un particolare rischio di violazione della sicurezza della rete, indicando i relativi costi e rimedi o situazioni che consentano di apprendere in modo non intenzionale il contenuto delle conversazioni o delle comunicazioni.

Sullo stesso tema è intervenuta anche la risoluzione del 28 gennaio del 2002 del Consiglio dell'Ue, tesa a fornire un approccio comune e azioni specifiche nel settore della sicurezza delle reti (2002/C43/02), la quale precisa che la sicurezza delle reti e dell'informazione presuppone che sia assicurata la disponibilità di dati e servizi. Ciò impedendo interruzioni o intercettazioni abusive delle comunicazioni, confermando che i dati trasmessi, ricevuti o archiviati sono completi e invariati, assicurando la riservatezza dei dati, proteggendo i sistemi da accessi non autorizzati e *software* maligni e garantendo, infine, l'affidabilità dell'autenticazione.

Anche l'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), nel corso del 2002, si è attivato nel settore delle misure di sicurezza tracciando alcune Linee guida approvate il 25 luglio, che prendono il posto di quelle elaborate nel 1992. Lo sviluppo esponenziale di *Internet* nei settori pubblico e privato ha imposto la necessità di indicare nuovi principi in materia di sicurezza dei sistemi informativi e delle reti. Esse, come espressamente raccomandato dall'OCSE, andranno riesaminate ogni cinque anni per l'esplicitato fine di promuovere una cooperazione internazionale sulle questioni connesse al sistema di sicurezza delle reti e dei sistemi informativi.

Le Linee guida si propongono di sviluppare una "cultura della sicurezza" fra i governi, le imprese e gli utenti, con l'invito a tutti gli utilizzatori di tecnologie dell'informazione a rispettare ed applicare nove principi base, fra cui la sensibilizzazione e la responsabilità in materia di sicurezza e il rispetto di valori etici e democratici, con particolare riguardo alla tutela dei dati personali.

Anche l'Autorità, nel corso del 2002, si è pronunciata numerose volte in materia di sicurezza, in seguito a ricorsi presentati ai sensi dell'art. 29, a segnalazioni o a procedimenti ispettivi.

Con alcuni ricorsi si è lamentato che il titolare, nell'effettuare il trattamento dei dati, non avesse osservato le specifiche disposizioni previste dalla legge n. 675/1996 anche con riferimento alla mancata adozione delle misure di sicurezza. In tali circostanze il Garante ha però ribadito che il procedimento disciplinato dall'art. 29 ha caratteri peculiari in quanto il ricorso che lo introduce può essere presentato solo per la tutela di precise richieste formulate in riferimento agli specifici diritti tutelati dall'art. 13, comma 1, della medesima legge e non si può rappresentare senza un collegamento a tale articolo qualsiasi violazione della disciplina del trattamento dei dati personali, compresa la mancata adozione delle misure minime di sicurezza (2 maggio 2002 - *Bollettino* n. 28).

In un altro caso il Garante, dopo aver esaminato il ricorso di un cittadino, ha disposto un'ispezione del sistema informatico di una importante banca *on line* per verificare i sistemi di sicurezza adottati dall'istituto di credito e il loro grado di affidabilità riguardo alla tutela della riservatezza dei dati personali della clientela. La decisione è stata assunta in quanto il ricorrente, cliente della stessa banca, è riuscito attraverso *Internet* a consultare non solo i dati del suo conto corrente, ma anche quelli di altri clienti della banca.

Sono da ricordare anche le segnalazioni di consumatori che lamentavano la violazione della normativa sulla *privacy* da parte di una società che, dopo aver sviluppato fotografie, le pubblicava come ulteriore servizio su un sito *web* dove, attraverso un codice personale, erano accessibili ai clienti i quali potevano così stamparle, raccoglierle in album virtuali o spedirle via *e-mail*. Nelle segnalazioni, oltre a sottolineare la mancanza della dovuta informativa preventiva sul tipo di servizio che veniva offerto, si evidenziava la carenza dell'adozione di idonee misure di sicurezza, in quanto il codice personale fornito dalla società era collocato all'esterno della busta che contiene le foto ritirate dal cliente, visibile anche da terzi non autorizzati a visionare il materiale fotografico.

Nella conseguente pronuncia il Garante ha disposto che la società attuasse i necessari accorgimenti volti a prevenire taluni rischi, tra i quali quelli di distruzione o perdita dei dati personali trattati o di accesso non autorizzato. Le misure da adottare assumono rilievo sia nelle diverse fasi del processo di realizzazione del servizio *"photosìonline"*, sia con riguardo ai diversi soggetti in esso coinvolti (i negozianti e gli altri addetti allo sviluppo delle fotografie; il gestore del *server* nel quale viene conservato il *file* contenente le fotografie; la società titolare del sito su cui queste ultime vengono pubblicate) (*Provv.* 16 maggio 2002, in *Bollettino* n. 28).

I trasferimenti all'estero dei dati

60 Paesi che offrono una protezione adeguata

A seguito del primo recepimento in Italia -con le autorizzazioni del Garante (v. *Relazione 2001*, pag. 91)- delle decisioni della Commissione europea in materia di trasferimento di dati personali all'estero, e in considerazione delle modifiche apportate dal d.lg. n. 467/2001 all'articolo 28 della legge 675/1996, l'Autorità ha iniziato a svolgere un attento monitoraggio in relazione ad operazioni ed attività di esportazione di dati da parte di operatori italiani e al tipo di garanzie e strumenti adottati per tutelare i diritti degli interessati.

Nell'aprile 2002 sono state formulate nei confronti di alcune importanti società, che avevano inviato comunicazioni o notificazioni sul trasferimento di dati all'estero e, in particolare, negli Usa, richieste di informazioni circa il rispetto delle disposizioni nazionali e comunitarie sui presupposti di liceità delle operazioni di trasferimento, con particolare riguardo, da un lato, alle relative finalità e modalità, alle categorie di dati e di persone interessate, nonché agli estremi dei soggetti importatori, e, dall'altro, all'eventuale adesione di questi ultimi al *Safe Harbor* o all'utilizzazione di clausole contrattuali tipo.

Dagli elementi acquisiti è risultato che, nella maggior parte dei casi, i dati personali oggetto di trasferimento all'estero riguardavano dipendenti e altre società e imprese (clienti, concorrenti, fornitori, ecc.) e che i flussi di dati erano stati effettuati previa acquisizione di specifico consenso degli interessati o avvalendosi di uno degli altri presupposti di liceità previsti dal citato art. 28 (esecuzione di obblighi contrattuali, ecc.)

In alcune ipotesi in cui la gestione del personale all'estero viene effettuata negli U.S.A., gli importatori dei dati (società capogruppo o comunque collegate o controllate) hanno aderito all'accordo sui principi dell'approdo sicuro, dichiarandosi disponibili a cooperare con le Autorità di vigilanza degli altri Paesi europei.

In nessuno di questi primi casi esaminati dal Garante è emerso che le società interpellate abbiano utilizzato le clausole contrattuali standard indicate dalla Commissione europea, trattandosi peraltro di strumenti introdotti solo recentemente.

Nell'ambito della stessa indagine, è stato infine evidenziato che, accanto alla proposta di una società di predisporre un apposito contratto per i propri flussi di dati all'estero da sottoporre al Garante al fine di ottenere una specifica autorizzazione, il gruppo societario di appartenenza stava sviluppando un contratto "multilaterale" per tutte le consociate da sottoporre anch'esso al parere preventivo delle Autorità Garanti europee.

Nel mese di marzo 2003 l'Autorità ha disposto un'ampia verifica preliminare, tuttora in atto, circa le modalità di applicazione da parte delle principali società industriali e di servizi delle disposizioni comunitarie e nazionali in materia di trasferimento dei dati personali all'e-

stero. Tale verifica è risultata necessaria al fine di valutare lo stato di attuazione delle disposizioni sui flussi di dati all'estero, prima d avviare specifici accertamenti relativi a singole società.

Oggetto dell'indagine è, in particolare, l'analisi dei presupposti, delle finalità e modalità del trasferimento di dati all'estero, anche in relazione ad operazioni effettuate da eventuali società collegate o controllate, delle categorie di dati trasferiti e delle persone interessate, degli estremi e delle attività dei soggetti importatori, nonché delle garanzie assunte per la tutela dei dati personali nei confronti di ciascuna tipologia di trasferimento. E' stato inoltre richiesto di indicare in termini percentuali, l'incidenza dell'utilizzo di clausole contrattuali tipo, dell'adesione ai principi di approdo sicuro e di uno dei casi indicati dall'art. 28, comma 4, della citata legge n. 675 (consenso degli interessati, esecuzione di obblighi contrattuali, ecc.), rispetto al volume complessivo dei trasferimenti di dati all'estero.

Il Garante ha, da ultimo, dato attuazione (*Deliberazione* n. 6 del 30 aprile 2003) alla decisione comunitaria del 20 dicembre 2001 con cui la Commissione europea ha riconosciuto anche il Canada tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali. (v. *Relazione 2001*). Tale deliberazione, al momento in cui il presente testo viene redatto, è in fase di pubblicazione nella *G.U.*

61 *"Safe Harbor"*

La Commissione europea ha riconosciuto in passato che i principi internazionali di riservatezza del *Safe Harbor*, pubblicati dal Dipartimento del commercio degli Stati Uniti, costituiscono un'adeguata protezione ai fini del trasferimento di dati personali dall'Unione europea verso tale Paese (decisione n. 2000/520/CE).

Il Garante, con l'autorizzazione del 10 Ottobre 2001 (pubblicata in G.U. 26 novembre 2001), ha attuato la suddetta decisione riservandosi di controllare la legittimità dei trasferimenti e di adottare i provvedimenti ad essa eventualmente conseguenti.

La stessa Commissione europea ha effettuato un primo rapporto (in data 13 febbraio 2002) sull'applicazione della decisione 2000/520/CE, corrispondendo a quanto auspicato dal Parlamento europeo che, con risoluzione del 5 luglio 2000, aveva invitato la Commissione ad assicurare uno stretto monitoraggio del funzionamento del sistema dell'approdo sicuro (v. *Relazione 2001*, p. 93).

Si tratta di un rapporto provvisorio che offre, comunque, significativi spunti di riflessione ed evidenzia alcuni punti critici sulle carenze che si registrano in termini di effettiva applicazione dell'Accordo e di trasparenza in relazione alle prassi applicative ed alle decisioni adottate sulle dispute. Vari spunti di riflessione sono giunti al riguardo dal Gruppo dell'art. 29 della direttiva 95/46/CE.

In questo quadro, il Garante continua a partecipare all'attività di monitoraggio, in vista ormai della valutazione d'insieme sul funzionamento del *Safe Harbor*, prevista per il 2003 da parte della Commissione europea, ed è attivamente impegnato nel favorire la cooperazione al riguardo. In tal senso, va ricordata la visita negli Usa il 13 e 14 marzo 2002 di una delegazione di rappresentanti delle autorità di protezione dati europee, che ha consentito incontri con rappresentanti del Congresso, dell'amministrazione Usa, con imprese multinazionali aderenti al meccanismo del *Safe Harbor* e con numerose organizzazioni non governative da anni impegnate nella tutela della *privacy*.

Dai risultati assai proficui di tale visita è derivato un nuovo pronunciamento del Gruppo europeo in data 2 luglio 2002.

In tale documento è stata evidenziata la necessità di collaborazione di tutte le autorità competenti a dare piena esecuzione all'accordo.

In particolare, conformemente alla richiesta fatta dal Parlamento europeo nella sua risoluzione del 5 luglio 2000, si richiamano le autorità, le organizzazioni e le associazioni coinvolte a collaborare per raccogliere -in particolare attraverso le autorità nazionali per la protezione dei dati e la Commissione europea- informazioni aggiornate, con particolare attenzione:

- ad accordi per l'aumento della trasparenza nei confronti delle organizzazioni firmatarie, in particolare se una dichiarazione di adesione non è accompagnata da adeguate politiche per la *privacy*;
- alla possibilità di fornire meccanismi di controllo addizionali nei confronti della procedura d'adesione all'accordo, la conformità di condotta degli aderenti allo stesso con le proprie politiche di *privacy* e l'eventuale perdita dei benefici dell'Approdo sicuro;
- alle iniziative da adottare al fine di aumentare la conoscenza dei prerequisiti per l'adesione all'Approdo sicuro, anche attraverso di documenti brevi, facilmente comprensibili e l'eventuale integrazione nel *Safe Harbor Workbook*;
- ai provvedimenti da adottare per mettere a punto meccanismi di risoluzione delle controversie, aumentare l'uniformità e la conoscenza dei criteri salienti, aumentare la trasparenza circa l'esito delle controversie e semplificarne i meccanismi di pubblicazione;
- alle eventuali difficoltà derivanti dall'esistenza di molteplici politiche di *privacy* dichiarate dal medesimo operatore;
- ai criteri di priorità ed alle possibili ulteriori iniziative intraprese dalle competenti autorità statunitensi ed agli accordi per una rinnovata cooperazione tra il comitato europeo per la protezione dei dati, gli organi di risoluzione delle controversie e la Federal Trade Commission.