50 Elenchi abbonati e diritto alla riservatezza

Hanno formato oggetto di esame anche le problematiche legate alla compilazione, alla diffusione e all'utilizzo degli elenchi telefonici. Tale tematica presenta diversi aspetti di particolare complessità in ordine alla protezione dei dati personali, anche con riferimento alla fase transitoria che porterà all'applicazione di quanto previsto dal d.P.R. 11 gennaio 2001, n. 77.

Al riguardo, occorre dapprima ricordare che, nonostante i ripetuti richiami in ordine alla necessità che siano sempre rispettate le disposizioni secondo cui il Presidente del Consiglio dei ministri e ciascun ministro sono tenuti a consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 31, comma 2, l. n. 675/1996), la stessa Autorità non è stata consultata durante la predisposizione del d.P.R. appena citato, con conseguente vizio dell'atto.

L'art. 20 dello stesso d.P.R., benché di imprecisa formulazione, subordina la disciplina relativa ai servizi elenchi abbonati alla normativa generale sulla riservatezza ed a quella dettata con specifico riguardo ai trattamenti realizzati nell'ambito delle telecomunicazioni (in particolare, al d.lg. 13 maggio 1998, n. 171). Tale disposizione (benché presenti alcuni aspetti problematici anche sul piano transitorio) ha dunque inteso salvaguardare le garanzie contenute nell'art. 9 del d.lg. n. 171/1998 che prevede, in particolare: la possibilità di limitare i dati inseriti negli elenchi a quelli necessari per identificare l'abbonato, salvo consenso espresso di quest'ultimo alla diffusione di dati ulteriori; la possibilità di chiedere gratuitamente che il proprio indirizzo sia in parte omesso nonché, qualora ciò sia fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso.

Queste garanzie sono del resto in fase di possibile rafforzamento da parte degli artt. 12 e 16 della proposta di modifica della direttiva 97/66/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM (2000)385 - COD 2000/0189), in cui – secondo la posizione comune definita dal Consiglio il 28 gennaio 2002 – si prevede, tra l'altro, il previo consenso dell'interessato per l'inserimento dei dati personali in elenchi telefonici (v. par. 126).

Con riguardo a tale problematica, inoltre, l'Autorità per le garanzie nelle comunicazioni ha richiesto al Garante un parere su un provvedimento predisposto in materia; in tale occasione, sono state già fornite alcune prime indicazioni al fine di assicurare che i trattamenti di tali dati, effettuati attraverso la predisposizione e la pubblicazione di elenchi, siano conformi a quanto previsto dalla vigente normativa in materia di *privacy*.

La decisione dell'Autorità per le garanzie nelle comunicazioni appena richiamata prevede l'emanazione di un ulteriore provvedimento, specificatamente dedicato alla tutela dei dati personali utilizzati nella predisposizione degli elenchi, che dovrebbe essere adottato in breve tempo in cooperazione tra le Autorità.

51 Comunicazioni indesiderate su utenze telefoniche mobili

Con specifico riguardo al settore della telefonia mobile, l'Autorità si è anche occupata a più riprese dell'utilizzo del sistema di messaggeria (*sms*) dei telefoni cellulari.

La questione è stata inizialmente esaminata nell'ambito di un ricorso presentato al Garante con riguardo alla ricezione di alcuni *sms* su utenze telefoniche mobili contenenti indicazioni di voto a favore di un parlamentare (*Provv.* 20 giugno 2001, in *Bollettino* n. 21, p. 39).

Un successivo intervento, invece, ha preso le mosse da notizie apparse sugli organi di stampa riguardanti l'iniziativa di alcuni enti pubblici di inviare messaggi di pubblica utilità o di emergenza avvalendosi di alcuni fornitori di servizi di telefonia mobile. Sulla base di esse, sono state assunte informazioni presso enti e fornitori al fine di verificare la rispondenza di tali trattamenti alle vigenti norme in materia di protezione dei dati personali; dalle informazioni acquisite è emerso che l'utilizzo di tale sistema di comunicazione era stato predisposto per consentire alle persone che in un dato momento si trovavano in una determinata area geografica di venire tempestivamente a conoscenza dei provvedimenti adottati in via d'urgenza dalle autorità locali.

Oltre a questa iniziativa, si è venuti a conoscenza di altre, in fase di progettazione o di sperimentazione, riguardanti la possibilità, per taluni enti locali, di fornire ai cittadini – sempre attraverso *sms* – informazioni concernenti i servizi di pubblica utilità resi dagli stessi enti (es. informazioni sulla viabilità, sugli avvenimenti culturali in corso, sugli scioperi, sul pagamento delle imposte, sui termini di validità dei documenti).

A tutto ciò, si aggiunge, altresì, l'ormai noto sistema di utilizzo di tali mezzi di comunicazione, soprattutto da parte di soggetti privati, per l'invio di messaggi a fini di commercializzazione diretta. È infine in fase di definizione il profilo concernente i messaggi promozionali inviati, rispetto a propri servizi, dagli stessi fornitori di servizi di telecomunicazione.

Pur riconoscendo la possibile utilità di tali nuovi servizi, non si può sottovalutare la particolare forza invasiva che caratterizza le comunicazioni realizzate attraverso l'invio di *sms*, avvalendosi peraltro del numero del telefono cellulare, generalmente considerato come personale e riservato. Pertanto, si è ritenuto necessario offrire alcune indicazioni in materia e l'Autorità è in procinto di definire alcuni provvedimenti volti a segnalare misure ed accorgimenti idonei ad evitare che il trattamento di dati personali, effettuato con servizi *sms*, determini un'ingiustificata lesione della riservatezza dei soggetti cui i dati stessi si riferiscono.

Trattamento di dati personali in *Internet*

52 Profili generali

Con riguardo ai trattamenti realizzati sulle reti telematiche, la continua evoluzione tecnologica che ha interessato il settore ha determinato il sorgere di nuove problematiche con riguardo alla protezione degli utenti rispetto al trattamento e alla circolazione dei loro dati personali.

Ciò è testimoniato anche dagli innumerevoli quesiti, segnalazioni, richieste di chiarimenti pervenuti sia da parte dei singoli utenti (in particolare in relazione alle modalità con cui gli stessi possono ottenere la cancellazione dei propri dati raccolti per il tramite dei siti Internet), sia da parte degli stessi gestori dei siti *web*.

È stato avviato un nuovo monitoraggio sulle modalità utilizzate da siti *web* italiani per fornire l'informativa e richiedere il consenso, ove necessario, nonché per ottemperare agli obblighi in materia di protezione dei dati.

L'Autorità ha già fornito alcuni primi chiarimenti circa le modalità con cui è possibile esercitare i diritti riconosciuti dall'articolo 13 della legge n. 675/1996 sulla rete *Internet*, fornendo di volta in volta indicazioni agli utenti al fine di ottenere la cancellazione dei propri dati personali o indicando ai gestori dei siti gli accorgimenti necessari per conformarsi alla disciplina sulla tutela dei dati personali e, quindi, le misure da adottare al fine di favorire l'esercizio dei diritti medesimi.

Con riguardo al diritto di accesso in questione, si segnala un intervento dell'Autorità, a seguito di un ricorso, in cui è stata riconosciuta la legittimità della richiesta dell'interessato di conoscere, ai sensi dell'art. 13, i propri dati personali contenuti nei messaggi di posta elettronica (*Provv.* 30 ottobre 2001, in *Bollettino* n. 23, p. 86).

Sono state altresì affrontate le problematiche legate all'utilizzo, da parte dei gestori di siti *web*, di particolari dispositivi e/o programmi (*software* spia, *cookies*) che, specie ove introdotti nel terminale dell'utente a sua insaputa, magari all'atto del suo collegamento ad un determinato sito, permettono di seguirne la navigazione, consentendo finanche l'accesso a informazioni archiviate dallo stesso.

Per tali ragioni, il Garante, anche a seguito di numerose segnalazioni prevenute in tal senso, ha provveduto a richiedere puntuali informazioni sui trattamenti realizzati a diversi gestori di siti *Internet*. Sulla base delle risultanze di tali controlli, nonché di quelli effettuati in via autonoma su altri siti, l'Autorità provvederà fra breve ad offrire alcune indicazioni con un provvedimento anche di carattere generale, al fine di invitare i gestori dei siti a conformarsi alle garanzie previste dal nostro ordinamento a tutela della riservatezza, tenendo conto anche dei principi della Raccomandazione adottata dal Gruppo dei garanti europei lo scorso 17 maggio 2001.

53 Comunicazioni indesiderate ed utilizzo dei nomi di dominio *Internet*

Il Garante si era occupato del problema dell'invio di messaggi di posta elettronica contenenti comunicazioni pubblicitarie indesiderate – il cosiddetto *spamming* – anche in passato (v. *Relazione 2000*, p. 68) ed aveva già avuto modo di confrontarsi, fra l'altro, con le differenti discipline previste in materia, in Europa e negli USA, a seconda dell'adozione di regimi fondati sul consenso positivo – ossia, sulla possibilità per l'utente di scegliere se accettare o meno tali comunicazioni pubblicitarie (cd. *opt-in*) – oppure sul consenso negativo (cd. *opt-out*).

L'occasione per un nuovo esame della questione da parte dell'Autorità, è stata offerta dall'intenso contributo fornito nel quadro dei lavori di modifica della direttiva 97/66/CE del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM (2000)385 – COD 2000/0189; v. anche par. 77). Dopo un lungo dibattito in sede comunitaria, il 28 gennaio 2002, il Consiglio dell'Unione europea ha definito la cd. posizione comune in vista dell'adozione della direttiva, con la quale, seguendo l'orientamento innovativo proposto dalla Commissione rispetto alla direttiva del 1997, si prevede che la disciplina relativa all'invio di chiamate con sistemi automatizzati debba riferirsi anche ai messaggi di posta elettronica, applicando obbligatoriamente anche ad essi la regola del consenso positivo (*opt-in*) già osservata in alcuni Paesi europei.

In particolare, per quanto attiene specificamente all'invio di chiamate indesiderate, nella posizione comune si rinviene l'impostazione originaria, distinguendo anche l'ipotesi in cui le chiamate vengano effettuate con o senza l'intervento di un operatore (in quest'ultimo caso, che fa riferimento all'uso di strumenti automatizzati di chiamata, è stato previsto che per autorizzare l'invio sia necessario, in ogni caso, ottenere il consenso preventivo ed esplicito del ricevente). Tutto ciò in considerazione delle più ampie possibilità di invio anche durante orari notturni, nonché del fatto che, al di là della valenza intrusiva propria di tali forme di comunicazione, esse comportano spesso costi legati alla ricezione del messaggio (es. la carta del fax su cui viene stampato il messaggio o – ed è l'ipotesi che qui maggiormente ci interessa – i costi necessari a collegarsi alla rete telefonica per scaricare i messaggi di posta elettronica).

Va anche ricordata una pronuncia – alla quale si è fatto cenno al par. 29 – relativa all'invio non consensuale e generalizzato di *e-mail* con finalità di comunicazione politica (*Provv.* 11 gennaio 2001, in *Bollettino* n. 16, p. 39): nell'accogliere il ricorso, si è ribadita la nozione di pubblici registri, contenuta nella legge 675/1996, al fine di evidenziare il fatto che la rinvenibilità di indirizzi di posta elettronica in spazi pubblici di *Internet* non ne comporta un uso libero per l'ulteriore invio di posta elettronica.

In occasione di altri ricorsi, sono state esaminate questioni relative alla protezione dei domini *Internet* con specifico riguardo alla rettifica dei dati relativi al "*registrant*" (*Provv.* 7 marzo 2001, in *Bollettino* n. 18, p. 5) e alla pubblicazione di alcuni dati personali sulle pagine *web* lesive dell'onore e della reputazione (*Provv.* 16 gennaio 2001, in *Bollettino* n. 16, p. 36; v. anche *Relazione 2000*, p. 72).

54 Il codice deontologico

Come accennato, al fine di garantire la piena attuazione dei principi previsti dalla disciplina in materia di trattamento dei dati personali, il Garante, sulla base di quanto stabilito dal decreto legislativo 28 dicembre 2001, n. 467, ha promosso la sottoscrizione di un codice di deontologia e di buona condotta riguardante il trattamento dei dati personali effettuato nell'ambito dei servizi di comunicazione e informazione offerti per via telematica e in particolare nella rete *web*. Il codice avrà, fra l'altro, l'obiettivo di assicurare 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, in particolare attraverso informative fornite in linea in modo agevole ed interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti.

Con l'intento di garantirne un'adeguata pubblicità, si è previsto che il codice venga pubblicato sulla Gazzetta Ufficiale e che il suo testo sia allegato al testo unico sulla protezione dei dati personali che dovrà essere emanato entro la fine del 2002.

È necessario infine sottolineare che, al pari di quanto previsto per i codici sui trattamenti realizzati a fini storici o statistici, e nonostante la sua denominazione, tale codice non avrà il valore di una qualunque altra disposizione di carattere deontologico, ma assumerà la veste di una vera e propria fonte dell'ordinamento generale, come si evince dal fatto che il rispetto delle disposizioni in esso contenute costituirà condizione essenziale per la liceità del trattamento dei dati (art. 20 d.lg. n. 467/2001).

Sicurezza dei dati e dei sistemi

55 Le misure di sicurezza: casi applicativi

Il titolare e, se designato, il responsabile del trattamento dei dati personali, hanno l'obbligo di custodire e controllare i dati trattati mediante l'adozione di idonee e preventive misure di sicurezza – individuate alla luce delle conoscenze acquisite in base al progresso tecnico, in relazione alla natura dei dati e alle specifiche caratteristiche del trattamento – tali da ridurre al minimo i rischi di distruzione, perdita accidentale, accesso non autorizzato, trattamento non consentito o, comunque, non conforme alle finalità della raccolta (art. 15, comma 1, l. n. 675/1996).

Le "*misure minime di sicurezza*" – definite con il d.P.R. 28 luglio 1999 n. 318 e la cui mancata osservanza comporta sanzioni di carattere penale (art. 36 l. n. 675/1996) e civile (art. 18 l. n. 675/1996) – in virtù dell'art. 15, comma 3, sono soggette ad adeguamento, con cadenza almeno biennale, in relazione all'evoluzione tecnica e all'esperienza maturata. Il Garante fornirà un contributo per il loro aggiornamento rendendo noti i risultati di un gruppo di lavoro, la cui attività potrebbe risultare utile nel quadro di un'autonoma revisione del d.P.R. o della sua integrazione all'interno dell'atteso testo unico.

Dal punto di vista applicativo, la questione delle misure di sicurezza ha formato oggetto di vari provvedimenti: in data 23 febbraio 2001, è stata ad esempio valutata la conformità al d.P.R. n. 318/1999 della richiesta, avanzata da un'azienda ai propri dipendenti – che utilizzano strumenti informatici – di servirsi di *password* loro singolarmente assegnate, con il contestuale divieto di autonoma modifica della stessa (v. nota prot. 2074/01, in *Bollettino* n. 17, p. 32); in merito, l'Autorità ha ricordato che gli incaricati, ove tecnicamente possibile, devono poter procedere autonomamente alla sostituzione della *password*, previa comunicazione, però, ai soggetti preposti alla loro custodia (es. comunicazione effettuata tramite busta chiusa) per consentire al titolare del trattamento eventuali interventi nel caso di assenza o di impedimento dell'incaricato; inoltre, in caso di "elaboratori accessibili in rete", oltre la parola chiave, è necessario utilizzare i codici identificativi.

Anche nel fornire, poi, il cd. "decalogo" per l'utilizzazione di dati da parte di partiti e movimenti politici durante il periodo di propaganda elettorale ovvero per la presentazione di liste e candidature o per la sottoscrizione di referendum (per il quale v. par. 29), è stata ribadita la necessità di rispettare alcuni principi sulla raccolta dei dati, sottolineando altresì l'obbligo di adottare le misure di sicurezza, ed in particolare quelle minime di cui al d.P.R. n. 318/1999, con riferimento ai trattamenti di dati cartacei e automatizzati. Analoga indicazione è stata fornita in un parere relativo ad uno schema di regolamento volto ad istituire un sistema di comunicazione tra regioni ed enti locali per pianificare e gestire la relativa autonomia tributaria e per consentire il decentramento catastale, evidenziando che la complessa articolazione dei flussi di dati che saranno trattati in base alle citate disposizioni presuppone la doverosa adozione di idonee misure di sicurezza "*a prescindere da eventuali regole tecniche indicate per i sistemi utilizzati*" (*Provv.* 27 giugno 2001, in *Bollettino* n. 21, p. 15).

In alcuni casi, l'Autorità ha esaminato segnalazioni riguardanti l'utilizzazione di dati estratti dall'anagrafe della popolazione per l'invio di lettere ai cittadini da parte del Sindaco e ha avviato accertamenti presso i comuni interessati su alcuni aspetti, tra cui le misure di sicurezza adottate, anche sotto il profilo inerente all'eventuale collaborazione di terzi all'inoltro delle lettere.

Non diversamente è accaduto in relazione alle questioni dei trattamenti di dati in sede di svolgimento del censimento nella provincia di Bolzano (*Provv.* 6 febbraio 2001, in *Bollettino* 17, p. 11) e dell'installazione all'entrata degli istituti bancari di sistemi di rilevazione delle impronte digitali degli utenti – eventualmente associate ad immagini – per i quali occorre adottare parimenti misure di sicurezza che osservino i parametri fissati dalla l. 675/1996 e dal d.P.R. 318/1999, in particolare per quanto riguarda la custodia delle chiavi di accesso. Inoltre, si è stabilito che detti sistemi di rilevazione devono offrire una "*rigorosa garanzia di affidabilità ed integrità dei dati*", anche sulla base di eventuali certificazioni od omologazioni dei dispositivi, e che le informazioni relative a immagini e impronte devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della loro rilevazione (*Provv.* 28 settembre 2001, in *Bollettino* n. 22, p. 82).

I trasferimenti all'estero di dati

56 Paesi che offrono una protezione adeguata

Il crescente rilievo delle questioni riguardanti il trasferimento all'estero di dati personali è segnalato anche dalla recente modifica, ad opera del decreto legislativo n. 467/2001, dell'articolo 28 della legge 675/1996, in base alla quale è demandato al Garante il compito di autorizzare il trasferimento dei dati verso Paesi terzi sulla base di adeguate garanzie per l'interessato, prestate anche con un contratto, ovvero individuate dalla Commissione europea (al cui sito *http://europa.eu.int/comm/internal-market* è opportuno fare riferimento per una completa ricognizione dei materiali pertinenti, i più rilevanti dei quali sono richiamati in allegato alla presente relazione).

Viene così esplicitamente individuato lo strumento di attuazione delle decisioni comunitarie previste dagli articoli 25, par. 6, e 26, par. 4, della direttiva 95/46/CE, rispettivamente riguardanti l'adeguatezza della protezione dei dati personali offerta dall'ordinamento di un Paese terzo e le garanzie risultanti da clausole contrattuali, reputate idonee a tal fine dalla Commissione.

Con il medesimo decreto legislativo, semplificando gli adempimenti per i destinatari del citato art. 28, si è stabilito che il trasferimento di dati personali all'estero deve essere notificato al Garante solo qualora sia diretto verso un Paese non appartenente all'Unione europea e ricorra uno dei casi individuati ai sensi dell'articolo 7, comma 1, della legge, disposizione anch'essa oggetto di rivisitazione.

In alcune circostanze, tuttavia, anche il trasferimento a Paesi membri può porre questioni di natura particolare. Rispondendo ad una richiesta di parere del Ministro delle comunicazioni, il 3 settembre 2001, l'Autorità, in sede di primo riscontro e rimanendo a disposizione per ogni approfondimento, ha richiamato la necessità della massima cautela relativamente al trasferimento di dati di traffico ad una società spagnola *partner*, prospettato – per esigenze gestionali – da un gestore italiano di servizio di telefonia mobile secondo lo standard Umts. La competente Direzione generale del Ministero aveva peraltro già fornito al gestore risposta negativa, evidenziando che esigenze giudiziarie richiedono che i dati siano conservati nella loro integrità originaria in Italia.

Il Garante – che ha poi riferito sul caso al Gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE – nel sottolineare che si tratta di dati tutelati anche costituzionalmente, ha invitato a considerare, inoltre, le problematiche relative alla sicurezza dei dati ed al loro possibile incrocio con i dati detenuti dalla società spagnola. La questione sembra aver successivamente perso di attualità per il sostanziale venir meno delle prospettate esigenze gestionali.

Delle decisioni comunitarie in materia di adeguatezza degli ordinamenti stranieri, riguardanti l'Ungheria e la Svizzera, si è dato conto nella relazione annuale dello scorso anno (v. *Relazione 2000*, p. 85).

Esse sono state attuate con deliberazioni dell'ottobre 2001 (pubblicate sulla *Gazzetta Ufficiale* e consultabili sul sito *web* dell'Autorità anche ai fini dell'invio di osservazioni, volte ad evidenziarne eventuali problemi applicativi), nelle quali il Garante si è comunque riservato di procedere ai necessari controlli sulla legittimità dei trasferimenti.

Passando ora al piano internazionale, va tenuto presente che la disciplina comunitaria si applica anche ai Paesi che, con quelli dell'Unione, costituiscono lo Spazio economico europeo – cioè Norvegia, Lichtenstein ed Islanda – e che negli Usa sono in vigore i principi cd. del *Safe Harbor* (v. paragrafo successivo).

Con decisione del 20 dicembre 2001 (2002/2/CE, in *G.U.C.E.* L 002, 4 gennaio 2002), la Commissione europea ha riconosciuto che la legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (*Canadian Personal Information Protection and Electronic Documents Act*) assicura una protezione adeguata per il trasferimento di alcuni dati personali dall'Unione europea al Canada. Viene così facilitato il flusso di dati

dall'Europa verso un Paese terzo in cui, come previsto dall'art. 25, par. 6, della direttiva sulla protezione dei dati (95/46/CE), si riconosce l'esistenza di un livello adeguato di protezione.

Il gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE si era espresso sul grado di protezione offerta dall'ordinamento canadese, con un parere del 26 gennaio 2001 (parere n. 2/2001) sostanzialmente interlocutorio e che, tra l'altro, sottolineava le questioni relative all'ambito di applicazione della legge canadese ed alla problematica del rapporto tra norme federali e norme delle diverse province (v. anche *Relazione 2000*, p. 85).

La decisione della Commissione, in qualche misura, ha tenuto conto di tale parere, commisurando il proprio ambito di applicazione a quello della legge canadese che, in prima approssimazione, è applicabile (dal 1° gennaio 2002) ai soggetti disciplinati da norme di livello federale, e (dal 1° gennaio 2004) a tutte le organizzazioni federali o non federali, che rilevano, utilizzano o comunicano dati personali nell'ambito di attività commerciali, con eccezione dei soggetti ai quali sia applicabile la legislazione provinciale, considerata sostanzialmente simile a quella federale.

Nella decisione comunitaria viene sottolineato che l'applicazione delle norme canadesi di protezione è garantita da ricorsi giurisdizionali nonché dal controllo indipendente esercitato da Autorità quali il Commissario federale per la *privacy* (*Federal Privacy Commissioner*), che ha poteri di investigazione ed intervento ed al quale ci si può rivolgere anche nei casi in cui non sia chiaro l'ambito di applicazione della citata legge; nel caso di conseguenze pregiudizievoli per la persona si applicano inoltre le norme canadesi sulla responsabilità civile.

Le autorità degli Stati membri hanno facoltà di sospendere flussi di dati verso i destinatari in Canada nei casi in cui sia stato accertato dalle competenti autorità canadesi che il destinatario dei dati stessi non rispetta le norme sulla loro protezione, ovvero in altre complesse ipotesi, sostanzialmente corrispondenti a quelle previste nelle decisioni relative ad Ungheria e Svizzera.

Gli Stati membri devono adottare tutte le misure necessarie per conformarsi alla decisione – modificabile in qualsiasi momento alla luce delle esperienze relative al suo funzionamento o a modifiche dell'ordinamento canadese – entro 90 giorni dalla sua notifica, il che avverrà, per l'Italia, nel breve periodo.

La deliberazione del Garante attuativa della decisione, al momento in cui il presente testo viene redatto, è in fase di predisposizione.

57 "*Safe Harbor*"

Il 10 Ottobre 2001 l'Autorità ha adottato un'autorizzazione (pubblicata in *G.U.* 26 novembre 2001) che attua la decisione n. 2000/520/CE, in base alla quale la Commissione europea ha riconosciuto che i principi internazionali di riservatezza del *Safe Harbor* (letteralmente, "approdo sicuro"), 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. Dei principi e della complessa negoziazione che ha portato alla loro determinazione si è detto nella precedente relazione (v. *Relazione 2000*, p. 86).

Anche in questa autorizzazione il Garante si riserva di controllare la legittimità dei trasferimenti e di adottare i provvedimenti ad essa eventualmente conseguenti.

Sull'applicazione della decisione 2000/520/CE, la Commissione europea ha adottato un primo documento il 13 febbraio 2002, 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.

Il documento si basa su informazioni raccolte in Europa presso le autorità di garanzia dei Paesi membri e negli Stati Uniti, presso il sito *Internet* del Dipartimento del commercio, autorità pubbliche e private in vario modo interessate all'esecuzione dei principi, nonché presso i siti delle organizzazioni aderenti all'accordo alla data del 4 giugno 2001.

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. In sintesi, viene anzitutto rilevata l'importanza, in termini di semplificazione e riduzione delle incertezze, di aver identificato uno *standard* che corrisponde all'adeguata protezione richiesta dalla direttiva, e viene altresì osservato, in linea generale, che i principi, tanto negli Usa quanto nell'Ue, sono in atto.

In proposito, per quanto riguarda gli Stati uniti, il Dipartimento del commercio cura l'elenco pubblico delle organizzazioni insediate negli Usa che hanno autocertificato la propria adesione ai principi (183 al 19 aprile 2002) ed ha assunto iniziative opportune per far conoscere agli operatori il contenuto dell'Accordo. Per quanto concerne invece l'Unione europea, i Paesi membri hanno adottato, ove richieste dai loro ordinamenti interni, le misure necessarie per consentire il flusso dei dati verso gli aderenti all'Accordo, ed è stato reso operativo l'elenco di autorità garanti cui possono rivolgersi gli aderenti per la soluzione delle dispute negli Usa.

Dei pochi interpelli negli Usa provenienti da cittadini, a conoscenza della Commissione, nessuno è rimasto in sospeso.

Sono stati segnalati alcuni problemi invece, per quanto riguarda, in sintesi, il grado di trasparenza richiesto agli aderenti all'Accordo: sia perché dai loro siti *Internet* non sempre risulta dichiarata o agevolmente visibile la dichiarazione di adesione ai principi; sia perché le politiche sulla *privacy* adottate non riflettono sistematicamente i principi stessi; sia perché i cittadini che vogliono esercitare i loro diritti sui dati che li riguardano sono spesso tenuti all'oscuro dei modi per farlo.

Inoltre, gli enti di risoluzione delle controversie possono operare senza dover pubblicamente dichiarare l'intenzione di applicare i principi, ovvero senza dover seguire pratiche di tutela della *privacy* ad essi conformi, ancorché solo 2 enti sui 6 operanti non abbiano né autocertificato la loro adesione ai principi, né dichiarato pubblicamente di agire quali enti di risoluzione di controversie per gli aderenti all'approdo sicuro.

Almeno una parte di tali problemi è stata imputata a "difetti di avviamento", ed i servizi della Commissione hanno positivamente accolto la disponibilità espressa dal Dipartimento statunitense del commercio al miglioramento del sistema.

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 tra Usa ed Ue. In tal senso, va ricordata da ultimo la visita negli Usa nel marzo 2002 di una delegazione di rappresentanti delle autorità di protezione dati europee, guidata dal Prof. Rodotà – quale Presidente del Gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE – 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 deriverà probabilmente un nuovo pronunciamento a breve del Gruppo europeo.

58 Clausole contrattuali standard

Come riferito nella scorsa relazione, il 27 marzo 2001 il Comitato previsto dall'art. 31 della direttiva 95/46/CE ha espresso parere favorevole allo schema di decisione della Commissione europea sulle clausole contrattuali standard relative al trasferimento di dati personali ad un titolare autonomo di trattamento in un Paese terzo (v. *Relazione 2000*, p. 87).

La Commissione, con decisione del 15 giugno 2001 (2001/497/CE, in *G.U.C.E.* L 181 del 4 luglio 2001), ha approvato le clausole con le quali l'importatore di dati del Paese terzo si impegna nei confronti dell'esportatore comunitario dei dati, ma anche a beneficio dei soggetti cui i dati si riferiscono, ad adottare un certo livello di protezione dei dati medesimi.

Nel dare attuazione alla decisione comunitaria – con deliberazione del 10 ottobre 2001 (riportata negli allegati) – l'Autorità, riservandosi di procedere ai necessari controlli sulla legittimità dei trasferimenti, ha altresì escluso la necessità di ottenere, se non su sua richiesta, copia del contratto relativo al trasferimento dei dati; deve comunque essere comunicata all'Autorità la scelta, effettuata in caso di controversia non risolta in via amichevole, di sottoporre la risoluzione della stessa a soggetto diverso dal Garante o dall'autorità giudiziaria (clausola 7, par. 2 e par. 1, lett. *a)*; art. 31 l. n. 675/1996).

Su un altro schema di decisione, relativo alle clausole contrattuali sul trasferimento di dati personali a responsabili del trattamento residenti in Paesi terzi, il Gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE ha espresso parere favorevole il 13 settembre 2001; il testo, ottenuto il parere favorevole da parte del Comitato previsto dall'art. 31 della medesima direttiva, è stato poi adottato con decisione della Commissione del 27 dicembre 2001 (2002/16/CE in *G.U.C.E.* L 6 del 10 gennaio 2002).

Tali clausole, che anche nel nostro Paese sono applicabili dal 3 aprile 2002 (deliberazione del Garante n. 3 del 10 aprile 2002), riguardano il trasferimento dei dati a soggetti insediati in Paesi terzi che si impegnano a riceverli dall'esportatore per trattarli per suo conto e secondo le sue istruzioni. Esse riprendono la terminologia adoperata nella direttiva – che distingue tra responsabile e incaricato del trattamento – e a cui corrispondono, nel diritto nazionale, rispettivamente le figure del titolare e del responsabile del trattamento.

Anche queste clausole, come quelle riguardanti il trasferimento ad un titolare autonomo di trattamento, non sono "obbligatorie", ma il loro utilizzo comporta che gli ordinamenti dei Paesi membri debbano riconoscere come adeguata la protezione offerta da contratti che le contengono.

Ciò non toglie da un lato che tale protezione possa essere riscontrata anche in clausole di diverso contenuto, dall'altro che permangano in capo alle autorità garanti poteri di vigilanza e di adozione dei provvedimenti conseguenti.

Una valutazione complessiva della Commissione sul funzionamento delle clausole è prevista dopo tre anni di applicazione della decisione comunitaria.

Le clausole prevedono l'applicabilità della legge del Paese membro in cui ha sede l'esportatore. Per quanto riguarda la giurisdizione, l'importatore si obbliga ad accettare la decisione dell'interessato, che agisca nei suoi confronti per il risarcimento del danno, di deferire la controversia al giudice dello Stato membro in cui ha sede l'esportatore, oppure alla mediazione di un terzo indipendente o di un'autorità di controllo, ovvero, in ordinamenti che presentino determinate garanzie di esecuzione, ad organi arbitrali.

Nella sostanza l'importatore e l'esportatore convengono l'attuazione di determinate misure, e rispondono dei rispettivi obblighi, ma i soggetti cui i dati si riferiscono possono far valere, anche verso l'importatore, la responsabilità dell'esportatore nei cui confronti non sia più possibile agire perché di fatto scomparso, non

più esistente giuridicamente, ovvero insolvente.

Da questo complesso intreccio tra i diversi piani, interno, estero e sopranazionale da un lato, e gli strumenti di diritto privato e pubblico dall'altro, con i quali si disciplina la materia del trasferimento di dati verso i Paesi terzi, si evidenzia il rilievo che decisioni e determinazioni relative al singolo caso sono destinate ad assumere e si conferma la delicatezza, prima ancora che la centralità, delle funzioni demandate alla nostra Autorità garante.

Da qui anche l'esigenza sostanziale di un continuo raffronto con l'esperienza degli altri Stati membri e, più in generale, con gli altri ordinamenti in cui si dia adeguato rilievo alla protezione dei dati personali. In tal senso assume un significato più ampio di quello che la sua formulazione palesa, la decisione con cui, il 13 dicembre 2001, il Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46/CE ha previsto la possibilità di invitare alle proprie riunioni, quali osservatori, i rappresentanti delle autorità di protezione dei dati personali dei Paesi che abbiano richiesto l'adesione alla Ue.

IL GARANTE

La nuova composizione del Collegio

59 La continuità nell'attività dell'Autorità

Il 28 febbraio 2001 la Camera dei deputati e il Senato della Repubblica hanno eletto i quattro componenti del collegio del Garante, in vista del completamento del primo mandato quadriennale che aveva avuto inizio il 17 marzo 1997, subito dopo l'approvazione della legge n. 675/1996, con l'accettazione della nomina da parte dei componenti.

Il nuovo collegio si è insediato il 19 marzo 2001, alla presenza dei professori Stefano Rodotà e Giuseppe Santaniello (già componenti del collegio nel precedente quadriennio) e degli onorevoli Mauro Paissan e Gaetano Rasi, eletti nuovi componenti il 28 febbraio 2001.

Il 19 marzo 2001 il collegio del Garante ha eletto all'unanimità il prof. Stefano Rodotà e il prof. Giuseppe Santaniello, rispettivamente come Presidente e Vice presidente dell'Autorità, ed ha dato inizio al nuovo mandato ribadendo anche il carattere collegiale dell'organo nel lavoro interno ed esterno dell'istituzione, secondo le linee già affermatesi nel corso della precedente composizione della stessa Autorità.

La trattazione dei ricorsi

60 Principali problemi esaminati

I ricorsi al Garante ai sensi dell'art. 29 della legge n. 675/1996 sono divenuti ormai, a solo tre anni dall'entrata in vigore delle norme regolamentari relative alla loro trattazione (contenute nel d.P.R. n. 501 del 1998), uno strumento di tutela utilizzato sempre più frequentemente dagli interessati (direttamente o ricorrendo al patrocinio di un legale). Molti titolari di trattamento (soprattutto enti di livello nazionale o grandi società di servizi) hanno anzi predisposto apposite unità organizzative per rispondere alle richieste provenienti dagli interessati.

Negli ultimi mesi, invero, si è registrato un flusso crescente di ricorsi: a fronte dei 381 pervenuti complessivamente al 1° giugno 2001, al 1° aprile 2002 il loro totale era già salito a 540.

Se il dato numerico è di per sé significativo, un esame del contenuto dei ricorsi medesimi sollecita ulteriori considerazioni.

Va anzitutto rilevato che si è arricchito il panorama delle posizioni giuridiche, comunque specificatamente tutelate dall'art. 13, comma 1, della legge n. 675 (le sole per le quali sia attivabile, in caso di mancato o inidoneo riscontro, il meccanismo di tutela di cui all'art. 29 della medesima legge), in concreto fatte valere. Mentre in una prima fase la quasi totalità dei ricorsi era incentrata su problematiche attinenti all'accesso ai dati, negli ultimi tempi lo spettro dei diritti di cui al medesimo art. 13, comma 1, concretamente esercitati è cresciuto e si è diversificato.

Sono infatti sempre più frequenti le richieste di integrazione, di correzione o anche di cancellazione dei dati, o le richieste di opposizione al trattamento per motivi legittimi. Conseguentemente, anche la struttura delle decisioni è divenuta più complessa. Ne sono prova molti dei dispositivi adottati nel periodo più recente che racchiudono una variegata articolazione di decisioni (accoglimenti parziali, profili di infondatezza, non luogo a provvedere).

È altresì interessante notare come sia migliorata, in generale, la qualità redazionale degli atti introduttivi, con la proposizione di domande sempre più specifiche e pertinenti: il (particolare) campo di applicazione della legge – la tutela dei dati personali – viene sempre meglio evidenziato dagli interessati, diradandosi i riferimenti ad altri plessi normativi non sempre strettamente pertinenti (come, ad esempio, le norme sull'accesso agli atti e documenti amministrativi).

Per quanto attiene infine, alle macro-aree nelle quali i ricorsi sono stati presentati, se pure si conferma la rilevanza di alcuni "filoni" emersi con forza fin dalla prima fase applicativa del nuovo strumento, nuovi settori sono stati portati all'attenzione dell'Autorità nel corso di quest'ultimo anno, i quali senza pretesa di esaustività, sono qui tratteggiati rinviando per una loro più approfondita trattazione alle singole parti della Relazione.

Accesso ai dati personali dei lavoratori. È una delle ipotesi più ricorrenti che, verosimilmente, corrisponde alla tendenza, sempre più diffusa, di chiedere al proprio datore di lavoro l'accesso al complesso dei dati personali dallo stesso detenuti, comprendendo (specie per funzionari, quadri e dirigenti) le (eventuali) valutazioni espresse in giudizi o rapporti annuali. Dopo le inevitabili difficoltà del primo momento è però possibile constatare come, nella maggior parte dei casi, le risposte dei titolari siano ora più pronte e complete e, attraverso strumenti sia cartacei, sia automatizzati, consentano ormai un'ampia possibilità di acquisizione dei dati da parte degli interessati.

Dati sanitari e dati contenuti in perizie medico legali. Si sono presentati diversi casi volti ad ottenere pieno accesso a questa particolare e delicata categoria di dati personali a seguito di richieste destinate sia ad a.s.l. o