sizioni normative che consentano tale comunicazione (quali ad es. quelle sull'accesso ai documenti amministrativi).

Al contrario, le informazioni aggiuntive possono essere comunicate ad altri soggetti pubblici anche in assenza di un'apposita disposizione che lo consenta, qualora ciò risulti necessario per lo svolgimento delle funzioni istituzionali e ne venga data previa notizia al Garante (art. 19, comma 2, d.lg. n.196/2003).

# V - La privacy e le sfide del futuro
# *Reti di comunicazioni*

## 32 Telefonia e reti di comunicazioni

### *32.1. Profili generali*

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale. Sul punto il Codice ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lg. n. 171/1998, come modificato dal d.lg. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

### *32.2. Dati relativi al traffico telefonico*

Si è già sintetizzata in altra parte della presente Relazione (cfr. parag. 1.11.) la recente vicenda che ha portato a modificare l'art. 132 del Codice e ad individuare garanzie rafforzate in riferimento al più lungo periodo di conservazione dei dati del traffico telefonico. In questa sede giova solo ricordare che il Garante, in conformità a quanto previsto dall'art. 132, comma 5, come modificato dalla legge n. 45/2004, definirà al più presto le misure e gli accorgimenti al cui rispetto è subordinato il trattamento dei dati relativi al traffico telefonico per le finalità di accertamento e repressione dei reati.

### *32.3. Fatturazione dettagliata ed altre questioni*

Anche nel corso del 2003 l'Autorità si è occupata delle questioni connesse al mascheramento delle ultime tre cifre dei numeri telefonici nelle fatture inviate agli abbonati, che rappresenta una delle misure indicate dal Codice per tutelare la riservatezza degli abbonati chiamati, nonché degli utenti diversi dall'abbonato i quali effettuino chiamate dai terminali cui corrisponde l'abbonamento.

Nonostante i numerosi provvedimenti adottati in passato dal Garante, persistono alcuni nodi problematici testimoniati anche dai perduranti reclami e segnalazioni che pervengono all'Autorità.

Delle problematiche legate all'accesso alle informazioni incluse nella fatturazione,

ai limiti all'esercizio del diritto di accesso alle chiamate "in entrata" e alle cd. chiamate di disturbo, si è già parlato (cfr. *supra*, parag. 7.5.). In questa sede occorre, invece, sottolineare che durante il 2003 il Garante ha svolto approfondimenti in materia, destinati a confluire in un imminente provvedimento sulla fatturazione dettagliata, che riguarderà, fra l'altro, gli addebiti sulla linea telefonica dovuti a chiamate verso numeri a tariffazione speciale e a chiamate in entrata che comportano un costo per il ricevente.

**Modalità di pagamento alternative alla fatturazione**

In tale occasione saranno nuovamente esaminate le problematiche relative alla possibilità che le chiamate effettuate da qualsiasi terminale vengano pagate con modalità alternative alla fatturazione, e alla necessità di garantire in taluni casi la persona fisica del chiamante, ad esempio attraverso l'uso di carte prepagate (cfr. art. 5, comma 1, d.lg. n. 171/1998; ora, art. 124, comma 2, del Codice).

In proposito, secondo quanto confermato dal Codice, va ribadita l'importanza –per la tutela della sfera privata dei chiamanti, diversi dall'abbonato– dell'effettiva e diffusa disponibilità sul mercato di tali modalità alternative, il cui preventivo accertamento da parte del Garante, oltre che per eventuali provvedimenti sfavorevoli nei confronti dei titolari del trattamento inadempienti, costituirà presupposto indispensabile per autorizzare i fornitori ad indicare nella fatturazione i numeri completi relativi alle comunicazioni (art. 124, comma 5, del Codice).

In via preliminare, l'Autorità ha comunque già predisposto una prima nota di carattere generale volta a definire le modalità alternative alla fatturazione, anche anonime, che i fornitori di servizi di telefonia devono rendere disponibili da ogni terminale.

### *32.4. Banca dati unica dei numeri di telefonia fissa e mobile e nuovi elenchi telefonici*

Con la deliberazione dell'Autorità per le garanzie nelle comunicazioni n. 36/02/Cons del 6 febbraio 2002 è stata prevista la costituzione della banca dati dove confluiranno alcuni dati personali di tutti gli abbonati e titolari di carte prepagate e in base alla quale potranno essere realizzati nuovi elenchi telefonici in formato cartaceo ed elettronico. In proposito va segnalato che è in fase avanzata l'analisi di quei profili che, nell'ambito della realizzazione di tale banca dati, riguardano più propriamente l'osservanza della normativa sulla protezione dei dati personali.

In particolare, i principali fornitori di servizi di telefonia fissa e mobile stanno predisponendo, in collaborazione con il Garante, versioni perfezionate dei modelli di informativa e consenso ispirate al rispetto della normativa sulla tutela dei dati personali, da sottoporre (tramite diverse modalità, a seconda che si tratti o meno di clienti con i quali già sussiste un rapporto) all'attenzione degli interessati, al fine dell'inserimento dei loro dati nella banca dati in discorso e, quindi, nei nuovi elenchi telefonici.

La problematica ha richiesto particolari approfondimenti, venendo in considerazione un "serbatoio" di informazioni dal quale innumerevoli soggetti potranno attingere per utilizzare dati relativi ai recapiti ed al numero di utenza degli interessati. La chiarezza, sinteticità e univocità dell'informativa è quindi essenziale per far comprendere a tutti gli abbonati le conseguenze che si determinano nel breve e medio periodo allorché si acconsenta all'utilizzo da parte di terzi dell'indirizzo o del numero di telefono anche mobile per inviare messaggi, missive, *fax*, *Sms* o *Mms*, altre chiamate vocali, ecc.

Con specifico riguardo agli elenchi, il Garante ha infatti segnalato come la relativa disciplina normativa sia stata recentemente oggetto di significative modifiche che ne hanno mutato in radice la natura e le finalità. Non a caso, quindi, il Codice ha attribuito a questa Autorità il compito di individuare, con proprio provvedimento, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati (ed ai titolari di carte prepagate) negli elenchi cartacei o elettronici disponibili al pubblico (art. 129).

Il Garante è pertanto in procinto di adottare tale provvedimento al fine di individuare, in particolare, idonee modalità di manifestazione del consenso degli interessati con riguardo sia alla semplice inclusione dei loro dati negli elenchi, sia all'utilizzo ulteriore dei medesimi dati per finalità riconducibili ad operazioni commerciali, di *marketing*, sondaggi, o simili.

### *32.5. Altre attività di cooperazione con l'Autorità per le garanzie nelle comunicazioni*

In linea con gli obiettivi individuati nel corso della riunione congiunta fra il Garante e l'Autorità per le garanzie nelle comunicazioni del 20 febbraio 2003, si è intensificata l'attività di cooperazione fra le stesse.

Oltre ad incontri su temi di interesse comune, come il nuovo elenco telefonico unico per tutti gli operatori di telefonia fissa e mobile, nonché i servizi non richiesti, il Garante ha partecipato alla consultazione pubblica relativa all'introduzione in Italia del protocollo Enum (*e-number*), ponendo l'attenzione sulle problematiche concernenti la tutela della riservatezza degli interessati.

**Protocollo Enum**

Il protocollo Enum consente infatti di associare indirizzi Internet e numeri telefonici, al fine di realizzare un numero identificativo universale in grado di instradare il traffico verso i diversi recapiti dell'interessato, rendendo quest'ultimo facilmente rintracciabile.

L'Autorità, nel formulare le considerazioni preliminari sui possibili aspetti critici della materia, ha in particolare evidenziato agli operatori aderenti all'iniziativa alcuni profili relativi alla sicurezza e protezione dei dati personali. I primi risultati della consultazione, discussi anche all'interno di un *workshop* al quale hanno partecipato pure alcuni rappresentanti di questa Autorità, sono stati pubblicati nella *Gazzetta Ufficiale* del 24 aprile 2003, n. 95, e sono disponibili sul sito Internet dell'Autorità per le garanzie nelle comunicazioni *(www.agcom.it)*.

***Carrier preselection***

Sempre nel corso del 2003 si sono svolti incontri fra alcuni rappresentanti delle due Autorità di garanzia, al fine di verificare diversi punti problematici relativi alla tematica della *carrier preselection (Cps)*, ossia del sistema mediante il quale l'abbonato può instradare il proprio traffico telefonico verso un operatore preselezionato. Ciò, con particolare riferimento agli eventuali limiti ed alle modalità dei trattamenti dei dati connessi alle procedure per la disattivazione della *Cps*. Sull'argomento, l'Autorità ha già predisposto uno schema di provvedimento volto a chiarirne gli aspetti più controversi, ad esempio la necessità o meno per l'operatore di accesso di richiedere il consenso degli interessati.

### *32.6. Servizi non richiesti e consenso dell'interessato*

Anche durante il periodo considerato il Garante ha prestato attenzione alle delicate questioni concernenti l'attivazione di contratti e servizi di telefonia mobile e fissa senza il preventivo consenso degli interessati, in riferimento a casi nei quali si verificano seri danni per gli interessati stessi. Sono stati effettuati anche taluni impegnativi interventi di carattere ispettivo. Uno degli interventi più significativi forma oggetto di trattazione dettagliata nel paragrafo di questa *Relazione* concernente le attività ispettive del capitolo relativo all'attività del Garante (cfr. *infra*, parag. 51.3.).

Sulla base delle informazioni acquisite, è già allo studio l'emanazione di un provvedimento di carattere generale volto ad offrire ulteriori indicazioni e chiarimenti in materia.

### *32.7. Comunicazioni indesiderate ed utenze telefoniche mobili*

Il fenomeno delle comunicazioni di carattere pubblicitario o informativo realizzate su utenze telefoniche mobili ha subito di recente un'enorme espansione, vista la particolare efficacia con cui l'invio di *Sms (Short message service)* permette di comunicare in tempo reale con un numero elevato di interessati, ovunque essi si trovino, con modalità che possono, tra l'altro, risultare particolarmente invasive (si pensi alle ipotesi di ricezione del messaggio in orari notturni).

L'uso pur legittimo degli *Sms* presuppone dunque apposite cautele, specificamente evidenziate da questa Autorità in alcuni provvedimenti.

Sms *istituzionali*

**Sms istituzionali**

Il Garante ha individuato i principi che i fornitori di servizi di telecomunicazioni e le amministrazioni pubbliche sono tenuti a rispettare per l'invio degli *Sms* cd. istituzionali e cioè di quei messaggi utilizzati da amministrazioni centrali o locali per campagne informative e di sensibilizzazione (ad esempio, in relazione a giornate dedicate a particolari tematiche) o per diffondere notizie ritenute di pubblica utilità (ad esempio, in tema di viabilità, avvenimenti culturali, termini di pagamento di tasse o imposte o validità di documenti).

In un provvedimento del 12 marzo 2003, l'Autorità ha innanzitutto distinto l'ipotesi dell'invio effettuato da gestori di servizi telefonici su incarico delle pubbliche amministrazioni (con utilizzazione dei dati dei propri abbonati senza trasmetterli all'amministrazione che dispone l'invio) da quella dell'inoltro effettuato direttamente dal soggetto pubblico (che ha raccolto in proprio i dati degli abbonati).

Con riguardo al primo caso, è stato osservato che l'utilizzazione dei numeri di telefonia mobile da parte dei gestori per conto della pubblica amministrazione non può prescindere dal consenso espresso degli abbonati, prestato in forma specifica e documentato per iscritto, sia per semplici comunicazioni informative (blocco del traffico, pagamento tributi, ecc.), sia per ulteriori fini di pubblica utilità legati ad eventi culturali, ricorrenze o altro.

Si è inoltre specificato che gli operatori telefonici possono inviare *Sms* istituzionali, prescindendo dal consenso, solo in caso di disastri e calamità naturali o altre reali emergenze di ordine pubblico, e che l'invio dei messaggi in deroga alla disciplina sulla protezione dei dati può essere legalmente disposto solo da un soggetto

pubblico che adotti, se consentito dalla legge, un provvedimento d'urgenza per ragioni di ordine pubblico, igiene e sanità pubblica.

L'amministrazione pubblica deve a tal fine valutare preventivamente se la norma di legge che prevede l'adozione di provvedimenti urgenti conferisca effettivamente anche il potere di derogare alla disciplina in materia di trattamento dei dati personali e che, in presenza di accertati presupposti di necessità ed urgenza, la situazione di pericolo per la popolazione non possa essere affrontata con strumenti ordinari.

Gli operatori telefonici devono, in ogni caso, informare preventivamente ed adeguatamente gli utenti della possibilità di ricevere eventuali *Sms* istituzionali, nonché della possibilità di manifestare il consenso a ricevere solo alcune categorie di informazioni e non altre. L'interessato deve avere inoltre la possibilità di esercitare i propri diritti agevolmente e gratuitamente, anche in caso di precedente manifestazione del consenso. Gli operatori devono rispettare in ogni caso l'art. 9 della legge n. 675/1996 (ora, art. 11 del Codice). Di regola devono perciò essere seguite forme di comunicazione che non implichino l'identificazione nominativa degli abbonati. Inoltre l'operatore deve utilizzare i dati nei limiti e per il tempo necessario a trasmettere il messaggio.

Con riguardo, invece, all'invio di *Sms* istituzionali direttamente da parte dei soggetti pubblici ad utenti che abbiano liberamente lasciato i propri recapiti soltanto per essere informati sull'esito di una pratica o per ricevere sistematicamente alcuni tipi di messaggi (anche tramite reti civiche), il Garante ha chiarito che l'acquisizione del consenso è esclusa per l'invio di tali comunicazioni strettamente istituzionali.

È stato comunque richiamato l'obbligo dei soggetti pubblici di informare l'utente sulle modalità e sugli scopi dell'utilizzo dei dati che lo riguardano, nonché il principio secondo cui l'uso dei dati per l'invio degli *Sms* deve essere limitato alle finalità per le quali i dati sono stati rilasciati dagli utenti all'amministrazione.

Sms *pubblicitari*

***Sms* pubblicitari**

Con un provvedimento del 10 giugno 2003 il Garante ha sottolineato l'illiceità dell'invio di *Sms* pubblicitari senza il preventivo consenso libero ed informato degli abbonati, nonché dell'espediente adottato da alcuni fornitori di servizi telefonici, di subordinare la stipula del contratto o l'attivazione della carta prepagata alla prestazione del consenso a ricevere messaggi pubblicitari. Si è pure evidenziato come sia illecito inserire tra gli obblighi contrattuali una dichiarazione *standard* di "impegno" all'invio degli *Sms* commerciali.

Anche i ben distinti messaggi con i quali le società telefoniche pubblicizzano servizi o opportunità che presuppongono un onere aggiuntivo per la clientela –come ha avuto modo di indicare l'Autorità con decisione del 9 aprile 2003– danno luogo ad un trattamento di dati a scopo promozionale ammesso solo con il consenso informato dell'interessato.

L'Autorità ha, inoltre, precisato che il principio del consenso libero ed informato trova applicazione anche nei confronti dei soggetti che trasmettono *Sms* pubblicitari senza estrarre i numeri delle utenze telefoniche da un'apposita banca dati, bensì sulla base di una composizione casuale o automatizzata di numeri, che prescinda da una verifica della loro esistenza o attivazione.

È stato chiarito, ancora, che la necessità di raccogliere una chiara e specifica manifestazione di volontà dei destinatari sussiste anche nel caso in cui gli *Sms* pubblicitari siano inviati da soggetti diversi dai fornitori di servizi di telefonia mobile, quali i fornitori di servizi telematici (ad esempio, gestori di siti *web* che offrano la possibilità di disporre gratuitamente di una casella di posta elettronica).

L'inosservanza dei principi fin qui sintetizzati è stata accertata in diversi ricorsi esaminati dal Garante nel corso dell'anno e concernenti l'invio anche notturno di *Sms* promozionali indesiderati. In questi casi l'Autorità ha avviato procedimenti autonomi rispetto a quelli instaurati con i ricorsi, al fine di verificare i presupposti per applicare sanzioni amministrative, per adottare altri provvedimenti e per l'eventuale denuncia all'autorità giudiziaria penale, in relazione ai reati che si possono configurare anche a seguito della mancata acquisizione del consenso informato degli interessati (*Provv*. 13 e 19 novembre 2003).

Il Codice, nel dettare una disciplina specifica in materia di comunicazioni commerciali non sollecitate, ha peraltro equiparato, quanto alla normativa applicabile, strumenti quali posta elettronica, *Sms*, *Mms* e *fax* (art. 130). Ne discende l'inapplicabilità, ai trattamenti effettuati con tali mezzi, delle fattispecie equipollenti al consenso dell'interessato di cui all'art. 24 del Codice e, quindi, anche l'inoperatività della disposizione riguardante, all'interno di tale articolo, i trattamenti di dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

### *32.8. Messaggi multimediali (cd.* Mms*) e videochiamate*

Completata, con l'adozione del provvedimento del 12 marzo 2003 (in *Relazione* 2002, p. 115) l'analisi delle problematiche legate ai messaggi multimediali (*Mms*), il Garante ha esaminato la questione dei trattamenti di dati personali effettuati in occasione delle cd. videochiamate, ossia delle chiamate (realizzate attualmente tramite la rete *Umts*) nel corso delle quali possono essere trasmesse, oltre a suoni, immagini dei soggetti coinvolti nella conversazione.

La caratteristica peculiare di tali trattamenti consiste nel fatto che, a differenza di quanto accade per l'invio dei *Multimedia messaging service (Mms)*, vengono raccolte immagini contestualmente all'effettuazione della chiamata, le quali riguardano peraltro contemporaneamente il chiamante, il chiamato e persone eventualmente a loro vicine.

In proposito sono in corso di predisposizione chiarimenti ed indicazioni volte ad evitare che in occasione di questo tipo di chiamate si possano violare i diritti dei soggetti a vario titolo coinvolti.

### *32.9. Localizzazione*

Con l'adozione del d.lg. n. 196/2003 è stata introdotta nel nostro ordinamento una disciplina specifica sul tema della localizzazione, che prevede apposite cautele per il trattamento dei dati relativi all'ubicazione diversi dai dati di traffico (art. 126). Ciò, sia per la specifica informativa che il titolare deve rendere preventivamente all'attivazione del servizio, sia in termini di revocabilità del consenso o momentaneo "congelamento" del servizio. La norma dispone infatti che l'interessato possa interrompere gratuitamente e mediante una funzione semplice, anche temporaneamente, il servizio a valore aggiunto.

Proprio in ragione della particolare delicatezza che caratterizza questo tipo di dati, l'Autorità adotterà entro breve termine, sulla base dei risultati di uno studio già ultimato in proposito, un provvedimento per chiarire alcuni termini della questione. Appare comunque utile ricordare che la Commissione europea ha affrontato alcuni aspetti della materia nella Raccomandazione del 25 luglio 2003 (2003/558/CE) sul trattamento delle informazioni relative alla localizzazione del chiamante sulle reti di comunicazione elettronica a fini della fornitura di servizi di chiamata di emergenza con capacità di localizzazione.

# 33 Trattamento di dati personali in Internet

*33.1. Profili generali*

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Nel corso del 2003 il Garante ha proseguito l'opera di costante monitoraggio dell'evoluzione tecnica del settore, promuovendo incontri e consultazioni con i diversi operatori, nonché con gli altri organi istituzionali interessati dalle tematiche trattate.

Si deve tenere presente, inoltre, che in ragione delle peculiarità del settore e dell'estrema rapidità con cui la tecnologia va evolvendosi, sono opportunamente destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici e di buona condotta previsti da ultimo dal d.lg. 30 giugno 2003, n. 196.

Le diverse questioni emerse nella materia in esame confermano peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell'Autorità rispetto ai trattamenti di dati personali effettuati da soggetti situati all'estero (sul punto, cfr. il *Provv.* sullo *spamming* adottato dal Garante in data 29 maggio 2003, v. subito *infra*).

L'Autorità ha partecipato attivamente ai lavori svoltisi al riguardo nelle apposite sedi quali Ocse, Commissione europea e Gruppo dei garanti europei istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

In particolare, quest'ultimo ha esaminato le problematiche connesse a Internet ed alle reti di comunicazione nel parere n. 2/2003 del 13 giugno 2003. Sono stati

affrontati i problemi posti, in termini di protezione dei dati, dai cosiddetti *"database Whois"*, consultabili in rete, che contengono informazioni utili per contattare i responsabili dei domini o di siti Internet. In tale occasione, i Garanti hanno segnalato che non dovrebbero essere resi indiscriminatamente pubblici ed accessibili a chiunque i dati contenuti in tali elenchi, come pure l'esigenza di distinguere fra dati assolutamente necessari e dati "opzionali". Inoltre, l'utilizzazione di tali registri o elenchi per finalità di *marketing*, realmente massiccia, non è ammissibile alla luce della direttiva europea sulla protezione dei dati personali in quanto non è conforme agli scopi per i quali i registri stessi sono stati istituiti.

**Database Whois**

Degli orientamenti emersi a livello europeo il Garante italiano terrà conto anche nell'esame delle diverse segnalazioni e richieste di chiarimenti pervenute in ordine all'attuale regime di conoscibilità dei dati relativi ai soggetti che registrano siti *web* (cd. *registrant*). L'Autorità ha infatti in programma l'emanazione di un provvedimento generale che fornisca alcuni chiarimenti ed indicazioni agli operatori del settore. Specifici approfondimenti sono stati svolti in tal senso in occasione del *summit* mondiale organizzato da Icann a Roma nello scorso mese di marzo, durante il quale il segretario generale dell'Autorità è stato invitato ad illustrare le prospettive esistenti in materia in Italia alla luce del Codice.

### *33.2. Messaggi di posta elettronica non desiderati e nomi a dominio*

L'Autorità ha adottato, in data 29 maggio 2003, un provvedimento generale relativo alla pratica dell'inoltro di messaggi di posta elettronica non sollecitati aventi carattere pubblicitario o commerciale (fenomeno comunemente noto come *spamming*), al fine di precisare il quadro normativo di riferimento ed offrire indicazioni utili agli operatori del settore.

Il Garante ha in primo luogo precisato che il consenso deve essere manifestato liberamente, in modo esplicito e, soprattutto, in forma chiara e differenziata rispetto alle diverse finalità ed alle categorie di servizi e prodotti offerti, prima dell'inoltro del messaggio commerciale. Tale disciplina non può essere peraltro elusa inviando una prima *e-mail* che, pur chiedendo il consenso, presenti un contenuto comunque promozionale o pubblicitario, oppure riconoscendo in concreto al destinatario un mero diritto di opposizione a ricevere in futuro altri messaggi pubblicitari (sistema cd. *opt-out*). Simili precisazioni sono coerenti con la disciplina generale in materia di comunicazioni commerciali non sollecitate dettata dal Codice, che, all'art. 130, ha recepito e rafforzato il principio della necessità del consenso preventivo ed informato (sistema cd. *opt-in*).

**Il consenso del destinatario**

Tuttavia, come anticipato nel provvedimento ora citato e, poi, confermato dallo stesso Codice (art. 130, comma 4), è stato introdotto nell'ordinamento un parziale temperamento al principio del consenso preventivo. In particolare, le aziende potranno, previa idonea informativa, inviare comunicazioni pubblicitarie o commerciali ai propri clienti con i quali già sussistono rapporti contrattuali, qualora questi ultimi abbiano in precedenza fornito, pur sempre previa idonea informativa, le proprie coordinate di posta elettronica nel contesto della vendita di un prodotto o di un servizio. Ciò, purché si tratti di prodotti o servizi analoghi a quelli per i quali era già stato instaurato un rapporto e purché sia offerta esplicitamente e senza ambiguità, all'inizio del rapporto e in occasione di ogni singolo invio, la possibilità di rifiutare tale pratica commerciale (prime indicazioni utili al

riguardo sono rinvenibili nel recente parere del Gruppo art. 29 di cui si tratta in questo stesso paragrafo).

Inoltre è stato chiarito che, nel caso in cui una società acquisisca da altre aziende banche dati contenenti indirizzi di posta elettronica, deve accertarsi che ciascun interessato abbia effettivamente acconsentito validamente alla comunicazione dell'indirizzo anche per fini di promozione pubblicitaria. In ogni caso, la società deve inviare agli interessati un messaggio di informativa, al fine di facilitare a questi ultimi l'esercizio dei diritti di cui all'art. 7 del Codice.

È stato pure ribadito il principio, più volte affermato dall'Autorità, secondo il quale la semplice conoscibilità di fatto di un indirizzo di posta elettronica (ad esempio, in quanto rinvenibile tramite *newsgroup*, *forum* o *chat*) non legittima l'invio di messaggi in assenza del preventivo consenso informato dell'interessato.

Nell'esaminare un ricorso, il Garante ha anche avuto occasione di chiarire che non richiede il preventivo consenso informato dell'interessato l'utilizzo di un indirizzo di posta elettronica rinvenibile in un *newsgroup*, qualora questo sia stato indicato dal medesimo interessato nell'ambito del gruppo di discussione per una specifica finalità e il dato venga utilizzato conformemente alla finalità indicata. In questa ipotesi, è stato ritenuto lecito l'inoltro di una *e-mail* inviata in risposta alla richiesta di informazioni formulata dal ricorrente in un *newsgroup*, poiché l'*e-mail* si riferiva appunto a questioni del tutto pertinenti e correlate con il tema oggetto di discussione (*Provv*. 21 marzo 2003).

Deve però rilevarsi che, in ragione del principio di stabilimento recepito dal Codice, qualora i messaggi provengano da Paesi terzi, il Codice stesso potrebbe risultare inapplicabile. Tuttavia, a parte la possibilità che si applichi comunque la legge penale italiana in virtù di altre circostanze relative ad esempio a reati connessi (es. truffa), vi è non di rado l'ulteriore eventualità di potersi rivolgere alle competenti autorità del Paese nel quale lo *spamming* è considerato illecito in base alla relativa disciplina nazionale.

L'attività di *spamming*, specie se sistematica ed effettuata a fini di profitto o per arrecare ad altri un danno, quando provoca un nocumento costituisce reato e può essere denunciata all'autorità giudiziaria penale (cfr. art. 167 del Codice). È sanzionato penalmente anche l'invio di messaggi indesiderati a scopo promozionale o pubblicitario omettendo l'indicazione del mittente del messaggio e dell'indirizzo fisico presso il quale i destinatari possono rivolgersi per chiedere che i dati personali non vengano più usati.

Il Garante ha intensificato le attività di controllo e verifica presso fornitori di servizi di comunicazione elettronica, individuati grazie anche alle numerosissime segnalazioni pervenute pure nel 2003. In alcuni casi ciò ha portato a sospendere le attività illecite per effetto di provvedimenti di blocco delle banche dati o di divieto di ulteriori trattamenti. Altre volte ne è poi conseguita l'adozione di sanzioni, anche a seguito delle risultanze emerse dalla trattazione dei numerosi ricorsi decisi in materia.

**Lo *spamming* nel contesto internazionale**

Il tema dello *spamming* è stato oggetto di particolare attenzione altresì a livello internazionale.

A tale questione l'Ocse ha dedicato numerosi documenti e gruppi di lavoro, trattandosi di un argomento rispetto al quale c'è una particolare sensibilità nei Paesi membri. Dopo la creazione di un apposito gruppo di discussione, cui hanno partecipato ventitre delegazioni, si è organizzato un seminario internazionale ospitato dalla Commissione europea, per tracciare un bilancio delle iniziative intraprese ed elaborare una strategia di contrasto comune. Al Garante, rappresentato dal segretario generale, è stato chiesto di svolgere una relazione sui meccanismi di *enforcement* volti ad assicurare l'effettivo rispetto della legge.

È stata ribadita da molti, in questa circostanza, l'esigenza di affrontare il tema a livello sovranazionale e con un approccio che tenga conto della tutela dei consumatori, della sicurezza informatica e della protezione dei dati personali. Anche l'elenco delle soluzioni proposte mette in luce la necessità di combinare insieme misure tecniche, legislative, disposizioni di autoregolamentazione e campagne di sensibilizzazione rivolte ad utenti ed imprese. Un forte impegno su scala internazionale in questo settore è fondamentale per preservare la fiducia dei consumatori e delle imprese nello sviluppo di Internet. Lo *spamming* può essere collegato ad altre attività illegali, ciò che comporta il rischio di un arresto nello sviluppo sia dell'*e-commerce* sia dell'*e-government*. Per tali ragioni l'Ocse ha proposto una riflessione comune tra i rappresentanti dei governi, delle imprese e del mondo accademico. In proposito è stata effettuata una raccolta di materiali e documenti frutto dei lavori.

A livello comunitario, il Gruppo dei garanti europei ha di recente ritenuto doveroso adottare un parere (Parere n. 5/2004 WP 90 del 27 febbraio 2004), al fine di fornire un'interpretazione uniforme dell'art. 13 della direttiva n. 2002/58/CE in tema di comunicazioni commerciali non richieste, evitando divergenze nel suo recepimento e nella sua concreta applicazione da parte dei diversi Stati membri. Secondo il Gruppo, il concetto di *e-mail* deve essere interpretato nel senso di ritenere che si configura una comunicazione elettronica ogni qualvolta non sia richiesta la simultanea partecipazione del mittente e del destinatario. Il requisito del previo consenso *("opt-in")*, poi, può essere derogato solo nel caso in cui i dati siano stati già forniti nell'ambito di un rapporto commerciale preesistente ed il *marketing* si riferisca a prodotti o servizi che, eventualmente riguardati anche dal punto di vista obiettivo del destinatario della comunicazione, siano "simili" a quelli oggetto del rapporto, nei termini suggeriti dal parere.

### *33.3. Il codice deontologico*

Sulla base dell'art. 133 del d.lg. n. 196/2003, il Garante, nell'ambito di una più generale collaborazione con i diversi operatori del settore, intende portare a conclusione in tempi rapidi (nonostante la complessità dell'argomento) le attività necessarie per la sottoscrizione del codice di deontologia e buona condotta sui trattamenti dei dati personali effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica. Ciò consentirà di fornire ulteriori criteri per assicurare una più adeguata informazione e consapevolezza agli utenti delle reti di comunicazione elettronica, nonché di favorire una maggiore trasparenza e correttezza nei confronti dei medesimi utenti ed il pieno rispetto dei principi di cui all'art. 11 del Codice.

Nel codice deontologico saranno disciplinati, tra l'altro, i presupposti ed i limiti entro i quali è lecito l'utilizzo della rete di comunicazione elettronica per accedere

ad informazioni archiviate nell'apparecchio dell'utente. In tale sede potranno pertanto essere individuate le regole per l'utilizzo lecito dei cd. *cookies*, ai quali fa riferimento anche la Raccomandazione n. 2/2001 del Gruppo dei garanti europei, relativa ai requisiti minimi per la raccolta di dati *on line* nell'Unione europea.

La rilevanza del codice deontologico è accresciuta dal fatto che il rispetto delle disposizioni in esso contenute costituirà condizione di liceità e correttezza del trattamento dei dati personali (art. 12, comma 3, d.lg. n. 196/2003).

# *Il trasferimento di dati personali all'estero*

## 34 I trasferimenti all'estero di dati

Con il Codice è stata aggiornata la disciplina del trasferimento dei dati personali all'estero (Parte I, Capo VII), completando il recepimento della direttiva comunitaria n. 95/46/CE. È stato ribadito il principio generale in base al quale i flussi di dati verso un Paese situato al di fuori dell'Unione europea sono consentiti solo se tale Paese assicura un adeguato livello di tutela delle persone (v., al riguardo, le autorizzazioni rilasciate negli anni scorsi dal Garante in relazione al livello di adeguatezza del sistema di tutela dei dati personali previsto in Svizzera ed Ungheria, nonché ai principi del Safe Harbor circa il trasferimento dei dati verso gli Stati Uniti), ovvero se sussiste uno dei presupposti di liceità indicati dalla normativa nazionale (consenso dell'interessato, adempimento di obblighi contrattuali, ecc.).

Anche nel corso del 2003 e nei primi mesi del 2004, significativa è stata l'attività svolta dal Garante per dare attuazione ad alcune decisioni comunitarie relative al settore in esame.

Si segnalano, al riguardo:

- la deliberazione n. 6 del 30 aprile 2003, con cui l'Autorità italiana ha dato attuazione alla decisione della Commissione europea del 20 dicembre 2001, con la quale si è ritenuto adeguato il livello di protezione dei dati personali in Canada (v. *Relazione* 2002, p. 128);

- la deliberazione n. 2 del 15 aprile 2004, con cui il Garante ha attuato la decisione comunitaria del 21 novembre 2003 n. 2003/821/CE, recante il riconoscimento del Bailato di Guernsey tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali.

A tale ultimo riguardo va specificato che il Gruppo dei garanti europei istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, nel proseguire la propria attività di valutazione dell'adeguatezza del livello di protezione garantito da Stati non appartenenti all'Ue, si era pronunciato favorevolmente sul Bailato di Guernsey con il parere n. 5/2003 del 13 giugno 2003. Di conseguenza, la Commissione europea ha adottato la citata decisione n. 2003/821/CE con la quale ha stabilito che il livello di protezione dei dati nel territorio di Guernsey è "adeguato" ai fini del trasferimento di dati personali dall'Ue verso soggetti ivi residenti.

Sempre nella materia in esame, è in procinto di essere resa operativa in Italia anche la decisione della Commissione europea n. 2003/490/CE del 30 giugno 2003, riguardante l'adeguatezza del livello di tutela dei dati personali esistente in Argentina, su cui si era già espresso in senso favorevole, con il parere n. 4 del 3 ottobre 2002, il Gruppo dei garanti europei.

Infine, una decisione di contenuto analogo è in procinto di essere adottata dalla Commissione europea anche per l'Isola di Man, alla luce del parere favorevole del Gruppo (Parere n. 6/2003 del 21 novembre 2003).

Come anticipato nella *Relazione* per il 2002 (v. ivi, p. 127), il 2003 è stato inoltre caratterizzato da un intenso monitoraggio da parte dell'Autorità sulle attività di trasferimento di dati all'estero effettuate da alcuni operatori italiani, con particolare riguardo al tipo di garanzie adottate per tutelare i diritti degli interessati. Ciò allo scopo di verificare lo stato di attuazione delle disposizioni comunitarie e nazionali sui flussi di dati all'estero, prima di avviare specifici accertamenti relativi a singole società.

**Indagine del Garante sulle attività di trasferimento dei dati**

Dall'indagine svolta è emerso che:

- circa l'84% delle società interpellate effettua trasferimenti di dati all'estero; le aree geografiche di maggiore interesse sono rappresentate dagli Usa, dall'Europa dell'Est, dall'America centro-meridionale, dall'Africa, dalla Svizzera e dall'Asia;

- nel 40% circa dei casi analizzati, i dati personali oggetto di trasferimento all'estero riguardano principalmente dipendenti e, in misura minore, ma comunque non trascurabile, anche altre società o imprese (in qualità di clienti, concorrenti, fornitori, ecc.);

- i flussi di dati sono stati o sono effettuati, di regola, previa acquisizione del consenso specifico degli interessati o sulla base degli altri presupposti di legge (ad es., per l'esecuzione di obblighi contrattuali);

- soltanto in un numero ristretto dei casi esaminati (il 5% circa), relativi a flussi stabili e più complessi di dati, le società interpellate hanno utilizzato le clausole contrattuali *standard* indicate dalla Commissione europea;

- in alcune limitate ipotesi, caratterizzate dal fatto che la gestione delle risorse umane viene effettuata negli Usa, gli importatori dei dati (società capogruppo o comunque collegate o controllate) hanno aderito all'accordo sui principi del *Safe Harbor*, dichiarandosi in genere disponibili a cooperare con le autorità per la protezione dei dati dei Paesi europei.

L'indagine dimostra che nuovi strumenti, come le clausole contrattuali, cominciano ad essere utilizzati nell'ambito delle prassi economiche e commerciali con aziende di altri Paesi e che tali strumenti possono essere ancora migliorati, in particolare con riguardo alla disciplina di fenomeni più complessi e frequenti a livello internazionale, quali quelli relativi a gruppi societari, a rapporti multilaterali tra imprese, o al conferimento a terzi, all'estero, di attività o servizi precedentemente svolti in proprio (cd. *outsourcing*).

In argomento, il Gruppo di lavoro istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE ha evidenziato l'opportunità di introdurre eventuali correttivi, prevedendo ulteriori garanzie e regole di comportamento in aggiunta alle clausole contrattuali tipo già predisposte (v. il paragrafo seguente).

# 35 Le clausole contrattuali tipo

Diverse imprese e gruppi societari, operanti a livello internazionale, si sono rivolti al Garante per ottenere informazioni e chiarimenti sulla corretta applicazione della normativa in materia di trasferimento all'estero dei dati personali.

In particolare, l'Autorità ha esaminato un caso relativo alla realizzazione a livello internazionale di un sistema informativo centralizzato di gestione delle risorse umane di diverse società situate in vari Stati dell'Ue, tra cui l'Italia, affidato in *outsourcing* ad una società con sede negli Usa (ipotesi frequente in questi ambiti).

**Contratto globale**

Al fine di rendere lecito il trasferimento all'estero dei dati dei dipendenti nell'ambito di questa operazione, è stato sottoscritto, anche per conto delle società appartenenti ai gruppi societari coinvolti nella gestione di tali dati, un contratto cd. globale basato sulle clausole contrattuali-tipo relative ai flussi transfrontalieri di dati tra autonomi titolari del trattamento (cfr. decisione della Commissione europea del 15 giugno 2001, n. 2001/497/CE, attuata in Italia attraverso l'autorizzazione generale del Garante n. 35 del 10 ottobre 2001).

Le clausole contrattuali-tipo consentono alle imprese di trasferire dati personali nel rispetto dei principi della direttiva anche quando il Paese di destinazione non abbia una legislazione adeguata, prevedendo idonee garanzie attraverso strumenti negoziali.

Sulla base delle osservazioni formulate dal Garante e dalle altre Autorità di controllo europee interpellate, è stato predisposto poi uno schema di contratto integrativo del precedente, basato sulle clausole contrattuali-tipo indicate nell'autorizzazione generale n. 3 del 10 aprile 2002 e relative al trasferimento dei dati a responsabili del trattamento residenti in Paesi terzi.

L'Autorità si è, inoltre, espressa favorevolmente circa il mantenimento, nel contratto integrativo, della previsione di una responsabilità disgiunta e solidale dell'esportatore e dell'importatore dei dati per i danni subiti dagli interessati a causa della violazione delle regole contrattuali. Le imprese od enti che si avvalgono dei contratti *standard* possono infatti inserire ulteriori clausole pertinenti, purché non risultino limitative o incompatibili con le clausole-tipo approvate dalla Commissione europea. Si è ritenuto pertanto opportuno conservare nello schema di contratto la clausola sulla responsabilità appena descritta, in quanto espressiva di una maggiore garanzia per il risarcimento dei danni eventualmente causati agli interessati: questi ultimi potrebbero così attivare direttamente un'azione legale nei confronti di entrambe le parti contrattuali.

L'Autorità ha sottolineato, infine, la necessità che lo schema di contratto stipulato tra le società interessate anche in nome e per conto delle rispettive società controllate e collegate venga sottoscritto da ciascuna di queste società o, comunque, dalla maggior parte di quelle per le quali la capogruppo non abbia uno specifico mandato o procura a rappresentarle.

L'Autorità è anche giunta alla conclusione di considerare applicabile allo schema di contratto in esame l'autorizzazione generale n. 3 del 10 aprile 2002: non è,

quindi, necessario il rilascio di una specifica autorizzazione del Garante per trasferire all'estero i dati in questione.

Sempre in tema di trasferimento dei dati verso Paesi non appartenenti all'Ue (cd. Paesi terzi), il Gruppo dei garanti europei ha approfondito e sviluppato il lavoro sulle clausole contrattuali-tipo.

***Binding corporate rules***

Il Gruppo ha avviato una riflessione su quest'ultimo punto con riferimento al livello di tutela che può essere garantito dall'adozione di norme che possono apportare un vincolo nell'impresa (cd. *binding corporate rules*), una sorta di codici di condotta elaborati nell'ambito di un gruppo di imprese e impegnativi per tutti i soggetti che ne fanno parte. Con un documento di lavoro (WP del 3 giugno 2003) sono state formulate alcune indicazioni preliminari sulle condizioni in base alle quali questi speciali codici di condotta possono offrire garanzie sufficienti ai fini del trasferimento di dati verso Paesi terzi che non dispongano di un livello adeguato di protezione dei dati, con particolare riferimento ai trasferimenti fra società appartenenti ad uno stesso gruppo multinazionale.

Un modello alternativo di clausole contrattuali-tipo rispetto a quelle approvate con la decisione della Commissione n. 497/2001/CE ha formato oggetto di un successivo parere (Parere 8/2003 del 17 dicembre 2003). Il Gruppo ha espresso una valutazione positiva su un progetto di clausole contrattuali presentato dalla Camera di commercio internazionale e da altre organizzazioni commerciali, suggerendo alcune modifiche al fine rendere il livello di tutela equiparabile a quello delle clausole approvate dalla Commissione.