Stato di attuazione del Codice in materia di protezione dei dati personali

PAGINA BIANCA

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Principali interventi dell'Autorità nel 2007

1.1. *Provvedimenti più significativi*

1.1.1 *Banche dati Dna, Ris dell'Arma dei carabinieri e Ced del Dipartimento di pubblica sicurezza*

Il Garante ha inviato al Parlamento e al Governo una segnalazione, adottata il 19 settembre 2007 [doc. *web* n. 1456163], in relazione alle iniziative legislative che si sono registrate sul finire della XV legislatura per l'istituzione di una banca dati del Dna a fini di sicurezza e giustizia, con la quale ha individuato gli aspetti per i quali l'Autorità ritiene opportuno un intervento normativo e ha indicato le garanzie da assicurare alle persone interessate.

Il Garante, nel condividere l'esigenza di disciplinare organicamente la materia e potenziare le tecniche di indagine, anche per scopi di cooperazione internazionale, ha osservato che vi sono rilevanti effetti sui diritti e le libertà fondamentali delle persone; pertanto, una normativa adeguata sull'uso e la gestione dei dati relativi al Dna per finalità di accertamento e repressione dei reati dovrebbe prendere in esame alcuni profili fondamentali. In particolare, l'Autorità ha richiamato l'attenzione del Parlamento e del Governo sui seguenti aspetti:

- la banca dati dovrebbe avere esclusive finalità specifiche di identificazione delle persone, anche in armonia con quanto previsto dal Trattato di *Prüm* sulla cooperazione transfrontaliera e dalla normativa europea;
- la banca dati deve contenere solo profili Dna (sequenze alfanumeriche) e le relative informazioni non devono essere duplicate in altri archivi di singole forze di polizia;
- considerata la particolare delicatezza e natura dei dati genetici, che riguardano non soltanto l'individuo, ma il suo intero gruppo biologico, i relativi campioni non devono essere conservati in forma di banca dati e devono essere applicati sistemi di analisi che non consentano di individuare patologie di cui sia eventualmente affetto l'interessato;
- gli operatori che possono accedere ai dati devono essere individuati con modalità selettive e solo in rapporto ad attività investigative previste o disposte per legge;
- sempre per la particolare delicatezza di queste informazioni, occorre assicu-

rare un elevato livello di sicurezza e qualità dei dati tale da consentire il tracciamento di ogni accesso e lo svolgimento periodico di adeguate procedure di controllo;

- occorrono specifiche indicazioni circa le modalità con le quali le persone i cui dati sono conservati possano esercitare i diritti loro riconosciuti dal Codice *privacy*, ovvero l'accesso, l'aggiornamento, o l'eventuale cancellazione dei dati.

L'Autorità ha inoltre raccomandato di prestare la massima attenzione all'ambito della raccolta dei dati e ai motivi che la giustificano. L'istituzione di una banca dati a livello nazionale non impone necessariamente l'introduzione di un prelievo obbligatorio del Dna poiché un tale archivio può essere utilmente composto da dati raccolti nell'ambito di procedimenti penali, già molto numerosi. Tuttavia, per il caso in cui il Parlamento ritenesse di stabilire un prelievo obbligatorio per alcune categorie di soggetti (fermati, arrestati, indagati, imputati o condannati), l'Autorità ha sottolineato la necessità di individuare in maniera proporzionata i soggetti interessati e i relativi reati, da definire sulla base della loro gravità.

Il Garante ha infine concordato sull'utilità di specifiche previsioni che confermino i compiti di vigilanza e controllo dell'Autorità stessa su tali trattamenti di dati, anche con riferimento a un eventuale rapporto periodico al Parlamento.

Le indicazioni espresse nella segnalazione sono state richiamate e specificate nel parere che il Garante ha reso successivamente sullo schema di disegno di legge presentato dal Governo per l'istituzione della banca dati (*Parere* 15 ottobre 2007 [doc. *web* n. 1448799]).

Nel corso del 2007 è altresì proseguita l'istruttoria sull'utilizzo dei dati genetici per finalità di polizia giudiziaria da parte del Reparto investigazioni scientifiche dell'Arma dei carabinieri di Parma (*v. Relazione* 2006, p. 138). Al termine degli accertamenti, con *provvedimento* del 19 luglio 2007 adottato ai sensi degli artt. 143, 144, 154 e 160 del Codice, il Garante ha prescritto all'Arma dei carabinieri-Reparto investigazioni scientifiche di Parma di effettuare l'ulteriore utilizzo dei campioni biologici e dei profili genetici, anche con specifico riferimento all'attività di comparazione, in conformità a quanto disposto dalle competenti autorità giudiziarie e alle condizioni e nei limiti previsti dal codice di procedura penale; ha, altresì, impartito una serie di prescrizioni per rafforzare il livello di protezione dei profili genetici e dei campioni biologici conservati presso il Reparto.

Analogamente, seppure in relazione a profili tematici diversi da quelli sopra menzionati, con il *provvedimento* adottato l'8 maggio 2007 e relativo ai trattamenti dei dati posti in essere presso il Centro elaborazione dati (Ced) del Dipartimento della pubblica sicurezza del Ministero dell'interno, sulla base di accertamenti avviati nel 2006 (*cfr. Relazione* 2006, p. 72-73), il Garante ha prescritto le modificazioni da apportare ai trattamenti di dati personali svolti presso il Centro allo scopo di dare attuazione agli obblighi stabiliti dal Codice e dai princìpi posti nella Raccomandazione n. R(87) 15 del Consiglio d'Europa. Ciò, con particolare riferimento alla pertinenza e aggiornamento dei dati, alle informazioni acquisite da attività amministrative, ai tempi di conservazione dei dati, alla connessione con altre banche dati e all'esercizio dei diritti da parte degli interessati.

1.1.2. *Conservazione e sicurezza dei dati di traffico telefonico e telematico*

Vi sono stati alcuni interventi di particolare rilievo sulla conservazione dei dati di traffico telefonico e telematico volti a contemperare le esigenze di tutela della sfera privata di milioni di cittadini e le esigenze funzionali della magistratura e delle forze di polizia.

Con deliberazione del 19 settembre 2007 [doc. *web* n. 1442463], il Garante ha avviato una consultazione pubblica sulle regole essenziali per la messa in sicurezza dei dati conservati a fini di accertamento e repressione dei reati. Sono state interpellate le istituzioni interessate (in particolare Ministero della giustizia, Ministero dell'interno e Csm), le aziende e le relative associazioni di categoria, nonché le associazioni dei consumatori, allo scopo di adottare un provvedimento definitivo sulla base delle osservazioni pervenute.

Il documento oggetto della consultazione, frutto di un'attività anche ispettiva molto articolata, iniziata alla fine del 2005, indica in maniera organica le misure da rispettare per la conservazione dei dati a fini di giustizia da parte dei fornitori di servizi di comunicazione elettronica.

In particolare il documento, nel chiarire i soggetti destinatari e i dati oggetto di conservazione, stabilisce prescrizioni tecnico organizzative riguardo alla loro tenuta e alla loro messa in sicurezza.

Sono esclusi dall'ambito di applicazione di queste misure i gestori di esercizi pubblici e *Internet café*, di siti Internet che diffondono contenuti sulla rete (*"content provider"*), e di motori di ricerca, nonché le aziende o le amministrazioni pubbliche che mettono a disposizione del personale reti telefoniche e informatiche (*ad es.*, centralini aziendali) o che si avvalgono di *server* messi a disposizione da altri soggetti.

Le garanzie di base per la messa in sicurezza dei dati sono state poi individuate con *provvedimento* del 17 gennaio 2008, (in *G.U.* n. 30 del 5 febbraio 2008 [doc. *web* n. 1482111]), anche alla luce delle osservazioni pervenute nel corso della consultazione pubblica.

I dati di traffico telefonico e Internet sono particolarmente delicati: numero chiamato, data, ora, durata della chiamata, localizzazione del chiamante nel caso del cellulare, dati inerenti agli *Sms* o *Mms*, indirizzi *e-mail* contattati, data, ora e durata degli accessi alla rete consentono infatti di ricostruire tutte le relazioni di una persona e le sue abitudini.

Le garanzie riguardano, in sintesi:

Accesso ai dati: quest'ultimo è consentito solo al personale incaricato e mediante avanzati sistemi di autenticazione informatica, anche con l'uso di dati biometrici (*ad es.*, impronte digitali). Sono compresi nell'ambito applicativo della prescrizione, salvo limitati casi di necessità, gli amministratori di sistema, figure chiave della sicurezza delle banche dati sul cui ruolo, spesso sottovalutato anche nei settori più delicati, l'Autorità avvierà una più approfondita riflessione.

Accesso ai locali: i locali in cui sono ospitati i sistemi di elaborazione che trattano dati di traffico telefonico per esclusive finalità di giustizia devono disporre di sistemi biometrici di controllo degli accessi. In ogni caso, i sistemi che trattano dati di traffico di qualsiasi natura vanno installati in locali ad accesso selezionato.

Sistemi di autorizzazione: le funzioni tra chi assegna le credenziali di autenticazione e chi accede ai dati devono essere separate rigidamente. I profili di autorizzazione da attribuire agli incaricati devono essere differenziati a seconda che il trattamento dei dati di traffico sia effettuato per scopi di ordinaria gestione o per quelli di accertamento e repressione dei reati.

Tracciamento dell'attività del personale incaricato: ogni accesso effettuato e ogni operazione compiuta da parte degli incaricati e degli amministratori di sistema devono essere registrati in appositi *audit log*.

Conservazione separata: i dati tenuti per esclusive finalità di accertamento e repressione dei reati devono essere conservati separatamente da quelli utiliz-

zati per funzioni aziendali (*ad es.*, fatturazione, *marketing*, antifrode, statistiche) e i sistemi di elaborazione che li trattano vanno sottoposti a rigide misure di sicurezza fisica e controllo degli accessi.

Cancellazione dei dati: una volta decorso il tempo previsto di conservazione i dati devono essere immediatamente cancellati o resi anonimi, eliminandoli anche dalle copie di *backup* create per il salvataggio dei dati.

Controlli interni: devono essere effettuati controlli periodici sulla legittimità degli accessi ai dati da parte degli incaricati, sul rispetto delle norme di legge e delle misure organizzative tecniche e di sicurezza prescritte dal Garante, sull'effettiva cancellazione dei dati una volta decorsi i termini di conservazione.

Sistemi di cifratura: contro i rischi di acquisizione indebita, anche fortuita, delle informazioni registrate da parte di incaricati di mansioni tecniche (amministratori di sistema, amministratori di *database*, manutentori *hardware* e *software*), i dati di traffico trattati per esclusive finalità di giustizia devono essere protetti con tecniche crittografiche.

I fornitori di servizi di comunicazione elettronica dovranno applicare tali misure entro il 31 ottobre 2008. L'introduzione di alcune di esse è stata disposta dal Garante anche in relazione alla conservazione dei dati per finalità non di giustizia, (fatturazione, commercializzazione di servizi, statistica *ecc.*), al fine di favorire un quadro più ampio di sicurezza di dati e sistemi.

Prima del recente recepimento della direttiva europea in materia, il *cd.* decreto "milleproroghe" (d.l. 31 dicembre 2007, n. 248 conv. con legge 28 febbraio 2008, n. 31), ha, tuttavia, stabilito che i tempi di conservazione potevano, in sostanza, giungere a otto per i dati di traffico telefonico e superare i tre per quelli telematici.

Con lettere inviate al Presidente della Camera dei Deputati ed al Ministro delle Politiche Europee, il Garante ha quindi ribadito le proprie preoccupazioni sui tempi di conservazione dei dati detenuti per finalità di giustizia. L'Autorità ha richiamato l'esigenza che il bilanciamento degli interessi coinvolti sia conforme alle prescrizioni della predetta direttiva comunitaria (la *cd.* "direttiva Frattini") e che quest'ultima, la quale prevede tempi di conservazione dei dati di traffico sia telefonico che telematico compresi tra un minimo di sei mesi ed un massimo di due anni, fosse tempestivamente recepita; ha perciò auspicato l'introduzione di alcune modifiche correttive in sede di conversione del decreto, affinché fosse specificato che il periodo di conservazione dei dati era prorogato solo fino all'entrata in vigore del decreto di recepimento della direttiva e, comunque, non oltre il 31 dicembre 2008.

Con i provvedimenti del 10 gennaio 2008, a tutela degli utenti di alcuni dei maggiori gestori di servizi telefonici e telematici, è stata imposta a Telecom Italia S.p.A. [doc. *web* n. 1524263], Vodafone Omnitel N.V., [doc. *web* n. 1484758], e H3G S.p.A. [doc. *web* n. 1484726], la cancellazione di informazioni, conservate illegittimamente, riguardanti i siti Internet visitati dagli utenti. A Vodafone, H3G e Wind telecomunicazioni S.p.A. è stata impartita l'adozione di specifiche misure tecniche per la messa in sicurezza dei dati personali conservati a fini di giustizia.

I gestori devono infatti conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di traffico apparentemente "esterni" alla comunicazione (pagine *web* visitate o gli indirizzi *Ip* di destinazione) e che possono peraltro coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire meglio relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

La mancata adozione di alcune misure di sicurezza e l'indebita conservazione dei dati sulla navigazione in Internet era emersa nel corso dell'attività ispettiva disposta dal Garante anche nell'ultimo anno al fine di verificare il rispetto del Codice e delle

prescrizioni impartite dall'Autorità con il *provvedimento* del 15 dicembre 2005 [doc. *web* n. 1203890] riguardo alla protezione dei dati di traffico telefonico conservati a fini di giustizia e alle modalità con le quali i gestori di telefonia, fissa e mobile, adempiono alle richieste dell'autorità giudiziaria in materia di intercettazioni.

1.1.3. *Posta elettronica e rete Internet*

Soggetti privati come le società non possono svolgere attività di monitoraggio sistematico finalizzato all'individuazione di utenti che si scambiano *file* musicali o giochi su Internet.

Questa la decisione adottata il 28 febbraio 2008 [doc. *web* n. 1495246] al termine dell'istruttoria avviata sul "caso Peppermint", la società discografica con sede in Germania che aveva svolto, attraverso una società svizzera (la Logistep, utilizzata anche dalla società Techland sp. z.o.o., la quale commercializza giochi elettronici avente sede in Polonia), un monitoraggio delle reti *peer to peer* (P2p). Tramite l'utilizzo di uno specifico *software*, le società avevano individuato numerosissimi indirizzi Ip (che identificano i *computer* collegati ad Internet) relativi a utenti ritenuti responsabili dello scambio illegale di *file*: erano poi risalite ai nominativi degli utenti, anche italiani, al prevalente fine di potere ottenere un risarcimento del danno.

Il Garante ha ritenuto illecita l'attività svolta dalle società, richiamando anche la decisione dell'omologa autorità svizzera del 9 gennaio 2008 (*cfr. www.edoeb.admin.ch*).

Al riguardo, sono state altresì considerate le ordinanze con cui il Tribunale di Roma –come richiesto dal Garante– ha rigettato alcuni ricorsi con i quali le società Peppermint e Techland intendevano ottenere da taluni fornitori di servizi di comunicazione elettronica la trasmissione delle generalità dei soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer to peer*. Tale profilo della comunicazione dei dati di traffico è stato esaminato, da ultimo, dalla Corte di giustizia delle Comunità europee la quale si è pronunciata su una questione per molti aspetti simile (sentenza 29 gennaio 2008, pronunciata nella causa C-275/06 Promusicae c/ Telefonica de Espana Sau), escludendo la possibilità che tali dati potessero essere messi a disposizione per controversie civili relative ai diritti di proprietà intellettuale (*cfr.* punto 48 della sentenza; artt. 15, n. 2, e 18 della direttiva 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della Società dell'informazione, in particolare il commercio elettronico, nel mercato interno; artt. 8, nn. 1 e 2 direttiva 2001/29/Ce sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; art. 8 direttiva 2004/48/Ce sul rispetto dei diritti di proprietà intellettuale; artt. 17, n. 2 e 47 Carta dei diritti fondamentali dell'Unione europea).

La decisione del Garante del 28 febbraio ricorda che la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati, specie nei riguardi di un numero elevato di soggetti; ritiene poi violato il principio di finalità, essendo le reti P2p finalizzate allo scambio tra utenti di dati e *file* per scopi personali. Il predetto utilizzo dei dati dell'utente può avvenire, dunque, soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno).

Infine, non sono stati rispettati i princìpi di trasparenza e correttezza in quanto i dati sono stati raccolti ad insaputa sia degli interessati, sia di abbonati che non erano necessariamente coinvolti nello scambio di *file*.

Nel *provvedimento* si è stabilito quindi che entro il 31 marzo 2008 le società che

hanno effettuato il monitoraggio dovevano cancellare i dati personali degli utenti che hanno scambiato *file* musicali e giochi attraverso il sistema P2p.

1.1.4. *Misure in materia di propaganda elettorale*

In vista dell'avvio della campagna elettorale, con deliberazione del 28 febbraio 2008 (in *G.U.* n. 58 dell'8 marzo 2008 [doc. *web* n. 1493909]), l'Autorità ha consentito a partiti e candidati di non adempiere temporaneamente all'obbligo di informativa fino al 31 luglio 2008, rispetto ai dati raccolti da registri ed elenchi pubblici, in caso di invio di materiale propagandistico di dimensioni ridotte (*cd.* "santini").

La deliberazione richiama le modalità –fissate da uno specifico *provvedimento* generale del 7 settembre 2005 (in *G.U.* 12 settembre 2005, n. 212 [doc. *web* n. 1165613])– in base alle quali chi effettua propaganda elettorale può utilizzare correttamente i dati personali dei cittadini (*ad es.*, indirizzo, telefono, *e-mail ecc.*).

Per contattare gli elettori e inviare materiale di propaganda, partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono usare, senza il consenso dei cittadini, i dati contenuti nelle liste elettorali detenute dai comuni. Possono essere usati anche altri elenchi e registri in materia di elettorato passivo ed attivo (*ad es.*, elenco degli elettori italiani residenti all'estero) nonché altre fonti documentali detenute da soggetti pubblici se liberamente accessibili a chiunque e secondo le modalità eventualmente stabilite per accedere ad esse. Partiti e candidati possono inoltre usare lecitamente i dati personali di iscritti ed aderenti.

Per i titolari di cariche elettive vi è la possibilità di utilizzare dati raccolti nel quadro delle relazioni interpersonali con cittadini ed elettori.

Per particolari modalità di comunicazione elettronica come *Sms*, *e-mail*, *Mms*, telefonate preregistrate e *fax*, è necessario il consenso dell'interessato, che deve precedere la chiamata o il messaggio. Il consenso deve essere parimenti ottenuto nel caso si utilizzino dati raccolti automaticamente su Internet o ricavati da *forum* o *newsgroup*, liste abbonati a un *provider* o dati presenti sul *web* per altre finalità.

Possono essere presi in considerazione anche i dati degli abbonati presenti nei nuovi elenchi telefonici accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere posta o telefonate. Sono ugualmente utilizzabili, se si è ottenuto preventivamente il consenso degli interessati, i dati relativi a simpatizzanti o ad altre persone già contattate per singole iniziative o che vi hanno partecipato (*ad es. referendum*, proposte di legge, raccolte di firme).

Non sono invece in alcun modo utilizzabili, neanche da titolari di cariche elettive, gli archivi dello stato civile, l'anagrafe dei residenti, gli indirizzi raccolti per svolgere attività e compiti istituzionali o per prestazioni di servizi, anche di cura, le liste elettorali di sezione già utilizzate nei seggi, nonché i dati annotati privatamente nei seggi da scrutatori e rappresentanti di lista, durante operazioni elettorali.

Un *provvedimento* di analogo contenuto era stato adottato il 3 maggio 2007 (in *G.U.* n. 130 del 7 giugno 2007 [doc. *web* n. 1409206]) in vista delle elezioni amministrative.

1.1.5. *Trattamento di dati personali di lavoratori per la gestione del rapporto di lavoro in ambito pubblico*

Sono state individuate in un quadro unitario le misure e gli accorgimenti da adottare per garantire la riservatezza dei dati personali dei dipendenti pubblici senza venire meno al principio di trasparenza della pubblica amministrazione. Le linee-guida del 14 giugno 2007 (in *G.U.* 13 luglio 2007, n. 161 [doc. *web* n. 1417809]), che seguono quelle adottate per i lavoratori privati (in *G.U.* 7 dicembre 2006, n. 285 [doc. *web* n. 1364099]), oltre a fornire orientamenti utili per cittadini e amministra-

zioni pubbliche rispondono anche a numerose segnalazioni e quesiti rivolti Garante. Questi, in sintesi, alcuni dei punti principali del *provvedimento.*

Assenze per malattia, certificati e visite mediche

In caso di assenza per malattia, all'amministrazione vanno consegnati certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio deve astenersi dall'utilizzare queste informazioni e deve invitare il personale a non produrre altri certificati aventi le stesse caratteristiche. Particolari cautele devono essere adottate dall'ente pubblico quando tratta dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio all'Inail, abilitazioni al porto d'armi e alla guida.

Diffusione dei dati in Internet

Nell'utilizzare Internet come strumento di diffusione di dati personali (*ad es.*, per graduatorie e giudizi di valutazione), occorre prevedere forme adeguate di selezione delle informazioni che potrebbero essere altrimenti reperite indiscriminatamente mediante un comune motore di ricerca esterno ai siti. Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati effettivamente pertinenti (si pensi ad elenchi nominativi abbinati ai risultati, agli elenchi di ammessi alle prove scritte o orali, ai recapiti telefonici, al codice fiscale, *ecc.*). É sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati.

Dati biometrici dei lavoratori pubblici

Anche nell'ambito del pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (in particolare impronte digitali, iride) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare l'attivazione di tali sistemi di rilevazione solo in presenza di particolari esigenze (*ad es.*, per l'accesso ad aree adibite alla sicurezza dello Stato o alla conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, impiego di codice cifrato dell'impronta memorizzato nel solo *badge* del dipendente e non in archivi centralizzati).

Comunicazioni tra amministrazione e lavoratore

Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione deve adottare forme di comunicazione con il dipendente protette e individualizzate, inoltrando, ad esempio note in busta chiusa o inviandole a una *e-mail* personale o invitando l'interessato a ritirare personalmente la documentazione.

1.1.6. *Trattamento di dati personali della clientela in ambito bancario*

Con *provvedimento* generale del 25 ottobre 2007 (in *G.U.* n. 273 del 23 novembre 2007 [doc. *web* n. 1457247]), sono state adottate, anche alla luce delle segnalazioni e dei reclami pervenuti all'Autorità, le linee-guida sul "trattamento dei dati personali della clientela in ambito bancario", con le quali sono state individuate alcune garanzie per il corretto uso dei dati personali dei clienti da parte degli istituti bancari e degli operatori postali. Il Garante ha evidenziato, in particolare, che le comunicazioni di informazioni bancarie a terzi devono essere effettuate solo nei casi espressamente previsti dalla legge, dal Codice o quando sia l'interessato stesso ad autorizzare terzi (familiari, coniuge, professionisti legati da una rapporto di lavoro) ad operare per suo conto o a conoscere il tipo di rapporto intrattenuto con la banca. Le banche possono registrare le telefonate effettuate dalla clientela per dare particolari ordini e istruzioni o nei servizi di *"telephone banking"*, ma devono informare gli interessati. È inoltre necessario adottate misure di sicurezza contro l'alterazione o l'uso indebito del contenuto delle conversazioni. Occorre poi evitare indebite comunicazioni di dati a terzi: il personale deve pertanto astenersi dall'effettuare telefonate e colloqui con la clientela ad alta voce e in presenza di terzi e occorre predisporre distanze di cortesia agli sportelli. Le informazioni dei clienti trattate dalle banche devono essere sempre esatte e aggiornate e il cliente ha diritto ad ottenere la comunicazione in forma intelligibile dei

dati che lo riguardano (comprese le operazioni effettuate, le registrazioni telefoniche e gli ordini di investimento), ma non di quelli riferiti ad altre persone (se presenti, nella copia dei documenti da consegnare al cliente devono essere quindi oscurati). Nel caso infine che i titolari del trattamento siano cessionari di sportelli bancari essi possono effettuare l'informativa mediante pubblicazione della stessa nella Gazzetta ufficiale e una successiva comunicazione agli interessati alla prima occasione utile.

1.1.7. *Trattamento di dati personali in ambito assicurativo*

Con *provvedimento* del 26 aprile 2007 [doc. *web* n. 1410057] sono state individuate modalità più snelle per l'adempimento dell'obbligo dell'informativa da parte di imprese di assicurazione, con specifico riferimento alla pluralità di soggetti (persone fisiche e giuridiche, operanti in Italia e all'estero) che possono venire a conoscenza delle informazioni relative a una specifica posizione assicurativa (*cd.* "catena assicurativa"). In sostanza, il Garante (tenendo in considerazione la previsione contenuta nell'art. 13 della direttiva 95/46/Ce oltre alle indicazioni formulate dalla Raccomandazione del Consiglio d'Europa Rec (2002)9, del 18 settembre 2002), ha autorizzato le imprese di assicurazione stipulanti a rendere l'informativa alla clientela *una tantum*, in sede di conclusione del contratto di assicurazione, anche nell'interesse dei diversi soggetti che, in qualità di autonomi titolari del trattamento, utilizzano dati personali relativi al medesimo rischio assicurato.

Come chiarito in passato (*cfr. Provv.* 28 maggio 1997 [doc. *web* n. 40425]), l'informativa deve riferirsi a tutte le operazioni necessarie a dare corretta esecuzione al rapporto contrattuale, nonché agli altri trattamenti che (talora anche in base a esplicite previsioni di legge) possono essere effettuati lecitamente; deve poi illustrare i flussi comunicativi e indicare con precisione le finalità in concreto perseguite dall'impresa di assicurazione, nonché i soggetti o le tipologie di soggetti ai quali i dati possono essere comunicati (in qualità di autonomi titolari del trattamento) o che possono venirne a conoscenza quali "responsabili del trattamento".

Con il *provvedimento* sono state fornite, altresì, precisazioni in ordine alla formulazione che la modulistica in uso presso il settore assicurativo deve contenere nelle ipotesi in cui sia necessario il consenso dell'interessato. Salvo, infatti, il caso in cui il consenso non è richiesto (ovvero quando i dati sono necessari per instaurare o per dare esecuzione a un contratto di assicurazione, oppure sono trattati sulla base di uno dei presupposti di cui all'art. 24 del Codice), nei casi in cui il consenso dell'interessato è invece necessario (ad esempio, per il trattamento dei dati sensibili per i quali occorre comunque un consenso manifestato in forma scritta), l'impresa assicuratrice stipulante può circoscrivere la formula di consenso ai soli trattamenti da essa effettuati, oppure formularla in modo da ricomprendere, nei limiti del medesimo rischio assicurato, anche gli specifici trattamenti ulteriori effettuati da altri titolari appartenenti alla *cd.* "catena assicurativa".

Da ultimo, in considerazione del particolare ruolo svolto dai riassicuratori -che non instaurano un rapporto contrattuale con i soggetti coinvolti nel contratto di assicurazione- il Garante ha stabilito che l'eventuale comunicazione di dati (ad eccezione dei dati di natura sensibile) da parte della compagnia assicuratrice al riassicuratore rientra nell'ambito di applicazione dell'istituto del bilanciamento degli interessi tenuto conto del legittimo interesse dei titolari del trattamento coinvolti, e non richiede pertanto il consenso dell'interessato (art. 24, comma 1, lett. *g*), del Codice).

1.1.8. *Guida pratica e misure di semplificazione per le piccole e medie imprese*

Per facilitare le piccole e medie imprese nell'assolvimento degli obblighi che la normativa sulla *privacy* impone a chi raccoglie, utilizza e conserva dati personali è

stata anzitutto messa a punto una "Guida pratica e misure di semplificazione per le piccole e medie imprese" (in *G.U.* 21 giugno 2007, n. 142 [doc. *web* n. 1412271]), integrata da un questionario volto ad agevolare gli imprenditori nella più rapida verifica degli adempimenti previsti dal Codice. La guida chiarisce, in relazione alle circostanze concrete, chi può essere individuato quale titolare o responsabile del trattamento; in quali casi il trattamento deve essere notificato; quando occorre fornire l'informativa e quando è necessario acquisire il consenso dell'interessato; le misure da adottare per la sicurezza dei dati, i requisiti per il trasferimento dei dati in Paesi extracomunitari e i doveri del titolare del trattamento in caso di esercizio dei diritti da parte degli interessati ai sensi dell'art. 7 del Codice. La guida intende quindi rispondere all'esigenza, evidenziata dalle associazioni di categoria, di facilitare l'adempimento degli obblighi contenuti nella disciplina di protezione dei dati personali talvolta ritenuti onerosi per l'ordinaria attività di impresa. L'illustrazione di tali adempimenti mira peraltro a evidenziare come una corretta protezione dei dati personali possa rendere più efficiente l'attività d'impresa e incrementare la fiducia di consumatori e utenti.

1.1.9. *Bollette telefoniche: anche le ultime tre cifre possono essere "in chiaro"*

Con *provvedimento* del 13 marzo 2008 (in *G.U.* n. 79 del 3 aprile 2008, [doc. *web* n. 1501106]), le compagnie telefoniche sono state autorizzate ad emettere fatture dettagliate senza il mascheramento delle ultime tre cifre dei numeri chiamati. Gli abbonati che intendono continuare a ricevere bollette con la fatturazione dettagliata, ma con le ultime tre cifre oscurate, dovranno richiederlo espressamente al proprio gestore.

L'*autorizzazione generale* del Garante è stata rilasciata al termine di un'istruttoria preliminare avviata nel 2007, volta a verificare le modalità con le quali i gestori consentono agli utenti di effettuare chiamate addebitandone il costo non in fattura, ma attraverso carte di pagamento, anche prepagate.

La decisione tiene conto delle esigenze, manifestate più volte in questi anni da diversi abbonati, di poter verificare più agevolmente l'esattezza degli addebiti e le chiamate effettuate. L'abbonato, infatti, poteva conoscere i numeri totalmente in chiaro solo per contestare addebiti determinati o riferiti a periodi limitati.

A partire dal 1° luglio 2008, i gestori di telefonia fissa e mobile possono indicare nella fatturazione dettagliata i numeri completi delle comunicazioni. I gestori telefonici potranno esercitare tale facoltà a condizione che, come richiesto dal Garante, tutti gli abbonati vengano preventivamente portati a conoscenza di questa possibilità, mediante un'apposita informativa da inserire all'interno di almeno due fatture e nel sito *web* del fornitore.

L'informativa dovrà citare la decisione del fornitore di avvalersi dell'autorizzazione del Garante e specificare che tutti gli abbonati, che abbiano fatto o faranno richiesta di fatturazione dettagliata, la riceveranno "in chiaro", salvo che intendano mantenere il mascheramento delle ultime tre cifre.

Il Garante ha prescritto inoltre che nell'informativa i gestori invitino tutti gli abbonati che vorranno ricevere la fatturazione dettagliata in chiaro a informare quanti utilizzano la stessa utenza che la fatturazione perverrà completa di tutti i numeri chiamati.

1.1.10. *Pubblicazione e diffusione di atti e documenti di enti locali*

Con il *provvedimento* del 19 aprile 2007 ("Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali", in *G.U.* n. 120 del 25 maggio 2007 [doc. *web* n. 1407101]), il Garante ha definito princìpi e limiti che gli enti locali sono tenuti a rispettare riguardo al trat-

tamento di dati personali effettuato nelle attività connesse alla pubblicazione e diffusione di atti e documenti. Particolare attenzione è stata prestata alla diffusione di dati personali contenuti in atti e deliberazioni dai quali possono emergere delicate informazioni su condizioni di salute, *handicap* o situazioni di disagio (*ad es.*, di cittadini che concorrono per l'assegnazione di alloggi popolari, assistenza e contributi o per l'ammissione di minori agli asili nido).

Prima di pubblicare gli atti, renderli accessibili a terzi o metterli in rete, l'ente locale deve valutare se le finalità di trasparenza possono essere perseguite senza divulgare dati personali o attraverso modalità che permettano di identificare gli interessati solo se necessario. Negli atti, devono poi comparire solo dati pertinenti e non eccedenti rispetto alle finalità che l'ente intende raggiungere. I dati sensibili e giudiziari possono essere diffusi solo se realmente indispensabili e se l'ente abbia adottato il regolamento previsto dal Codice sull'uso di questi dati. É sempre vietato, comunque, diffondere informazioni sulla salute.

L'impiego delle nuove tecnologie impone all'ente locale sia di assicurare sempre l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete, sia di garantire il diritto all'oblìo delle persone interessate: ad esempio, trascorso un certo periodo dalla pubblicazione, risulta spesso necessario collocare determinati documenti in una parte del sito dove non sono più rintracciabili direttamente dai motori di ricerca esterni.

Specifiche cautele vanno adottate anche nel pubblicare gli elenchi delle persone che usufruiscono di crediti, sussidi o sovvenzioni: ad esempio, possono essere a volte pubblicati i nominativi dei beneficiari e la data di nascita, ma senza diffondere indirizzi, codici fiscali, coordinate bancarie o particolari della vita privata che possano creare imbarazzo agli interessati.

Le deliberazioni che approvano graduatorie dei vincitori dei pubblici concorsi possono essere pubblicate integralmente anche *on-line*, ma per visionare elaborati, verbali o titoli occorre prevedere accessi selezionati dei partecipanti, ad esempio attraverso una chiave personale (*username* e *password*, numero di protocollo o altri estremi identificativi).

1.1.11. *Maggiori garanzie a tutela degli invalidi civili*

Il Garante ha ricevuto alcune segnalazioni da parte di invalidi civili che lamentavano una violazione delle disposizioni in materia di protezione dei dati personali determinata dall'indicazione dei dati relativi alla diagnosi nelle istanze volte all'accertamento sanitario dell'invalidità civile e in alcuni tipi di certificazioni che attestano il riconoscimento della invalidità civile per finalità amministrative. Con *provvedimento* del 21 marzo 2007 (*G.U.* n. 82 del 7 aprile 2007 [doc. *web* n. 1395821]), l'Autorità ha pertanto indicato alcune misure per garantire un elevato livello di tutela della riservatezza anche in questo settore. Considerata la particolare natura delle informazioni richieste agli interessati, il Garante ha richiamato l'attenzione sull'obbligo degli uffici competenti alla ricezione delle istanze di adottare accorgimenti necessari a garantire un livello elevato di tutela dei diritti degli interessati, quali distanze di cortesia, spazi per colloqui riservati, consegna della documentazione in busta chiusa e obbligo di impartire precise istruzioni al personale sanitario (*v.* anche *Provv.* del 9 novembre 2005, sul rispetto della dignità delle persone nelle strutture sanitarie [doc. *web* n. 1191411]).

Le aziende sanitarie locali, inoltre, non devono indicare la diagnosi sui certificati che attestano il riconoscimento dell'invalidità civile per l'iscrizione alle liste del collocamento obbligatorie o per la richiesta di esenzione dalle tasse scolastiche o universitarie, specie nei casi in cui si riscontri lo stato di sieropositività o l'infezione da Hiv.

Riportare le patologie nei verbali delle commissioni mediche che accertano tipo e grado di invalidità è prescritto dalla normativa anche in vista di eventuali revisioni o ricorsi. Non è invece giustificato indicare gli stessi dati nelle certificazioni per l'iscrizione al collocamento o per ottenere un'esenzione dalle tasse scolastiche, sia perché non indispensabili, sia in ragione del quadro normativo di riferimento. Vi sono infatti alcune norme che prevedono tutele rafforzate per specifiche patologie (*ad es.*, la l. n. 135/1990, che limita la comunicazione dei risultati di accertamenti per l'infezione da Hiv alla sola persona che si è sottoposta agli esami). Inoltre, per avere diritto ad alcuni benefici o all'iscrizione a categorie protette, la normativa di settore prescrive spesso specifici requisiti quali l'appartenenza a una famiglia in disagiate condizioni economiche, o l'aver subito una riduzione della capacità lavorativa *ecc.*, tra i quali non risulta la patologia sofferta. Anche ai fini del collocamento, infine, è prevista solo una valutazione delle funzionalità della persona disabile, per individuarne le capacità lavorative.

Sulla base di tali presupposti normativi il Garante ha pertanto ritenuto necessario prescrivere alle aziende sanitarie locali, al fine di rendere il trattamento conforme alle norme in materia di protezione dei dati, di rilasciare le certificazioni che attestano il riconoscimento dell'invalidità civile per finalità connesse all'iscrizione alle liste del collocamento obbligatorio o alla richiesta di esenzione dalle tasse scolastiche e universitarie, senza indicare i dati personali relativi alla diagnosi.

1.1.12. *Accesso dei medici a zone a traffico limitato*

A seguito di alcune segnalazioni, il Garante si è pronunciato in merito alla legittimità della richiesta, rivolta da alcune amministrazioni comunali ai medici privi di un permesso per l'accesso ad una Ztl, di comunicare dati personali relativi alle persone visitate a domicilio in tali aree. In particolare, con il *provvedimento* del 14 giugno 2007 (in *G.U.* n. 161 del 13 luglio 2007 [doc. *web* n. 1424100], l'Autorità, ritenendo che il dovere degli organi comunali di applicare sanzioni in caso di accertata violazione delle norme di accesso e circolazione dei veicoli non debba tradursi in una indebita violazione della riservatezza dei pazienti, ha ritenuto sproporzionate e non indispensabili le richieste rivolte ai medici. L'accertamento delle violazioni per l'accesso alla Ztl, può essere perseguito infatti attraverso altre modalità, parimenti efficaci, ma rispettose del diritto alla protezione dei dati personali, quali, ad esempio, la comunicazione dell'indirizzo e del numero civico presso il quale è stato prestato intervento, la targa del veicolo del medico che ha effettuato la visita o il numero di iscrizione all'ordine professionale. Il Garante ha pertanto prescritto ai comuni di astenersi dal richiedere ai medici le generalità e altre informazioni che identificano le persone visitate a domicilio all'interno di aree Ztl. L'Autorità ha inoltre prescritto ai medici, in caso di ricorso avverso la contestazione amministrativa, di non presentare documenti contenenti le generalità e altre informazioni che identificano i pazienti visitati a domicilio, documenti che gli uffici territoriali di governo devono, pertanto, astenersi dal richiedere.

1.1.13. *Servizi telefonici. Adempimenti semplificati per i* customer care

Con il *provvedimento* del 15 novembre 2007 (in G. U. n. 285 del 7 dicembre 2007 [doc. *web* n. 1462788]), sono state prescritte misure per semplificare l'informativa fornita dalle società che (anche attraverso canali completamente automatizzati) si occupano di *customer care*, assistenza *post* vendita, prenotazioni di servizi, *phone banking* in modalità *"inbound"*, ossia a seguito di una chiamata dell'utente. È stato in primo luogo stabilito che non è necessario fornire l'informativa quando siano trattati i soli dati necessari ad assicurare il servizio richiesto, o il cliente sia già

stato informato precedentemente, *ad es.*, al momento della sottoscrizione di un contratto, o alcuni elementi dell'informativa emergano nel corso del colloquio telefonico. Per utilizzare i dati anche ad altri fini (*ad es.*, di *marketing* o profilazione) è necessario informare l'utente e ottenere un suo consenso specifico.

L'Autorità ha ricordato che, ove necessaria, l'informativa deve essere fornita con formule sintetiche, chiare e di immediata comprensione, ed ha autorizzato coloro che prestano i servizi in esame a indicare la modalità attraverso la quale l'interessato può consultare o ascoltare a richiesta un'informativa più specifica, ad esempio mediante un sito *web* o tramite operatore o messaggio registrato ascoltabile digitando una cifra sulla tastiera del telefono.

Nel *provvedimento*, adottato anche tenendo conto delle richieste di chiarimento provenienti da una associazione di categoria, l'Autorità ha inoltre invitato le società del settore ad assicurare elevati livelli di professionalità nel trattamento dei dati ponendo specifica attenzione anche al profilo della loro sicurezza.

In particolare, è stata sottolineata l'importanza di adottare adeguate cautele quando un medesimo *call center* si trovi a gestire contemporaneamente vari *database*, con tipologie diverse di informazioni, per una pluralità di committenti. Per tale motivo, prima della stipula del contratto che affida in *outsourcing* il servizio, deve essere effettuata un'attenta analisi delle implicazioni che il trattamento dei dati può comportare.

1.1.14. *Utilizzazione dei dati della clientela del mercato di energia e gas*

Con *deliberazione* del 25 luglio 2007 (in *G.U.* del 20 agosto 2007 [doc. *web* n. 1428567]), adottata al termine di una procedura di cooperazione con l'Autorità per l'energia elettrica e il gas, il Garante ha fornito una serie di indicazioni, nell'ambito della fornitura di energia elettrica e gas, per la informazione dei clienti e il corretto utilizzo dei dati che li riguardano.

La recente disciplina sulla liberalizzazione dell'energia prevede che, a partire dal 1° luglio 2007, i clienti domestici possano recedere dal contratto di fornitura di energia stipulato prima di tale data con il distributore operante nel proprio ambito territoriale e scegliere un fornitore diverso. Le società che vendono energia devono poter acquisire dalle banche dati dei distributori alcune informazioni di base relative agli utenti del mercato energetico, in modo da formulare proposte commerciali.

In base a tale *deliberazione* le società distributrici sono tenute a informare i clienti in maniera colloquiale e sintetica riguardo alla facoltà di recedere dal contratto e alla possibilità che alle aziende venditrici di energia siano forniti alcuni dati (generalità, consumi, potenza impegnata *ecc.*) al fine di far conoscere le loro migliori offerte sulla base di un profilo "minimo" del cliente medesimo. A tale proposito il Garante ha predisposto in allegato alla *deliberazione* un modello di informativa.

L'informativa deve essere recapitata insieme alla corrispondenza ordinaria riguardante la gestione del vigente contratto di fornitura o di distribuzione (*ad es.*, l'invio della bolletta), nonché resa disponibile anche sul sito Internet e attraverso i servizi di assistenza e informazione al pubblico.

Le proposte commerciali dei venditori devono essere rigorosamente cartacee: non è quindi consentito il *marketing* telefonico o per via telematica. I dati dei clienti non possono essere comunicati a terzi.

I dati personali dei clienti che non rispondono alle offerte commerciali devono essere cancellati non più tardi di sei mesi dall'invio della proposta.

1.1.15. *Schema preliminare del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria*

I lavori di redazione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria (art. 135 del Codice) si sono susseguiti con notevole intensità nel corso del 2007, specie nell'ambito di riunioni promosse dall'Autorità con i soggetti interessati.

Gli incontri, caratterizzati da elevato spirito di collaborazione, hanno reso possibile la definizione, negli ultimi mesi dell'anno, di uno schema preliminare di codice, sottoposto dalle medesime categorie interessate all'esame del Garante per le valutazioni di cui all'art. 6 del regolamento del Garante n. 2/2006.

Lo schema (che, sulla base di una prima verifica, il 20 marzo 2008 è stato ritenuto dall'Autorità conforme alla normativa vigente), è rimasto accessibile anche tramite il sito *web* del Garante [doc. *web* n. 1503511], al fine di consentire entro il 30 aprile 2008 (avviso in *G.U.* n. 83 dell'8 aprile 2008) la raccolta di eventuali osservazioni da parte dei "soggetti interessati" prima della sua formale sottoscrizione (art. 12 del Codice; artt. 5 e 6 del regolamento del Garante n. 2/2006).

Le principali novità introdotte nello schema del codice riguardano l'ambito di applicazione, i tempi di conservazione delle informazioni, i rapporti con i terzi e con la stampa e le modalità di trattamento dei dati personali per le finalità di difesa di un diritto in sede giudiziaria. Riguardo a quest'ultimo aspetto lo schema di codice sollecita i soggetti coinvolti a prestare specifica attenzione all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati con riferimento allo scambio di corrispondenza, specie per via telematica, all'esercizio contiguo di attività autonome all'interno di uno studio, all'utilizzo di particolari dispositivi o supporti, specialmente se elettronici, come le registrazioni audio/video o i tabulati di flussi telefonici o informatici, e all'acquisizione informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possano comportare, comunque, rischi specifici per gli interessati.

1.2. *Rapporti con il Parlamento e altre istituzioni*

1.2.1. *Le audizioni del Garante in Parlamento*

Anche nel 2007 il Garante ha partecipato ad alcune audizioni presso commissioni della Camera e del Senato o altri organismi anche bicamerali su temi d'interesse all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di proposte di legge aventi riflessi in materia di protezione dei dati personali.

In questo quadro si collocano, in particolare:

- il 28 novembre 2007, presso la Commissione politiche dell'Unione europea della Camera, un'audizione nell'ambito dei lavori per l'approvazione di due disegni di legge di ratifica di accordi internazionali concernenti il funzionamento del sistema satellitare Galileo, nel corso della quale sono state esaminate le implicazioni che il sistema presenta in relazione alla tutela dei dati personali, con specifico riferimento al contesto comunitario (*v.* anche *par.* 2.2.);
- il 17 luglio 2007, presso la Commissione di vigilanza sull'anagrafe tributaria, un'audizione nell'ambito dell'indagine conoscitiva sulle modalità di gestione e utilizzo dei dati dell'anagrafe tributaria;
- il 16 maggio 2007, presso il Comitato parlamentare di controllo sull'attua-

zione dell'Accordo di Schengen, un'audizione nell'ambito dell'indagine conoscitiva in materia di immigrazione che ha riguardato le problematiche connesse all'applicazione del Trattato di Prüm, con specifico riferimento alla raccolta e conservazione di dati relativi al Dna delle persone ed alle implicazioni sulla protezione dei dati personali;

- il 2 maggio 2007, presso la Commissione affari costituzionali del Senato, un'audizione nell'ambito dell'indagine conoscitiva sui rapporti fra libertà di informazione, sviluppo delle comunicazioni, tutela dei diritti della persona e sicurezza pubblica (una prima audizione del Garante si era tenuta nel novembre-dicembre 2006);
- il 13 marzo 2007, presso le Commissioni cultura e comunicazioni della Camera riunite, un'audizione nell'ambito della discussione del disegno di legge presentato dal Governo per la disciplina del settore televisivo nella fase di transizione al digitale;
- il 6 marzo 2007, innanzi all'ufficio di presidenza della Commissione finanze e tesoro del Senato, un'audizione (informale) nell'ambito della discussione di un disegno di legge relativo all'istituzione di un sistema di prevenzione delle frodi nel settore del credito al consumo;
- il 23 gennaio 2007, presso la Commissione igiene e sanità del Senato, un'audizione (informale) che ha avuto ad oggetto i disegni di legge in materia di "testamento biologico". L'intervento del Garante ha riguardato, in particolare, l'esame delle problematiche che emergono con riguardo alla protezione dei dati personali, come, ad esempio, le modalità di raccolta e di conservazione delle *cd.* "dichiarazioni anticipate di volontà", i soggetti legittimati a trattare i dati e il consenso informato dei pazienti;
- il 16 gennaio 2007, presso il Comitato parlamentare di controllo sull'attuazione dell'Accordo di Schengen, un'audizione che ha avuto per oggetto, in particolare, l'esame delle questioni attinenti alla evoluzione del sistema informativo Schengen (*cd.* "Sis-II") e allo scambio crescente di informazioni e di dati tra le forze di polizia. L'audizione ha riguardato anche il Trattato di Prüm, nonché lo sviluppo della cooperazione dell'Unione europea con gli Stati Uniti, in merito alle problematiche del *cd.* "Pnr" (*Passenger name record*) e del caso Swift e i connessi riflessi sui diritti fondamentali dei cittadini.

1.2.2. *L'Autorità e le attività di sindacato ispettivo del Parlamento*

Anche nel 2007 l'Autorità ha fornito propri contributi conoscitivi in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo del Parlamento riguardanti profili attinenti alla protezione dei dati personali.

Sono stati forniti al Governo elementi di valutazione in relazione ad atti di sindacato ispettivo fra i quali si ricordano, in particolare:

- un'interrogazione a risposta immediata presentata in Commissione giustizia della Camera dall'on. Balducci, relativa al caso "Peppermint" (*Nota* 13 giugno 2007). L'Autorità ha precisato che il Garante si è costituito in giudizio presso il Tribunale di Roma nelle controversie instaurate dalle società Peppermint Jam Records GmbH, tedesca, e *T*echland sp. z.o.o., polacca, nei riguardi di alcuni fornitori di servizi di comunicazione elettronica, al fine di verificare se nella vicenda siano state rispettate le garanzie previste per i cittadini dalla normativa in materia di protezione dei dati personali. L'Autorità ha precisato di aver avviato un distinto procedimento amministrativo di controllo per verificare autonomamente la liceità e la correttezza dei trattamenti di dati personali effettuati dalle predette società, e di aver rivolto una richie-

sta di collaborazione alle Autorità per la protezione dei dati personali nei Paesi interessati, in particolare per quanto riguarda altre eventuali informazioni utili o per agevolare, se necessario, un'idonea risposta alle richieste istruttorie rivolte alle società (sugli sviluppi del caso in questione *v. par.* 20.5);

- un'interrogazione a risposta scritta presentata dall'on. Urso, relativa all'invio massiccio e indiscriminato di *e-mail* pubblicitarie non richieste (*spamming*) che interessa singoli utenti della rete Internet e piccole e medie imprese costrette a sopportarne i costi (*Nota* 23 febbraio 2007). Al riguardo, l'Autorità ha ricordato che dopo una serie di interventi mirati che hanno portato a sospendere l'attività illecita di alcune aziende e persone fisiche e a denunciarne talune all'autorità giudiziaria, nel 2003 il Garante ha adottato un *provvedimento* generale (*Provv.* 29 maggio 2003 [doc. *web* n. 29840]) con il quale, sulla base della normativa all'epoca vigente (l. n. 675/1996 e d.lg. n. 171/1998) ha precisato vari aspetti legati all'invio di *e-mail* promozionali o pubblicitarie, anche alla luce della direttiva europea 2002/58/Ce poi recepita con il Codice in materia di protezione dei dati personali. I princìpi organicamente riassunti dal Garante nel *provvedimento* sono stati "confermati" e implementati dal Codice mediante specifiche garanzie a tutela dell'interessato previste, in particolare, nell'articolo 130. L'Autorità ha infine informato che continuano a pervenire al Garante numerosi reclami e segnalazioni con i quali sono lamentate ripetute violazioni del diritto al corretto e lecito utilizzo dei dati personali nell'invio dei messaggi promozionali e che particolare preoccupazione desta, poi, l'incremento delle segnalazioni che lamentano l'invio di *e-mail* riconducibili al fenomeno denominato *"phishing"*, volto ad acquisire fraudolentemente informazioni personali del destinatario dell'*e-mail*. Il Garante, anche in relazione a tale specifico fenomeno, ha, perciò, intensificato le attività di controllo e verifica dell'attività svolte da diversi operatori che, direttamente o per mezzo di soggetti specializzati, svolgono campagne pubblicitarie e di *direct marketing* utilizzando lo strumento della posta elettronica.

1.2.3. *L'attività consultiva del Garante sugli atti del Governo*

Nel quadro dell'attività consultiva prevista dal Codice in relazione a norme regolamentari e ad atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice), il Garante ha espresso anche nel 2007 diversi pareri i quali hanno riguardato, in particolare:

- uno schema di provvedimento dell'Agenzia delle entrate in materia di comunicazione in via telematica alla predetta agenzia dei dati acquisiti nell'attività di gestione del servizio di smaltimento dei rifiuti (art. 1, commi 106, 107 e 108 della l. 27 dicembre 2006, n. 296) (*Parere* 6 dicembre 2007 [doc. *web* n. 1470750]);
- uno schema di decreto interministeriale predisposto dal Ministero delle comunicazioni recante recepimento del codice di autoregolamentazione delle trasmissioni di commento degli avvenimenti sportivi denominato "Codice *media* e sport" (*Parere* 11 ottobre 2007 [doc. *web* n. 1449705]);
- uno schema di decreto predisposto dal Ministero dell'interno recante regole tecniche in materia di carta d'identità e documento d'identità elettronici (*Parere* 1° agosto 2007 [doc. *web* n. 1436216]);
- uno schema di decreto predisposto dalla Presidenza del Consiglio dei ministri-Dipartimento delle politiche per la famiglia, sul coordinamento delle attività delle pubbliche amministrazioni per la tutela dei minori dallo sfrutta-

mento e dall'abuso sessuale (*Parere* 25 luglio 2007 [doc. *web* n. 1436237]);
- uno schema di decreto predisposto dal Ministero dell'economia e delle finanze in materia di pagamenti da parte delle pubbliche amministrazioni (*Parere* 25 luglio 2007 [doc. *web* n. 1434395]);
- uno schema di decreto predisposto dal Ministero della giustizia in materia di rilascio di certificati del casellario giudiziale (*Parere* 25 luglio 2007 [doc. *web* n. 1431017]);
- uno schema di provvedimento dell'Agenzia delle entrate in materia di individuazione degli elementi informativi e di definizione delle modalità tecniche e dei termini relativi alla trasmissione di determinati elenchi (art. 37, commi 8 e 9, d.l. 4 luglio 2006, n. 223, convertito dalla l. 4 agosto 2006, n. 248) (*Parere* 26 aprile 2007 [doc. *web* n. 1402616]);
- uno schema di provvedimento dell'Agenzia delle entrate in materia di modalità e termini per la comunicazione dei corrispettivi giornalieri (art. 37, comma 34, d.l. n. 223/2006) (*Parere* 12 aprile [2007 doc. *web* n. 1402655]);
- uno schema di regolamento recante norme in materia di composizione e compiti della Commissione per le adozioni internazionali (*Parere* 12 aprile 2007 [doc. *web* n. 1401738]);
- uno schema di decreto del Ministero dell'università e della ricerca riguardante le prove di ammissione a corsi di laurea per l'anno accademico 2007-2008 *(Parere* 4 aprile 2007 [doc. *web* n. 1401716]);
- uno schema di decreto predisposto dal Ministero dell'economia e delle finanze in materia di archivi informatici delle tasse automobilistiche (*Parere* 16 marzo 2007 [doc. *web* n. 1397123]);
- uno schema di decreto recante regole procedurali di carattere tecnico operativo per l'attuazione del d.P.R. 14 novembre 2002, n. 313 recante il testo unico in materia di casellario giudiziale (*Parere* 18 gennaio 2007 [doc. *web* n. 1381963]);
- uno schema di decreto riguardante l'istituzione dei registri e delle cartelle sanitarie e di rischio dei lavoratori esposti ad agenti cancerogeni o biologici (*Parere* 11 gennaio 2007 [doc. *web* n. 1388712]);
- due schemi di provvedimenti dell'Agenzia delle entrate in materia di modalità e termini per la comunicazione all'anagrafe tributaria dei dati relativi alle somme di denaro erogate da imprese, intermediari e altri operatori del settore delle assicurazioni, nonché di altre informazioni da parte di operatori finanziari (artt. 35, comma 27, e 37, commi 4 e 5, d.l. n. 223/2006) (*Pareri* 11 gennaio 2007 [doc. *web* nn. 1381575 e 1381941]);
- uno schema di provvedimento recante modalità di trasmissione dei dati relativi ai crediti d'imposta per la ricerca scientifica e tecnologica, di cui all'art. 5 della l. 27 dicembre 1997, n. 449 (*Parere* 25 gennaio 2007 [doc. *web* n. 1381925]).

A fronte dei diversi pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità, fra i quali in particolare:
- decreto del Ministro della salute 21 dicembre 2007 (*G.U.* 16 gennaio 2008, n. 13) recante "Istituzione del sistema informativo dei servizi trasfusionali";
- decreto del Direttore dell'Agenzia del territorio 13 novembre 2007 (*G.U.* 24 novembre 2007, n. 274, S.O. n. 243) recante "Definizione delle regole tecnico-economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni, ai sensi dell'articolo 59, comma 7-*bis*, del d.lg. 7 marzo 2005, n. 82";
- decreti del Direttore dell'Agenzia del territorio 6 novembre 2007 (*G.U.* 13

novembre 2007, n. 264) e 4 maggio 2007 (*G.U.* 10 maggio 2007, n. 107) in materia di accesso al sistema telematico dell'Agenzia del territorio per la consultazione delle banche dati ipotecaria e catastale;

- decreto del vice Ministro dell'economia e delle finanze 3 ottobre 2007 (*G.U.* 8 novembre 2007, n. 260) recante "Individuazione dei soggetti esonerati dall'obbligo della tracciabilità dei pagamenti";
- tre decreti del Ministro del lavoro adottati di concerto con il Ministro per le riforme e le innovazioni nella pubblica amministrazione 30 ottobre 2007 (*G.U.* 27 dicembre 2007, n. 299), in materia di comunicazioni telematiche dovute dai datori di lavoro ai servizi competenti, scheda anagrafico-professionale e *standard* tecnici della borsa continua nazionale del lavoro;
- decreto del Presidente della Repubblica 22 giugno 2007, n. 116 (*G.U.* 2 agosto 2007, n. 178) recante "Regolamento di attuazione dell'articolo 1, comma 345, della l. 23 dicembre 2005, n. 266, in materia di depositi dormienti";
- decreto del presidente del Consiglio dei ministri 14 giugno 2007 (*G.U.* 5 luglio 2007, n. 154) e relativo comunicato di rettifica (*G.U.* 9 agosto 2007, n. 184) in materia di "Decentramento delle funzioni catastali ai comuni, ai sensi dell'articolo 1, comma 197, della l. 27 dicembre 2006, n. 296.";
- decreto del Ministro dell'economia e delle finanze 8 giugno 2007 (*G.U.* 18 giugno 2007, n. 139) recante "Criteri e modalità per la concessione di contributi per l'acquisto di *pc* da parte di collaboratori coordinati e continuativi e di collaboratori a progetto, in attuazione dell'articolo 1, comma 298, della legge 27 dicembre 2006, n. 296 (legge finanziaria 2007)";
- decreto 23 maggio 2007 e provvedimento 25 maggio 2007 del Direttore dell'Agenzia del territorio (*G.U.* 29 maggio 2007, n. 123) che, rispettivamente, istituiscono, presso il servizio di pubblicità immobiliare dell'Agenzia, il registro delle comunicazioni in materia di cancellazione di ipoteche e definiscono le relative modalità di trasmissione da parte del creditore, ai sensi dell'articolo 13, comma 8-*septies*, del d.l. 31 gennaio 2007, n. 7, convertito dalla l. 2 aprile 2007, n. 40.

1.2.4. *Altri pareri*

Su espressa richiesta, il Garante ha espresso parere anche su alcuni altri atti normativi del Governo e, in particolare, sui seguenti provvedimenti:

- uno schema di decreto legislativo volto a dare attuazione alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza nei luoghi di lavoro (*Parere* 31 marzo 2008);
- uno schema di decreto legislativo per l'attuazione della direttiva 2006/24/Ce riguardante la conservazione di dati di traffico trattati nell'ambito della fornitura di servizi di comunicazione elettronica (*Parere* 5 marzo 2008);
- uno schema di decreto legislativo recante norma di attuazione in materia di dichiarazione di appartenenza o aggregazione al gruppo linguistico in provincia di Bolzano (*Parere* 10 gennaio 2008 [doc. *web* n. 1484669]);
- un disegno di legge per l'istituzione di una banca dati contenente profili del Dna delle persone a fini di giustizia, presentato dal Governo anche in attuazione del Trattato di Prüm (*Parere* 15 ottobre 2007 [doc. *web* n. 1448799]);
- uno schema di decreto legislativo per il recepimento della direttiva 2004/82/Ce concernente l'obbligo dei vettori aerei di comunicare i dati relativi alle persone trasportate (*Parere* 13 febbraio 2007 [doc. *web* n. 1388444]).

2 Quadro normativo in materia di protezione dei dati personali

2.1. *Il percorso di "stabilizzazione" delle garanzie previste nel Codice.*

Le *Relazioni* del Garante degli scorsi anni hanno evidenziato il percorso normativo attraverso il quale sono state introdotte nel nostro ordinamento importanti garanzie per i diritti fondamentali della persona rispetto al trattamento dei dati personali che hanno trovato, poi, nel Codice in materia di protezione di dati personali (decreto legislativo 30 giugno 2003, n. 196), il loro pieno consolidamento, in particolare con il riconoscimento del diritto alla protezione dei dati personali.

Nelle *Relazioni* del 2004 e del 2005 si erano, tuttavia, evidenziati alcuni circoscritti interventi modificativi del Codice, in materia di conservazione dei dati di traffico telefonico e telematico e in ambito sanitario, sui quali l'Autorità aveva richiamato l'attenzione per evitare segnali in parziale controtendenza rispetto a quel percorso di "stabilizzazione" delle regole per la protezione dei dati.

Mentre nel 2006 il Codice non aveva subito modifiche significative (salva la reiterazione di proroghe già disposte negli anni precedenti per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili e giudiziari delle pubbliche amministrazioni), sul finire della XV legislatura si è registrato un nuovo intervento integrativo del Codice con riferimento ai dati di traffico telematico, ad opera della legge 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

La predetta Convenzione, come si dirà più diffusamente in altra parte della *Relazione* (*par.* 2.2.), prevede che ciascuno Stato membro introduca misure sostanziali e procedurali in ambito penale per il contrasto dei crimini informatici e per la raccolta di prove elettroniche utili nelle indagini concernenti qualunque reato, anche non informatico.

In tale quadro, la Convenzione reca alcune disposizioni che consentono, anche per finalità di collaborazione internazionale, la conservazione temporanea (per un periodo di tempo non superiore a novanta giorni, ma prorogabile) di specifici dati informatici, inclusi i dati sul traffico, già in possesso dei fornitori di servizi di comunicazione elettronica o comunque sotto il loro controllo (*cd.* "congelamento"), quando la disponibilità dei medesimi dati da parte delle competenti autorità sia necessaria e vi sia motivo di ritenere che i dati stessi, anche in ragione della loro particolare vulnerabilità, possano essere cancellati o modificati (artt. 16 e 17 Conv.).

In Europa, la conservazione dei dati di traffico per finalità di giustizia e, in particolare, per il perseguimento e la repressione di reati gravi, è oggetto della direttiva 2006/24/Ce, in fase di recepimento nei vari Paesi. Inoltre, l'istituto del "congelamento" dei dati trova, di regola, la sua naturale esplicazione in ordinamenti nei quali la conservazione sistematica dei dati di traffico non è consentita o è prevista per periodi di tempo assai ristretti.

La predetta legge n. 48/2008 (art. 10), integrando l'articolo 132 del Codice (nuovi commi 4-*ter*, 4-*quater* e 4-*quinquies*), ha previsto che specifici organi di polizia possano ordinare ai fornitori di servizi di comunicazione elettronica di conservare e proteggere, per un periodo non superiore a novanta giorni (prorogabile non