sono trattati dati di carattere sensibile o giudiziario, per rendere più snelle le procedure burocratiche e più semplici i moduli dell'informativa, favorendo una più agevole comprensione dei cittadini sulle modalità e finalità del trattamento dei dati personali.

Il Garante ha inoltre fornito indicazioni specifiche per la redazione di un'informativa unica per il complesso dei trattamenti di dati personali a fini esclusivamente amministrativi e contabili. Gli operatori potranno anche redigere una prima informativa breve rinviando ad un testo più articolato disponibile su siti Internet, reti Intranet, in bacheche o presso gli sportelli al pubblico del titolare del trattamento.

Le associazioni di categoria sono state invitate a predisporre informative-tipo per determinati settori o categorie di trattamenti, prevedendo la messa a disposizione, gratuitamente, di un *kit* di istruzioni concrete e *fac-simili* per facilitare l'opera di semplificazione degli adempimenti previsti.

Alle indicazioni relative all'informativa si aggiungono quelle relative al consenso, che deve essere acquisito solo nei casi veramente necessari.

Il Garante, considerati i princìpi di efficacia e proporzionalità e in relazione agli artt. 2, 18, comma 4, 24, comma 1, e 154, comma 1, lett. *c*), del Codice, ha chiarito che il consenso non deve essere richiesto in particolare, quando:

- il trattamento dei dati in ambito privato è svolto per adempiere a obblighi contrattuali o normativi o, comunque, per ordinarie finalità amministrative e contabili;
- i dati trattati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque o sono relativi allo svolgimento di attività economiche dell'interessato.

Misure di sicurezza

L'art. 29 del decreto-legge 25 giugno 2008, n. 112 (convertito in legge il 6 agosto 2008, n. 133) ha modificato gli artt. 34 e 38 del Codice.

In particolare, nell'art. 34 è stato aggiunto il comma 1-*bis*, in base al quale per tutte le imprese che trattano soltanto dati personali non sensibili e che trattano solo i dati sensibili relativi allo stato di salute dei dipendenti e collaboratori (certificati medici senza indicazione della relativa diagnosi) ovvero all'adesione ad organizzazioni sindacali, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'art. 47 del t.u. di cui al d.P.R. 28 dicembre 2000, n. 445.

Inoltre, il citato comma 1-*bis* ha demandato al Garante la semplificazione del Disciplinare tecnico in materia di misure minime di sicurezza.

In attuazione di tale previsione, gli adempimenti a carico dei titolari del trattamento sono stati rimodulati in funzione delle effettive caratteristiche dimensionali o di struttura delle imprese, della natura dei trattamenti, nonché in considerazione di esigenze di riduzione dei costi (*Provv.* 27 novembre 2008 [doc. *web* n. 1571218]. Le nuove garanzie, adottate sentito il Ministro per la semplificazione normativa, interessano:

a) amministrazioni pubbliche e società private che utilizzano dati personali non sensibili (nome, cognome, indirizzo, codice fiscale, numero di telefono) o che trattano come unici dati sensibili dei dipendenti quelli relativi allo stato di salute o all'adesione a organizzazioni sindacali;

b) piccole e medie imprese, liberi professionisti o artigiani che trattano dati solo per fini amministrativi e contabili.

In base al *provvedimento* del Garante, le categorie interessate:

- possono impartire anche oralmente le istruzioni agli incaricati in materia di misure minime;
- possono utilizzare per l'accesso ai sistemi informatici un qualsiasi sistema di autenticazione basato su un username e una *password*; lo username deve essere disattivato quando viene meno il diritto di accesso ai dati;
- in caso di assenze prolungate o di impedimenti del dipendente possono mettere in atto procedure che consentano comunque l'operatività e la sicurezza del sistema (*ad es.*, l'invio automatico delle *e-mail* ad un altro recapito accessibile);
- devono aggiornare i programmi di sicurezza (antivirus) almeno una volta l'anno ed effettuare *backup* dei dati almeno una volta al mese.

Con il *provvedimento*, inoltre, il Garante ha fornito a piccole e medie imprese, artigiani, liberi professioni, soggetti pubblici e privati che trattano dati solo a fini amministrativi e contabili, alcune indicazioni per la redazione di un documento programmatico per la sicurezza semplificato.

Procedure semplificate sono state indicate anche per chi tratta dati senza l'impiego di sistemi informatici.

Notificazione

Nel nuovo testo dell'art. 38 del Codice è stato sostituito il comma 2, precisando e circoscrivendo il contenuto del modello che deve essere utilizzato per effettuare la notificazione.

Insieme con quello sulle misure minime di sicurezza, il Garante ha adottato in data 22 ottobre 2008 [doc. *web* n. 1571196] un *provvedimento* che, in linea con le semplificazioni già adottate in precedenza snellisce ulteriormente il modello utilizzato per effettuare le notificazioni, e che non comporta l'obbligo di modificare le notificazioni già presentate.

11. Trasferimento di dati personali all'estero

La tematica delle *cd.* "*Binding corporate rules* (*Bcr*)" (Norme vincolanti d'impresa, *v. infra*, *par.* 20.1 e 20.7) ha formato oggetto di intenso lavoro anche nel corso del 2008, in particolare con riferimento alle numerose richieste, pervenute da parte di altre autorità di controllo, nell'ambito dell'attivazione di procedure di cooperazione concernenti alcuni progetti di *Bcr* elaborati da vari gruppi societari di carattere multinazionale.

L'Autorità italiana ha intensificato l'attività di verifica della richiesta, avanzata nel 2007 (*v. Relazione* 2007, *p.* 115) da un gruppo bancario italiano, volta a instaurare la procedura di coordinamento per l'approvazione di *Bcr* innanzi al Garante in qualità di *lead authority*, in ordine al trattamento di dati relativi al personale dipendente.

Constatata la sussistenza dei presupposti ad agire nell'ambito della procedura di cooperazione (in conformità al documento WP 107 del Gruppo art. 29) e ottenuta conferma, da parte delle altre Autorità interessate, a procedere in veste di *lead authority*, il Garante ha intrapreso una puntuale attività di analisi del testo preliminare di *Bcr* presentato dal gruppo societario, al fine di verificarne la conformità con i criteri di adeguatezza sanciti dai documenti del Gruppo art. 29 (*cfr.* WP 74 e 153). Tale riflessione ha determinato l'attiva partecipazione della società, cui sono state fornite diverse indicazioni volte a suggerire alcune modifiche al menzionato progetto di *Bcr*, soprattutto in vista dell'approvazione di alcuni nuovi documenti in ambito europeo (*cfr.* WP 153, 154 e 155) e della recente modifica legislativa al Codice (*cfr.* art. 44, lett. *a*), del Codice, come modificato dalla legge 6 agosto 2008, n. 133).

Nel 2008 si è, infatti, assistito all'intensificazione delle attività di approfondimento in materia di *Bcr* da parte del Gruppo art. 29, attraverso l'approvazione di tre documenti (*v.* anche, *par.* 20.1), volti a precisare alcuni aspetti di fondamentale importanza.

A tali nuovi sviluppi in sede europea si è accompagnato il recente intervento legislativo di modifica dell'art. 44 del Codice, già invocato dal Garante con apposita segnalazione al Parlamento e al Governo adottata nel corso del 2007 (*cfr. Relazione* 2007, *p.* 115).

Il nuovo testo, nell'includere le regole di condotta osservate all'interno di gruppi di società tra gli strumenti considerati adeguati ai fini del trasferimento dei dati personali al

di fuori dell'Ue e dello Spazio economico europeo, ha determinato l'entrata a pieno titolo del Garante nel novero delle Autorità in grado di rilasciare un'autorizzazione al trasferimento dei dati personali verso Paesi terzi, che non offrano adeguate garanzie di tutela, tramite lo strumento delle *Bcr*.

La norma non risolve tutte le questioni relative all'efficacia vincolante dello strumento delle *Bcr* nell'ordinamento italiano, pur collocandosi in un'ottica garantista volta ad imporre alle società l'obbligo di assicurare agli interessati l'esercizio dei propri diritti nell'ambito del territorio dello Stato italiano, in ordine all'inosservanza delle *Bcr* medesime (*cfr.* art. 44, lett. *a*), secondo capoverso del Codice).

12. Attività forense

Anche nel 2008 si è registrato un incremento dell'attività legata alle segnalazioni e ai reclami pervenuti in materia di attività forense, con riferimento al trattamento di dati personali, spesso sensibili, effettuato dagli avvocati e dalle agenzie investigative nell'ambito di procedimenti giudiziari civili e penali, specie in materia di separazione tra coniugi.

Di particolare rilievo appare la sottoscrizione, avvenuta il 27 ottobre 2008 da parte delle associazioni rappresentative dell'avvocatura e degli investigatori privati, del *"Codice di deontologia e di buona condotta per il trattamento di dati personali effettuato per svolgere le investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria"* (*G.U.* 24 novembre 2008, n. 275, in vigore dal 1° gennaio 2009 e allegato al Codice [doc. *web* n. 1565171]).

In materia di attività forense l'attenzione del Garante si è concentrata sulle modalità di acquisizione e utilizzazione delle prove dedotte in giudizio da parte degli avvocati.

È emersa infatti l'esigenza di richiamare gli operatori del settore ad un più attento rispetto dei princìpi di liceità, correttezza ed essenzialità del trattamento posto in essere, con riferimento alle modalità di acquisizione e raccolta dei dati stessi, soprattutto nell'ambito del processo civile e nei casi di giudizi di separazione tra coniugi.

In risposta a segnalazioni pervenute l'Autorità ha comunque ribadito che valutare la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di documenti e provvedimenti, anche se basati su un trattamento di dati personali non legittimo, spetta al giudice e non al Garante.

Il codice di deontologia e di buona condotta

Gli aspetti di maggiore novità introdotti dal codice per le indagini difensive, il cui rispetto costituisce, come noto, condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali (art. 12, comma 3, del Codice), riguardano l'ambito di applicazione, i tempi di conservazione delle informazioni, i rapporti con i terzi e la stampa e le modalità di trattamento dei dati personali per le finalità sopra richiamate.

In particolare, gli avvocati e gli investigatori privati possono informare la clientela anche oralmente in modo semplice e colloquiale sull'uso che verrà fatto dei loro dati personali. L'informativa scritta potrà anche essere affissa nello studio o pubblicata sul sito *web*.

I soggetti destinatari del codice deontologico devono fornire istruzioni al personale di studio in modo da adottare speciali cautele in caso di utilizzo di registrazioni audio/video, di tabulati telefonici, di perizie e di ogni altra documentazione utilizzata, e vigilare affinché si eviti l'uso ingiustificato di informazioni che potrebbero comportare gravi rischi per il cliente. Atti e documenti, una volta estinto il procedimento o il mandato, possono essere conservati, in originale o in copia, solo se necessari per altre esigenze difensive della parte assistita o dell'avvocato.

Gli investigatori, da parte loro, non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta dei dati. Le investigazioni sono lecite solo se l'incarico è conferito per iscritto da un difensore o da un altro soggetto. L'incarico ricevuto va eseguito personalmente: ci si può avvalere di altri investigatori privati se nominati all'atto del conferimento oppure successivamente purché tale possibilità sia stata prevista. Conclusa l'attività investigativa, e comunicati i risultati al difensore o a chi ha conferito l'incarico, i dati raccolti devono essere cancellati. L'archivio deve essere periodicamente controllato e contenere solo informazioni pertinenti ed indispensabili.

Dati genetici e difesa in giudizio

Con *provvedimento* del 27 novembre 2008 [doc. *web* n. 1581365] il Garante si è pronunciato in materia di trattamento di dati genetici da parte di avvocati e investigatori privati.

Il *provvedimento* trae origine da una vicenda in cui, su incarico del legale del genitore, un'agenzia di investigazioni ha prelevato campioni genetici del figlio, all'insaputa di questi, poi sottoposti, senza informare l'interessato, al *test* per appurare la compatibilità genetica tra figlio e genitore. Venuto a conoscenza del fatto al momento della proposizione dell'azione di disconoscimento di paternità proposta dal padre, il figlio si è rivolto al Garante. La società di investigazioni e l'avvocato si sono difesi affermando che la legge garantirebbe la possibilità di effettuare analisi genetiche senza richiedere il consenso dell'interessato qualora si tratti di far valere o difendere un diritto in sede giudiziaria.

L'Autorità ha invece ritenuto violati i diritti del figlio e ha vietato al genitore e al suo legale l'ulteriore trattamento dei dati genetici acquisiti, salvo quelli già depositati in giudizio.

Ha ricordato che, anche sulla base delle prescrizioni impartite dal Garante con le autorizzazioni generali al trattamento dei dati genetici, la raccolta e il trattamento di tale tipologia di dati, di natura particolarmente delicata, può avvenire esclusivamente con il consenso informato, *"manifestato previamente e per iscritto"*, dell'interessato. Si può derogare all'obbligo del previo consenso per far valere o difendere un proprio diritto in sede giudiziaria, ma solo nel caso in cui l'accertamento sia assolutamente *"indispensabile"*, circostanza che non ricorreva nel caso di specie.

13. TRATTAMENTO DEI DATI PERSONALI IN AMBITO CONDOMINIALE

Continuano a pervenire numerose segnalazioni, dal contenuto più vario, relative ad attività connesse all'amministrazione dei condomìni, già oggetto del *provvedimento* generale 18 maggio 2006 [doc. *web* n. 1297626] (Per quanto riguarda la videosorveglianza in ambito condominiale si rimanda al *par.* 15.3).

Dati personali nel regolamento condominiale

In una segnalazione la proprietaria di un immobile ha lamentato l'avvenuta indicazione, nell'atto di deposito del regolamento di condominio, del proprio stato civile (di persona legalmente separata) da parte dell'impresa costruttrice dell'immobile stesso. Invitata a fornire chiarimenti, la società in questione ha precisato che l'indicazione dello stato civile nella nota di trascrizione del regolamento condominiale risultava necessaria in quanto l'art. 2659 c.c. impone al richiedente la trascrizione di un atto tra vivi di presentare presso la conservatoria dei registri immobiliari una nota contenente anche il *"regime patrimoniale"* delle parti. Di qui la necessità di indicare la condizione di legalmente separata della segnalante, in quanto funzionale all'indicazione dello stesso regime patrimoniale di separazione dei beni della stessa. Alla luce di tale disposizione l'Autorità dopo aver richiesto alla segnalante eventuali ulteriori elementi di valutazione, non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali (*Nota* del 3 ottobre 2008).

Dati personali nelle tabelle relative alle spese di riscaldamento

In una segnalazione una condòmina ha contestato che nella tabella di ripartizione delle spese di riscaldamento fosse indicata la sua qualità di ex moglie di altro condomino. Poiché il condominio (tramite l'amministratore) ha dichiarato di essersi attivato ai fini della rettifica dell'anagrafica del riparto del riscaldamento non si è ritenuto necessario promuovere l'adozione di un provvedimento da parte dell'Autorità (artt. 14, comma 2, e 11, comma 1, lett. *d*), reg. Garante n. 1/2007) (*Nota* 31 ottobre 2008).

Partecipazione di terzi all'assemblea condominiale

In un caso, è stato chiesto di verificare se la partecipazione di alcuni soggetti non appartenenti alla compagine condominiale a due assemblee di condominio fosse conforme alla disciplina di protezione dei dati. Dalle risultanze istruttorie non è risultato chiaro a che titolo uno dei predetti soggetti avesse partecipato ad una delle due assemblee. Nondimeno, considerato che l'amministratore di condominio ha dichiarato, ai sensi dell'art. 168 del Codice, di aver preso atto delle indicazioni fornite dall'Autorità e di averne

fatto puntuale applicazione nei confronti dei soggetti attualmente amministrati, non si sono ravvisati gli estremi per promuovere l'adozione di un provvedimento da parte dell'Autorità (artt. 14, comma 2, e 11, comma 1, lett. *d*), reg. Garante n. 1/2007) (*Nota* 20 gennaio 2009).

L'Autorità è intervenuta anche nei confronti di due reclamanti che hanno lamentato, nel corso di un'assemblea condominiale tenutasi nel 2005, l'avvenuta comunicazione ad estranei alla compagine condominiale di dati personali relativi al loro contenzioso con il condominio, nonché alla loro condizione di morosità. Dagli elementi acquisiti non è risultato provato che i soggetti estranei (un tecnico e il rappresentante legale di una ditta appaltatrice di lavori condominiali) avessero assistito solamente alla trattazione del punto all'ordine del giorno che li riguardava, poiché il verbale non dava conto di tale circostanza. L'Autorità ha quindi ravvisato nel caso una comunicazione a terzi dei dati personali dei reclamanti, in violazione del principio di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), oltre che in assenza del consenso degli interessati (ovvero di altro presupposto di liceità del trattamento: art. 24 del Codice). Il titolare del trattamento è stato pertanto invitato a fornire riscontro (regolarmente pervenuto) in ordine alle misure adottate per evitare, in futuro, il ripetersi di eventi analoghi (*Nota* 16 aprile 2008).

Comunicazione di dati personali in occasione di contratti di fornitura di beni e servizi

Alcuni rappresentanti dell'Anaci hanno formulato a questa Autorità un quesito (occasionato dalla sentenza Cass. S.u. 8 aprile 2008, n. 9148) sulla liceità della comunicazione nei confronti di fornitori di beni e servizi condominiali (di regola a cura dell'amministratore) di dati personali dei condomini. Richiamati preliminarmente i princìpi sanciti nel *Provv.* del 18 maggio 2006 [doc. *web* n. 1297626], è stato rappresentato che, anche a seguito della richiamata sentenza, non sono ravvisabili ostacoli alla menzionata comunicazione. Infatti, questa può essere effettuata in assenza del consenso degli interessati per dare esecuzione agli obblighi derivanti da un contratto stipulato dai partecipanti alla compagine condominiale, ancorché di regola per il tramite dell'amministratore (art. 24, comma 1, lett. *b*), del Codice), ed eventualmente per far valere o difendere un diritto in sede giudiziaria (art. 24, comma 1, lett. *f*), del Codice). Le informazioni comunicate devono essere comunque pertinenti e non eccedenti (tali possono ritenersi quelle che con-

sentono di identificare i condòmini obbligati al pagamento di corrispettivi dei contratti, le rispettive quote millesimali ed eventuali ulteriori informazioni necessarie a determinare le somme individualmente dovute) (*Nota* 26 settembre 2008).

Affissione di dati personali in spazi condominiali accessibili al pubblico

Il conduttore di una stanza di un appartamento di proprietà di un condominio ha lamentato l'avvenuta diffusione della notizia relativa alla scadenza prossima del suo contratto di locazione e la contestuale intimazione al rilascio dell'immobile da parte della stessa compagine condominiale, ancorché per il tramite dell'amministratore. L'avviso avrebbe potuto essere comunicato agli altri condomini con modalità alternative all'affissione nella bacheca condominiale, quali l'inserimento nelle cassette postali di una comunicazione individualizzata.

Il condominio (in persona dell'amministratore), invitato ad adeguarsi alle prescrizioni del *Provvedimento* 18 maggio 2006 [doc. *web* n. 1297626], ha dichiarato di aver immediatamente sostituito il predetto avviso con altro privo di indicazione di dati personali. Il segnalante ha però contestato che il *"nuovo"* avviso, benché privo di riferimenti espressi, conteneva tuttavia indicazioni idonee a renderlo identificabile, ancorché indirettamente (art. 4, comma 1, lett. *b*) del Codice).

L'Autorità, ritenendo fondata la segnalazione (anche in ragione del fatto che la disdetta del contratto di locazione avrebbe potuto essere comunicata con modalità tali da non renderne edotti soggetti estranei alla compagine condominiale), ha vietato al condominio l'ulteriore diffusione dei dati personali riferiti anche indirettamente al segnalante e relativi alla scadenza del contratto di locazione (*Provv.* 20 novembre 2008 [doc. *web* n. 1576139]).

Assemblea condominiale e divulgazione dati personali

Alcuni condòmini hanno lamentato un'illecita divulgazione della loro situazione debitoria nei confronti del costruttore del medesimo immobile a fronte della fornitura, resa loro in passato di servizi per l'erogazione di energia elettrica da parte dell'amministrazione condominiale, che avrebbe allegato all'avviso di convocazione dell'assemblea di condominio un prospetto contenente anche i predetti dati. A detta dei segnalanti la predetta situazione debitoria sarebbe stata ascrivibile a spese afferenti non la gestione condominiale, ma servizi fruiti uti singuli dagli interessati. L'istruttoria espletata ha confermato la fondatezza di questa prospettazione, sicché le modalità di comunicazione sono risultate in contrasto

con la disciplina applicabile (art. 23 del Codice; *Provv.* 18 maggio 2006 [doc. *web* n. 1297626]). Il condominio (tramite dell'amministratore) è stato invitato ad adeguarsi ai princìpi di protezione dei dati personali richiamati nel menzionato *provvedimento* generale; a seguito del riscontro fornito non sono stati ravvisati presupposti per l'adozione di un provvedimento da parte dell'Autorità (art. 14, comma 2, e 11, comma 1, lett. *d*), reg. Garante n. 1/2007) (*Nota* 26 giugno 2008).

14. Sicurezza dei dati e dei sistemi

14.1. Conservazione dei dati di traffico: misure e accorgimenti a garanzia dei cittadini

Il Garante, anche nel 2008 ha seguito con attenzione le questioni legate al tema della conservazione dei dati di traffico telefonico e telematico sia per finalità di accertamento e repressione dei reati sia per altre finalità ordinarie.

Nella *Relazione* 2007 si è riferito del *provvedimento* del 17 gennaio 2008 (*G.U.* 5 febbraio 2008 n. 30 [doc. *web* n. 1482111]), con il quale l'Autorità ha prescritto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, ai sensi degli artt. 17, 123 e 132 del Codice, l'adozione entro il 31 ottobre 2008 di specifici accorgimenti e misure in grado di garantire un elevato livello di protezione dei predetti dati di traffico.

Il *provvedimento* del 17 gennaio è stato successivamente aggiornato con quello del 24 luglio 2008 (*G.U.* 13 agosto 2008, n. 189 [doc. *web* n. 1538224]), in ragione delle modifiche nel frattempo apportate alla normativa di riferimento da diversi interventi legislativi quali, in particolare, il d.lg. 30 maggio 2008, n. 109 e la l. 18 marzo 2008, n. 48.

Con tale *provvedimento* il Garante ha inoltre accolto – in ragione della complessità degli interventi necessari per adeguare i sistemi informativi dei fornitori alle prescrizioni del *provvedimento*, nonché delle predette modifiche normative – la richiesta presentata singolarmente da alcuni gestori, nonché dall'associazione Asstel, di un differimento del suindicato termine del 31 ottobre 2008.

Il termine è stato così prorogato al 30 aprile 2009 con riferimento alle nove prescrizioni previste per i trattamenti di dati per finalità di accertamento e repressione dei reati, nonché alle cinque prescrizioni relative ai trattamenti di dati ai sensi dell'art. 123 del Codice. È stato infine differito al 30 giugno 2009, il termine riguardante la *strong authentication* riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di *call center*.

Successivamente, nel mese di aprile 2009 sono pervenute all'Autorità numerose richieste da parte di alcune associazioni rappresentative del mondo delle telecomunicazioni, con

le quali è stata descritta una situazione di sostanziale, ma non ancora integrale, adeguamento, per la quasi totalità dei fornitori, alle prescrizioni contenute nel *provvedimento* del 24 luglio 2008 in materia di *data retention*, con particolare riferimento alle misure e agli accorgimenti prescritti alla lettera *a*), nn. 3, 6 e 9 e alla lettera *c*) dello stesso.

Le medesime associazioni hanno, quindi, richiesto al Garante un rinvio dei termini indicati nel *provvedimento*, al fine di realizzare il completamento dell'attuazione delle richiamate prescrizioni.

Il Garante in ragione dell'elevato numero di piattaforme e sistemi aziendali coinvolti negli adempimenti previsti dal *provvedimento*, e, quindi, della complessità degli interventi necessari ha accordato la richiesta proroga, limitatamente alle misure specificamente indicate.

L'Autorità, pertanto, con il *provvedimento* del 29 aprile 2009 (in corso di pubblicazione nella *G.U.* [doc. *web* n. 1612508]), ha fissato il nuovo termine al 15 dicembre 2009, prevedendo altresì che, entro la medesima data, tutti i titolari del trattamento interessati debbano dare conferma al Garante delle misure e degli accorgimenti adottati, attestandone l'integrale adempimento (*cfr.* lett. *b*) del *provvedimento* 24 luglio 2008).

Come si è detto, il quadro normativo in materia di conservazione dei dati di traffico (*v.* anche, *par.* 2.1.) a partire dall'entrata in vigore del Codice, ha subito numerose modificazioni ad opera di altrettanti interventi legislativi, che hanno fissato di volta in volta differenti tempi di conservazione dei dati di traffico telefonico e telematico.

L'art. 132 del Codice, modificato prima della sua entrata in vigore dal d.l. n. 354/2003 (convertito in legge, con modificazioni, dall'art. 1 della l. n. 45/2004), ha introdotto un distinto obbligo, per i fornitori di servizi di comunicazione elettronica, di conservare per finalità di accertamento e repressione dei reati i dati di traffico telefonico relativi ai servizi offerti per due periodi di ventiquattro mesi ciascuno.

Un successivo provvedimento d'urgenza del 2005 (d.l. n. 144/2005, convertito in legge, con modificazioni, dall'art. 1 della l. n. 155/2005) ha poi introdotto: l'obbligo di conservazione dei dati di traffico telematico, escludendone i contenuti, per due periodi di sei mesi ciascuno; l'obbligo di conservazione dei dati relativi alle chiamate telefoniche

senza risposta; particolari modalità di acquisizione dei dati con riferimento ai primi ventiquattro mesi di conservazione dei dati del traffico telefonico e ai primi sei mesi di conservazione dei dati del traffico telematico.

Il predetto provvedimento d'urgenza ha, inoltre, introdotto un regime transitorio in virtù del quale è stata sospesa temporaneamente l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati di traffico, anche se non soggetti a fatturazione, fissando il termine al 31 dicembre 2007. Questo è stato successivamente prorogato al 31 dicembre 2008 dal d.l. n. 248/2007 (convertito in legge, con modificazioni, dall'art. 1 della l. n. 31/2008).

Successivamente, è intervenuta in materia la Direttiva 2006/24/Ce, la quale contiene specifiche indicazioni sia sui tempi di conservazione dei dati di traffico (minimo sei mesi e massimo due anni), sia sulla corretta e uniforme individuazione delle categorie di dati da conservare, in relazione ad alcuni specifici servizi offerti dai fornitori (telefonia di rete fissa e telefonia mobile, accesso a Internet, posta elettronica in Internet e telefonia via Internet).

In attuazione della Direttiva 2006/24/Ce della quale, come si è detto, il Garante aveva già tenuto conto nell'adozione del provvedimento del 17 gennaio 2008, il d.lg. 30 maggio 2008 n. 109, modificando l'art. 132 *citato*, ha previsto un periodo unico di conservazione pari a ventiquattro mesi per i dati di traffico telefonico, a dodici mesi per i dati di traffico telematico e a trenta giorni per i dati relativi alle chiamate senza risposta, senza ulteriori distinzioni in base al tipo di reato.

La legge n. 48/2008, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica stipulata a Budapest il 23 novembre 2001, ha poi nuovamente modificato l'art. 132 del Codice, prevedendo una specifica ipotesi di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati.

Sulla materia è successivamente intervenuto il d.l. 2 ottobre 2008, n. 151 (convertito in legge, con modificazioni, dall'art. 1 della l. n. 186/2008), il quale, introducendo alcune modifiche e integrazioni nell'art. 6 del citato d.lgs. 109/2008, ha prorogato al 31 marzo

2009 il regime transitorio sopra descritto, che consente di conservare i dati di traffico telefonico e telematico, differendo così ulteriormente l'applicazione della disciplina contenuta nella Direttiva 2006/24/Ce.

14.2. MISURE DI SICUREZZA

Sicurezza dei dati e dei sistemi

In riscontro a taluni quesiti della Federazione nazionale agricoltura (Fna-Confsal), l'Autorità è tornata a fornire chiarimenti sulle misure di sicurezza prescritte dal Codice (artt. 31 e *ss.* ed Allegato B. al Codice).

Muovendo dalla preliminare necessità di chiarire – anche in base all'atto costitutivo o allo statuto – se i soggetti indicati dall'associazione operino quali titolari del trattamento (artt. 4, comma 1, lett. *f*) e 28 del Codice) l'Autorità ha precisato che: le *cd. "misure minime di sicurezza"* vanno applicate con una diversa gradazione a seconda che i trattamenti di dati personali, siano effettuati con o senza l'ausilio di strumenti elettronici (artt. 33-35 del Codice e Allegato B.); il documento programmatico sulla sicurezza (Dps) deve essere redatto da ogni titolare, anche attraverso il responsabile, se designato (regola 19 dell'Allegato B. *cit.*), se i dati sensibili e/o giudiziari sono trattati con strumenti elettronici (art. 34, comma 1, lett. *g*), del Codice e regola 19 dell'Allegato B. al Codice) considerando, ove opportuno, la *"Guida operativa"*, curata dal Garante (doc. *web* n. 1007740) e le recenti semplificazioni introdotte dall'art. 29 del decreto-legge 25 giugno 2008, n. 112 (delle quali il Garante ha tenuto conto nell'adottare il *provvedimento* del 27 novembre 2008 [doc. *web* n. 1571218]. Tali disposizioni si applicano ai trattamenti con strumenti elettronici di dati non sensibili o dei soli dati sensibili inerenti allo stato di salute di dipendenti e collaboratori, senza indicazione della relativa diagnosi, ovvero di dati relativi all'adesione a organizzazioni sindacali. In tali casi, la tenuta di un aggiornato dps è stata sostituita da un'autocertificazione (resa dal titolare del trattamento ai sensi dell'articolo 47 del d.P.R. 28 dicembre 2000, n. 445) che attesta che il trattamento riguarda soltanto tali dati personali nell'osservanza delle altre misure di sicurezza prescritte come modificato dalla legge di conversione 6 agosto 2008, n. 133). La Federazione può predisporre un unico modello di dps recepibile dai titolari del trattamento che ad essa afferiscono, ciascuno tenendo conto delle