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

operazioni in concreto effettuate e delle modalità di trattamento utilizzate; ciascun titolare può designare uno o più *"responsabili del trattamento"* purché in possesso dei requisiti prescritti dall'art. 29 del Codice (*Nota* 3 febbraio 2009).

14.3. PRESCRIZIONI SULLA SICUREZZA DEI DATI NEGLI UFFICI GIUDIZIARI

È stato riferito nella *Relazione* 2007 che con *provvedimento* del 15 novembre 2007 (doc. *web* n. 1480605) il Garante ha indicato al Tribunale ordinario di Roma la necessità di apportare alcune modificazioni e integrazioni alle misure di sicurezza adottate, volte a rafforzare il livello di protezione dei dati personali trattati ai sensi dell'art. 47, comma 2, del Codice.

Nel dare tempestivo riscontro al *provvedimento*, il Tribunale ha rappresentato di avere dato attuazione solo parziale a tali indicazioni, adducendo, per le misure non realizzate, attinenti alla complessiva organizzazione e funzionamento dei servizi, la mancanza di spazi disponibili e la cronica mancanza di personale, e comunicando, quanto all'adozione delle misure di natura informatica, di avere interessato le competenti strutture del Ministero della giustizia (già destinatario di copia del *provvedimento* del 15 novembre 2007).

Il Garante ha quindi adottato il *provvedimento* del 13 ottobre 2008 [doc. *web* n. 1565790] con il quale, preso atto della mancata realizzazione delle misure prescritte, e considerato che tale attuazione dipende per lo più da misure strutturali e dalla disponibilità delle indispensabili risorse finanziarie, ha indicato al Ministero della giustizia la necessità di fornire al Tribunale ordinario di Roma le risorse materiali, tecniche e umane idonee a consentire al Tribunale stesso di apportare le modificazioni e integrazioni indicate nel *provvedimento* del novembre 2007.

14.4. SICUREZZA DEI DATI RELATIVI A RIFIUTI ELETTRICI ED ELETTRONICI

Disciplina di protezione dei dati personali e rifiuti elettrici ed elettronici (Raee)

A seguito di alcune segnalazioni (relative al rinvenimento di dati personali all'interno di apparecchiature cedute a rivenditori per la dismissione o per far valere la garanzia) e di notizie di stampa sul rinvenimento di dati bancari di oltre un milione di individui in un disco rigido usato commercializzato attraverso un sito Internet, il Garante ha adottato un

provvedimento generale sui rischi derivanti dalla circolazione di componenti elettroniche "usate" contenenti dati personali, con particolare riguardo all'eventuale accesso di terzi ai dati memorizzati all'interno di apparecchiature destinate alla dismissione (o oggetto di nuova commercializzazione). Ciò anche in ragione dell'adozione del d.lg. 25 luglio 2005, n. 151 (attuativo di normativa comunitaria in materia), che prevede misure volte a favorire il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti.

La menzionata disciplina (e la normativa secondaria che ne è derivata) – che non si occupa dei profili di protezione dei dati personali – lascia impregiudicati gli obblighi gravanti sui titolari del trattamento relativamente alle misure di sicurezza adottate. Ne consegue che ogni titolare è tenuto ad adottare misure organizzative e tecniche per garantire l'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali contenuti nei supporti elettrici ed elettronici in occasione della dismissione di apparati elettrici ed elettronici (art. 31 e *ss.* del Codice). Ciò, anche incaricando soggetti tecnicamente qualificati (che attestino l'esecuzione di tali operazioni o si impegnino ad effettuarle), qualora il titolare non sia in grado di cancellare effettivamente i dati o di anonimizzarli. L'Autorità ha anche indicato ai titolari dei trattamenti alcune procedure (suscettibili di aggiornamento alla luce dell'evoluzione tecnologica) ritenute idonee a garantire che, in sede di reimpiego, riciclaggio, ovvero di smaltimento di apparecchiature elettriche ed elettroniche, siano effettivamente cancellati (o resi anonimi) i dati personali ivi memorizzati (*Provv.* 13 ottobre 2008 [doc. *web* n. 1571514]).

14.5. IL RUOLO DEGLI AMMINISTRATORI DI SISTEMA NELLA SICUREZZA DEI TRATTAMENTI

Individuazione degli amministratori di sistema e controllo del loro operato

Il ruolo dell'amministratore di sistema, rilevante per alcuni profili nel diritto penale (*v.* artt. 615-*ter*, 635-*bis*, *ter*, *quater* e *quinquies*, nonché 640 del c.p.) e nella disciplina di protezione dei dati previgente al Codice del 2003, non ha avuto adeguata disciplina, nonostante la sua particolare delicatezza, tenuta in considerazione nell'ambito di piani di sicurezza o di documenti programmatici elaborati da aziende e organizzazioni. L'attività ispettiva svolta dal Garante rispetto a banche dati di grande rilievo, ma anche in sistemi di minore complessità, ha consentito tuttavia di rilevare preoccupanti sottovalutazioni

dei rischi e carente consapevolezza delle criticità insite nello svolgimento di tali delicate mansioni.

Pertanto l'Autorità è intervenuta (*Provv.* 27 novembre 2008, in *G.U.* 24 dicembre 2008, n. 300 [doc. *web* n. 1577499]) per richiamare tutti i titolari di trattamenti effettuati, anche solo in parte, mediante strumenti elettronici, alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema, fissando nel contempo le regole per l'adozione da parte di enti, amministrazioni pubbliche e società private delle misure tecniche e organizzative che riguardano tale peculiare figura.

Sono stati compresi nella definizione di *"amministratore di sistema"* i soggetti chiamati a svolgere funzioni di gestione e manutenzione di un impianto di elaborazione che possono comportare la possibilità tecnica di accesso a tutti i dati personali memorizzati o trasmessi tramite i sistemi informatici; pertanto sono stati considerati equivalenti, e compresi nella definizione ai fini del *provvedimento*, gli amministratori di basi di dati, di reti e di apparati di sicurezza, di sistemi *software* complessi.

Le misure sono dirette ad agevolare la verifica sull'attività degli amministratori da parte di chi ha la titolarità delle banche dati e dei sistemi informatici, e non riguardano i trattamenti di dati effettuati a fini amministrativo contabili, che pongono minori rischi per gli interessati e che sono stati oggetto di misure di semplificazione.

Tra le misure prescritte è compresa la registrazione degli accessi (autenticazioni informatiche) degli amministratori ai sistemi di elaborazione e agli archivi elettronici, da conservare per un periodo non inferiore a sei mesi. Analogamente a quanto avviene per i responsabili del trattamento, l'operato degli amministratori di sistema deve essere verificato, ma con periodicità annuale, dai titolari del trattamento, mentre i loro estremi identificativi e l'elenco delle funzioni loro attribuite devono essere riportati in un documento da rendere disponibile in caso di accertamenti da parte del Garante, anche nel caso in cui la funzione sia svolta a qualsiasi titolo da soggetti esterni all'organizzazione, ovunque operanti. Quale misura di trasparenza interna alle aziende e alle organizzazioni, è stata poi prevista l'instaurazione di un regime di conoscibilità dell'identità degli amministratori di

sistema addetti a trattamenti di dati personali che riguardino i lavoratori operanti a qualsiasi titolo in aziende e in organizzazioni.

Il Garante, in ragione della complessità degli interventi organizzativi e tecnici necessari, su richiesta di alcune associazioni di operatori interessati ha prorogato i termini per gli adempimenti. In particolare, dopo l'unificazione dei termini e il differimento al 30 giugno 2009 (*Provv.* 12 febbraio 2009, in *G.U.* n. 45 24 febbraio 2009 [doc. *web* n. 1591970]), ha avviato una consultazione pubblica (*Provv.* 21 aprile 2009 – in corso di pubblicazione in *Gazzetta Ufficiale* – per *"acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del dispositivo del provvedimento del 27 novembre 2008"*), fornendo nel contempo, tramite il proprio sito, le risposte alle domande più frequenti (*faq*).