16 Sicurezza dei dati e dei sistemi

Il Garante ha proseguito l'attività di divulgazione delle norme del Codice e delle regole dell'Allegato B. al Codice medesimo in materia di misure di sicurezza, prescrivendo a diversi titolari del trattamento gli accorgimenti da porre in essere per garantire la rigorosa osservanza di dette disposizioni.

Così è avvenuto nelle decisioni adottate ai sensi dell'art. 17 del Codice a seguito di interpello dei titolari del trattamento interessati a dotarsi di sistemi di riconoscimento biometrico nei luoghi di lavoro (sulle quali *v.* il *par.* 17.1).

In un caso, riguardante il trattamento di dati personali di lavoratori con finalità di accesso ai locali aziendali mediante un sistema basato sull'impiego della tecnologia *Rfid cd.* "passiva", la società titolare del trattamento è stata invitata a farsi rilasciare dall'installatore il prescritto attestato di conformità e a conservarlo presso la propria struttura (*cfr.* regola n. 25 dell'Allegato B. al Codice), come pure a designare per iscritto i soggetti che effettuano operazioni di trattamento dei dati registrati nel sistema come incaricati o, eventualmente, responsabili di tali operazioni, impartendo loro idonee istruzioni alle quali attenersi (*cfr. par.* 10.3.1).

I principi in materia sono stati richiamati anche nei provvedimenti adottati, nel corso del 2006, in materia di tessere elettroniche rilasciate dai concessionari dei servizi di trasporto pubblico dei Comuni di Roma e Milano (*Provv.* 6 settembre 2006 [doc. *web* n. 1339531 e n. 1339692]), sui quali *v.* il *par.* 13.

Puntuali indicazioni e prescrizioni sulla sicurezza dei dati sono contenute, poi, sia nelle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", sia nel provvedimento generale "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori" (*Provv.* 23 novembre 2006 [doc. *web.* n.1364939] e *Provv.* 1° marzo 2007 [doc. *web* n. 1387522]), sui quali si *v.* il *par.* 10.3.2).

Con un provvedimento adottato in materia di trattamento di dati di un ex-dipendente di banca, il Garante ha infine prescritto al datore di lavoro (artt. 143, comma 1, lett. *b*), e 154, comma 1, lett. *c*), del Codice) la misura opportuna dell'aggiornamento delle istruzioni scritte rese ai lavoratori designati quali incaricati del trattamento dei dati trattati nell'ambito delle mansioni rivestite (*Provv.* 25 gennaio 2007 [doc. *web* n. 1381999], sul quale si *v.* il *par.* 10.3.1).

16.1. *La messa in sicurezza dei sistemi dei gestori telefonici*

Prescrizioni tecniche per eseguire intercettazioni giudiziarie

Sono stati svolti numerosi accertamenti e verifiche in merito all'adozione, da parte dei fornitori di servizi di comunicazione elettronica, delle misure e degli accorgimenti prescritti in materia di sicurezza con il *provvedimento* del 15 dicembre 2005 [doc. *web* n. 1203890] in relazione alle attività poste in essere per adempiere alle richieste dell'autorità giudiziaria nell'ambito delle intercettazioni telefoniche e telematiche (*cfr. Relazione* 2005, *par.* 15.7). Per facilitare il corretto adempimento delle prescrizioni contenute nel predetto provvedimento, l'Autorità ha collaborato anche con associazioni di categoria.

16

Il Garante ha prestato attenzione al problema della sicurezza anche in riferimento al versante degli uffici giudiziari, intervenendo con numerose note dirette ai vertici dell'amministrazione giudiziaria e a tutte le procure.

Il tema del trattamento dei dati connessi alle intercettazioni presso i fornitori di servizi telefonici riveste particolare importanza in riferimento alla sfera personale degli indagati (e delle altre persone estranee alle indagini, ma coinvolte nelle comunicazioni e conversazioni), nonché alla segretezza delle indagini. Pur non dovendo venire a conoscenza dei "contenuti" i fornitori raccolgono, selezionano ed elaborano una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali essi comunicano. Si tratta di dati personali riservati e delicati che attengono, in particolare, all'identità dei soggetti sottoposti ad intercettazione, all'arco temporale di svolgimento dell'intercettazione e ai dati di traffico telefonico o telematico inerenti alle linee intercettate (data, ora, numero chiamato e durata della comunicazione o conversazione). A seconda dei casi, tenendo conto delle specifiche richieste dell'autorità giudiziaria, i medesimi dati sono integrati da informazioni tecniche aggiuntive relative ai dettagli delle chiamate entranti, ai tentativi di chiamata in entrata o in uscita e ai dati di localizzazione geografica dell'utenza intercettata. I fornitori di telefonia mobile tengono traccia anche dell'identificativo numerico della stazione base impegnata dall'utenza intercettata. I servizi di messaggistica del tipo *Sms*/*Mms* sono compresi nelle attività di intercettazione. Le intercettazioni telematiche sono quantitativamente meno rilevanti rispetto a quelle telefoniche e riguardano in prevalenza sia il traffico Ip sviluppato su linee telefoniche o collegamenti a larga banda, sia comunicazioni tramite posta elettronica. Queste ultime vengono realizzate predisponendo un inoltro automatico della corrispondenza ricevuta e spedita dall'intercettato mediante un'utenza di posta elettronica messa a disposizione dal fornitore.

Le operazioni svolte a supporto dell'attività investigativa possono riguardare aspetti diversi dalle intercettazioni. Tra tali operazioni sono comprese le interrogazioni anagrafiche, la localizzazione dell'utenza, l'identificazione della linea chiamante o della linea connessa, il tracciamento, la sospensione o la limitazione dei servizi agli utenti, la documentazione del traffico pregresso contabilizzato e la documentazione integrale del traffico storico. A differenza di quanto avviene in occasione delle conversazioni telefoniche intercettate, i fornitori hanno la possibilità di conoscere tali informazioni prodotte o raccolte nel compimento delle predette operazioni. Sono i fornitori, infatti, a estrarre i dati, a selezionarli secondo i criteri richiesti dall'autorità giudiziaria, a organizzarli in tabulati e a spedirli al richiedente. In tutte queste fasi, i dati restano nella disponibilità del fornitore e non può essere escluso che gli incaricati operanti in ambito aziendale debbano poterli conoscere, anche in parte, per svolgere alcune operazioni.

Dopo aver esaminato la documentazione trasmessa dai fornitori relativamente alle misure e agli accorgimenti adottati [doc. *web* n. 1348670], il Garante ha prescritto agli stessi un nuovo, breve termine di novanta giorni per completare e comunicare all'Autorità l'adozione delle misure e degli accorgimenti non ancora attuati. Le misure adottate, infatti, sono risultate conformi alle prescrizioni impartite solo in termini generali, in attuazione parziale di quanto prescritto con il provvedimento del 2005 citato. In particolare, l'Autorità ha comunicato a ciascun fornitore coinvolto nel procedimento i singoli punti rispetto ai quali lo stesso doveva provvedere all'integrale adeguamento (*Provv.* 20 settembre 2006 [doc. *web* n. 1341009]).

Tra l'altro, è stato prescritto che le funzioni aziendali cui compete lo svolgimento di servizi per conto dell'autorità giudiziaria adottino un modello organizzativo in grado di limitare al minimo la conoscibilità delle informazioni relative alle attività svolte per esigenze di giustizia, con una rigida partizione della visibilità dei dati su

base organizzativa, funzionale e di area geografica di competenza. Il personale che a qualsiasi titolo tratti questi dati deve essere designato in termini selettivi quale incaricato del trattamento.

Particolare rigore deve essere assicurato nella gestione e nel mantenimento della qualità delle credenziali di autenticazione per l'accesso informatico ai dati trattati, conformando le procedure di gestione delle credenziali e i sistemi di autorizzazione a principi rigidi di coerenza delle abilitazioni nei sistemi informativi con i ruoli e le funzioni assegnate agli incaricati designati.

Deve essere altresì realizzata, anche attraverso l'opportuna configurazione dei sistemi informatici utilizzati, una separazione marcata tra i dati di carattere amministrativo-contabile e i dati documentali prodotti nel corso delle operazioni svolte su richiesta dell'autorità giudiziaria, inibendo la possibilità per un operatore amministrativo-contabile di accedere ai dati documentali prodotti. I fornitori devono provvedere affinché l'interscambio di informazioni con l'autorità giudiziaria avvenga evitando il ricorso a canali non affidabili, o affidabili solo parzialmente, sia dal punto di vista delle prestazioni, sia da quello della sicurezza, adottando a tal fine sistemi di comunicazione basati su aggiornati strumenti telematici sviluppati con protocolli di rete sicuri.

Il Garante ha poi ritenuto necessario che i fornitori sviluppino o integrino strumenti informatici idonei ad assicurare il controllo delle attività svolte da ciascun incaricato sui singoli elementi di informazione presenti nei *data-base* utilizzati. Tutti i dati personali acquisiti o formati per scopi di giustizia devono essere protetti con moderni strumenti di cifratura, precludendo la loro conoscibilità da parte di soggetti non legittimati.

La persistenza di dati personali nei sistemi informativi dei fornitori, se imposta da ragioni tecniche, deve essere comunque strettamente limitata a quanto necessario per attuare i provvedimenti dell'autorità giudiziaria, prevedendone la cancellazione immediatamente dopo la loro corretta comunicazione.

Dall'analisi della documentazione inoltrata dai singoli gestori destinatari delle prescrizioni, pervenuta a fine dicembre, è emerso un quadro di sostanziale conformità alle prescrizioni impartite dall'Autorità, salvo il caso di un fornitore che non ha inizialmente approntato sistemi di posta elettronica certificata (Pec) o altri sistemi sicuri di comunicazione, mantenendo la prassi di ricevere richieste e inviare i dati tramite *fax* analogico e posta elettronica non certificata, modalità non ritenute più conformi agli *standard* di sicurezza più elevati richiesti per i flussi informativi con l'autorità giudiziaria. In ragione di ciò, l'Autorità ha disposto, nei confronti del medesimo fornitore, il blocco della trasmissione dei dati personali da e verso gli uffici giudiziari effettuata con strumenti non idonei (*Provv.* 25 gennaio 2007 [doc. *web* n. 1384870]).

Il Garante ha inoltre proseguito i controlli sul rispetto delle prescrizioni impartite per lo svolgimento delle intercettazioni, monitorando contestualmente l'adozione delle misure anche da parte degli uffici giudiziari e riservandosi la possibilità di elevare ulteriormente i livelli di sicurezza.

Sicurezza presso i gestori telefonici e conservazione dei dati di traffico

Il tema dell'obbligo di conservazione dei dati di traffico telefonico e telematico, che determina la creazione di banche dati di enormi dimensioni, è stato oggetto di grande attenzione da parte dell'Autorità. In particolare, al fine di predisporre il provvedimento generale previsto dall'art. 132 del Codice, con il quale verranno individuate le modalità di conservazione dei dati di traffico delle comunicazioni elettroniche, è stata avviata una serie di complessi accertamenti *in loco* nei confronti di numerosi gestori.

In tale ambito, merita menzione anche l'attività svolta dal Garante in relazione ad un ricorso proposto nel febbraio 2006 da un cittadino che, con riferimento ad

un'utenza telefonica mobile allo stesso intestata, si era visto recapitare in forma anonima presso la propria abitazione un plico contenente un tabulato relativo a chiamate, sia in entrata, sia in uscita, riferite al mese di ottobre 2005 e comprendente un elenco di *cd.* "celle di localizzazione".

Il Garante si è pronunciato su tale ricorso (*Provv.* 1° giugno 2006 [doc. *web* n. 1296533]) prescrivendo all'operatore, anche con un altro provvedimento adottato in pari data (*Provv.* 1° giugno 2006 [doc. *web* n. 1298716]), una serie di accorgimenti volti ad assicurare quelle elevate misure di protezione a garanzia degli interessati con riferimento al trattamento dei dati di traffico che, invece, le concrete vicende esaminate nel corso dell'istruttoria avevano riscontrato essere insufficienti.

Gli accertamenti effettuati dal Garante hanno appurato che il sistema di controllo non era in grado di registrare il dettaglio delle operazioni effettuate da alcuni soggetti che svolgono in particolare operazioni di gestione e manutenzione dei sistemi; circostanza, questa, che esponeva gli abbonati al rischio di gravi abusi per ciò che concerne l'illecita acquisizione dei loro dati di traffico. Il gestore telefonico ha dovuto pertanto adottare misure per assicurare l'identificazione degli accessi ai dati e il controllo sulle operazioni effettuate da ciascun incaricato. Tutte le operazioni compiute sui dati di traffico, anche la sola consultazione, devono ora essere registrate in appositi registri informatici (*audit log*) mentre i profili di autorizzazione degli incaricati devono essere limitati ai dati e alle operazioni loro affidate e non devono consentire di trattare dati personali diversi da quelli necessari.

Con successivo *provvedimento* del 7 dicembre 2006 [doc. *web* n. 1371041] il Garante ha differito il termine per adottare tali misure sino al 31 marzo 2007, ordinando a Telecom Italia S.p.A. di far pervenire, rispettivamente entro il 31 gennaio 2007 e il 28 febbraio 2007, due ulteriori *report* di aggiornamento circa le altre misure di adeguamento nel frattempo adottate, nonché di dare conferma al ricorrente e all'Autorità, entro il 31 marzo 2007, del completamento delle misure di attuazione alle predette prescrizioni.

16.2. *Prescrizioni sulla sicurezza dei dati negli uffici giudiziari*

Il Garante ha preso in esame anche la problematica relativa all'applicazione delle misure di sicurezza nei trattamenti dei dati personali cartacei ed automatizzati, di tipo amministrativo e per ragioni di giustizia, effettuati presso gli uffici giudiziari. Sono state così intraprese iniziative volte anche a sollecitare la collaborazione delle istituzioni e degli uffici interessati, in particolare del Ministero della giustizia e del Consiglio superiore della magistratura, nella convinzione che l'introduzione di livelli elevati di sicurezza nel trattamento dei dati personali contribuisca anche al buon funzionamento delle strutture giudiziarie.

In tale quadro, l'Autorità ha avviato un'attività di verifica in tema di concreta attuazione ed idoneità delle misure di sicurezza adottate presso i tribunali e le procure della Repubblica delle città sedi di corte d'appello.

Il Garante ha altresì previsto una prima serie di accertamenti in relazione ai trattamenti di dati personali effettuati, per motivi di giustizia (art. 47, comma 2, del Codice), presso il Tribunale ordinario di Roma. Gli accertamenti, intrapresi nei modi previsti dalla legge, per il tramite di un componente del Garante da questo designato e con l'assistenza di personale specializzato (art. 160 del Codice), sono tuttora in corso di svolgimento.