SCiNTLEX
Diritto e Società dell'Informazione

SICUREZZA DEI DATI DI TRAFFICO TELEFONICO E TELEMATICO

Tabulati sotto chiave: il Garante detta ai gestori le regole per la tenuta dei dati di traffico telefonico e Internet - 1 febbraio 2008

Un sistema di comunicazioni elettroniche italiane più sicuro e più protetto. Con un provvedimento generale il Garante per la protezione dei dati personali (Francesco Pizzetti, Giuseppe Chiaravalloti, Mauro Paissan, Giuseppe Fortunato), dando attuazione a quanto previsto dal Codice privacy, ha fissato le regole di base per la messa in sicurezza dei dati di traffico telefonico e Internet che vengono conservati dai gestori per finalità di accertamento e repressione dei reati, e per le altre finalità ammesse dalla normativa.

Dopo i gravi abusi emersi in questi ultimi anni, con un provvedimento di cui è stato relatore Francesco Pizzetti, l'Autorità ha imposto ai gestori di servizi telefonici e telematici le misure tecniche e organizzative che garantiscano un elevato livello di protezione, comune a tutto il settore dei servizi di comunicazione elettronica. I dati di traffico telefonico e Internet, che comunque non riguardano il contenuto, 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 di ricostruire tutte le relazioni di una persona e le sue abitudini.

É bene ricordare, peraltro, che in Italia, dopo la recente proroga di fine anno del cosiddetto pacchetto Pisanu, il periodo di conservazione di questi dati a fini di giustizia toccherà gli 8 anni per il traffico telefonico e quasi 4 per quello telematico.

Le prescrizioni impartite sono, in particolare:

Accesso ai dati: l'accesso ai dati è consentito solo al personale incaricato mediante avanzati sistemi di autenticazione informatica, anche con l'uso di dati biometrici (es., impronte digitali). Sono compresi nella prescrizione, salvo limitati casi di necessità, anche gli amministratori di sistema, figure chiave della sicurezza delle banche dati, sul cui ruolo, spesso sottovalutato anche nei settori più delicati, il Garante prevede di iniziare una riflessione approfondita.

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 rigidamente separate. 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 utilizzati per funzioni aziendali (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 rischi di acquisizione indebita, anche fortuita, delle informazioni registrate da parte di incaricati di mansioni tecniche (amministratori di sistema, amministratori di data base, manutentori hardware e software) i dati di traffico trattati per esclusive finalità di giustizia vanno protetti con tecniche crittografiche.

Gestori telefonici e fornitori di servizi di comunicazione elettronica dovranno applicare tali misure entro il 31 ottobre 2008. L'applicazione di alcune di esse viene disposta dal Garante anche alla conservazione dei dati per finalità non di giustizia, ma di fatturazione, commercializzazione di servizi, statistica etc., al fine di favorire un quadro più ampio di sicurezza di dati e sistemi.

Restano esclusi dall'ambito di applicazione di queste regole - sia perchè non assimilabili a veri e propri gestori di servizi tlc e di comunicazione elettronica sia per evitare ingiustificate conservazioni di dati - i gestori di esercizi pubblici e Internet cafè, i gestori di siti Internet che diffondono contenuti sulla rete (content provider), i gestori dei motori di ricerca, le aziende o le amministrazioni pubbliche che mettono a disposizione del personale reti telefoniche e informatiche (es. centralini aziendali) o che si avvalgono di server messi a disposizione da altri soggetti.