

Telefonia e web, dati più protetti
Le nuove disposizioni del garante sulla privacy

ROMA. Un sistema di comunicazioni elettroniche italiane più sicuro e più protetto: questo il senso del provvedimento generale con il quale il Garante per la protezione dei dati personali, dando attuazione a quanto previsto dal codice della 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».

«I dati di traffico telefonico e internet, che comunque non riguardano il contenuto, sono - dice il Garante - 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». Il periodo di conservazione di questi dati a fini di giustizia, con la proroga a fine anno del cosiddetto «pacchetto Pisanu» toccherà gli 8 anni per il traffico telefonico e quasi 4 per quello telematico».

Queste le prescrizioni indicate dal Garante:

Accesso ai dati. E' consentito solo al «personale incaricato mediante avanzati sistemi di autenticazione informatica, anche con l'uso di dati biometrici (esempio, impronte digitali». Sono compresi nella prescrizione, «salvo limitati casi di necessità, anche gli amministratori di sistema».

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 - ha disposto il Garante - «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.

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».