PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 819 di mercoledì 16 luglio 2003

File di log, "nuova" privacy e finalita' investigative

A cura del dott. G. Costabile. "Una delle innovazioni del nuovo codice della privacy, stranamente difficilmente reperibile e non ancora pubblicato in GU, è la previsione ex lege della conservazione di alcuni dati..."

Come già indicato sul numero 813 di PuntoSicuro, il 27 giugno scorso il Consiglio dei Ministri ha accorpato, in un unico codice, le disposizioni in materia di protezione dei dati personali.

Una delle innovazioni più importanti di questo decreto legislativo, stranamente difficilmente reperibile e non ancora pubblicato in Gazzetta Ufficiale, è la previsione ex lege della conservazione di alcuni dati, da parte delle società di telecomunicazione, ai fini investigativi, per favorire l'identificazione e l'accertamento dei responsabili di fatti penalmente rilevanti.

Anche se a molti può sembrare strano fino ad oggi non esisteva alcun obbligo di conservazione dei dati ai fini investigativi. Il decreto legislativo 13 maggio 1998, n. 171 all'art. 4 prevedeva (rectius: prevede fino all'entrata in vigore del T.U.) che i dati personali relativi al traffico potevano essere trattati meramente per finalità di fatturazione e di conseguenza fino alla fine del periodo durante il quale poteva essere legalmente contestata la fattura o preteso il pagamento.

In realtà le società di telecomunicazione fino ad oggi garantivano la conservazione delle informazioni utili all'Autorità Giudiziaria in via generale per 5 anni, pur senza un preciso obbligo giuridico, aderendo all'assunto secondo il quale tali dati potevano essere trattati secondo le stesse modalità e tempistiche della conservazione delle fatture ai fini fiscali.
Negli ultimi anni, a livello internazionale, si è registrato un forte contrasto tra coloro che aspramente contestavano ogni sorta di conservazione, paventando pericolose profilazioni degli utenti e violazioni della privacy, contro i fautori dell'introduzione per legge dell'obbligo di conservazione di queste informazioni digitali, senza il consenso dell'interessato, in quanto asseritamente indispensabili ad accertare i reati informatici, in particolare per l'aumento di quelli aventi ad oggetto la pedopornografia.

Sicuramente la restrizione del diritto alla riservatezza non è necessariamente sinonimo di riduzione dei computer crimes, in quanto gli i cybercriminali più esperti utilizzano tecniche sempre più evolute per aggirare i controlli e non lasciare tracce, ma sarà più agevole effettuare i dovuti accertamenti a posteriori per una buona percentuale di illeciti, avendo cura di incrociare le varie informazioni disponibili.

Con l'approvazione del citato testo unico quindi, che entrerà in vigore per la quasi totalità dal 1 gennaio 2004, le società di telecomunicazioni potranno conservare i dati relativi al traffico, ai fini della fatturazione, contestazione o pretesa del pagamento, per un periodo non superiore ai sei mesi.

Parallelamente invece, in attuazione all'art. 15 della direttiva 2002/58 che attribuisce allo Stato membro la facoltà di adottare disposizioni volte a limitare alcuni diritti ed obblighi previsti dalla medesima direttiva quando ciò sia necessario per eccezionali esigenze di tutela di particolari interessi pubblici delimitati, è stato introdotto l'obbligo di conservazione dei dati relativi al traffico per un periodo non superiore a trenta mesi, per finalità di accertamento e repressione di reati.

Per le modalità operative di "gestione" delle informazioni il legislatore ha preferito rimandare ad un successivo decreto del Ministro della giustizia, di concerto con i ministri dell'interno e delle comunicazioni, su conforme parere del Garante.

Sarà necessario però, in quella sede, impartire modalità operative che consentano di garantire integrità, attendibilità e non ripudiabilità delle informazioni conservate e trattate, da esibire all'Autorità Giudiziaria, agevolando altresì gli investimenti per l'implementazione dei processi di preservazione, archiviazione e protezione dei dati.

Infatti i file di log, che tracciano le varie attività in rete dei navigatori dal momento della connessione, seppure creati in modo

automatico da sistemi informatici e quindi aventi un valore più pregnante nella formazione della prova in un procedimento penale, sono comunque dei semplici file di testo.

Purtroppo in Italia è ancora sottovalutato il problema della conservazione e della "certificazione" di questi preziosi ma "aleatori" dati ai fini investigativi

Attendiamo quindi le disposizioni di dettaglio del legislatore, auspicando che sia garantita la genuinità del dato informatico (Nota 1) , la provenienza e, non in ultimo, un riferimento temporale certo, già previsto per la firma digitale e per la posta elettronica certificata, sensibilizzando quindi i provider ad una maggiore accuratezza ovvero ottemperando sempre meglio ai principi di "confidentiality, integrity, availability" (Nota 2) delle tracce informatiche, fragili per antonomasia.

Per ulteriori approfondimenti si rimanda a quanto scritto dal medesimo autore e reperibile su www.diritto.it.

(Nota 1) Associando un'impronta digitale che distinguerà in maniera univoca il dato, al fine di ottemperare alle citate esigenze di integrità del dato. Tale "sigillo" viene creato con un'operazione cosiddetta di hashing a senso unico, ad esempio con algoritmo MD5.

(Nota 2) Confidenzialità, integrità e disponibilità delle informazioni.

---

www.puntosicuro.it