Hot-Spot, Internet Point e Legge 155/05 Antiterrorismo

di **Nicola Sotira** (nsotira@infomedia.it)

La legge 155/05 firmata dai Ministri ministri Pisanu (Interno), Landolfi (Comunicazioni) e Stanca (Innovazione e tecnologie), riguardante le nuove misure antiterrorismo, sancisce l'obbligo di conservazione da parte di titolari e gestori di Hot-Spot ed Internet Point, sino al 31 dicembre 2007

La costante minaccia del terrorismo internazionale ha spinto i ministri dell'Interno, delle Comunicazioni e dell'Innovazione ad emanare una legge che fa parte delle norme speciali promesse dal governo per contrastare ogni attività sospetta sul territorio. Ogni punto di accesso pubblico dovrà registrare i dati anagrafici e le abitudini di navigazione di tutti gli utenti. L'obiettivo è quello di monitorare la rete delle "postazioni pubbliche non vigilate per comunicazioni telematiche" sempre più usata dai terroristi per scambiarsi messaggi. Pertanto chiunque fornisce un accesso alla Rete, stabilisce la legge, deve "***identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente***".
Inoltre tutti i dati raccolti, tranne i contenuti delle comunicazioni, dovranno essere a completa disposizione delle autorità giudiziarie - almeno fino al 31 dicembre 2007. Fino a questa scadenza i titolari degli Internet Point dovranno "***memorizzare e mantenere i dati relativi alla data ed ora della comunicazione ed alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni***".
Moltissimi i dissensi su questa legge ed autorevoli commentatori hanno gi espresso in forme diverse le loro rimostranze facendo valutazioni sulla valenza giuridica di questa norma.
Comunque al di là dei giudizi di merito, rimane il fatto che le norme del "pacchetto Pisanu" sono legge dello Stato e dunque fatto obbligo di osservarle.

FIGURA 1 Internet point: favorisca i documenti...

Il decreto Pisanu

La prima cosa da chiarire è che non bisogna confondere "dati di traffico" con "contenuto della comunicazione". Questo equivarrebbe a confondere, ad esempio, tra "tabulato di traffico" e "intercettazione della comunicazione". Questo decreto non menziona e non impone nessuna archiviazione del contenuto della comunicazione e non si parla di intercettazione delle comunicazioni.
Vediamo quindi le norme che sono a carico dei "titolari o gestori di un esercizio pubblico o di un circolo privato di qualsiasi specie" nel quale "sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche".
Da quanto si deduce la legge si applica, inequivocabilmente, a Internet-cafè, alberghi che offrano un servizio di Internet, locali pubblici, quali ad esempio aeroporti o biblioteche, università dove si trovino "totem" (o dispositivi similari) mediante i quali i visitatori possano navigare in rete.
I gestori queste tipologie di locali devono adottare misure per il "monitoraggio delle operazioni dell'utente e per l'archiviazione dei relativi dati", nonchè per la "preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili.". Queste misure sono meglio specificate nel Decreto del Ministero degli Interni del 16 agosto 2005 http://www.interno.it/legislazione/pages/pagina.php?idlegislazione=650 .

FIGURA 2 Hot-Spot Manager: la soluzione della società svedese Clavister per la gestione degli accessi conforme al decreto Pisanu.

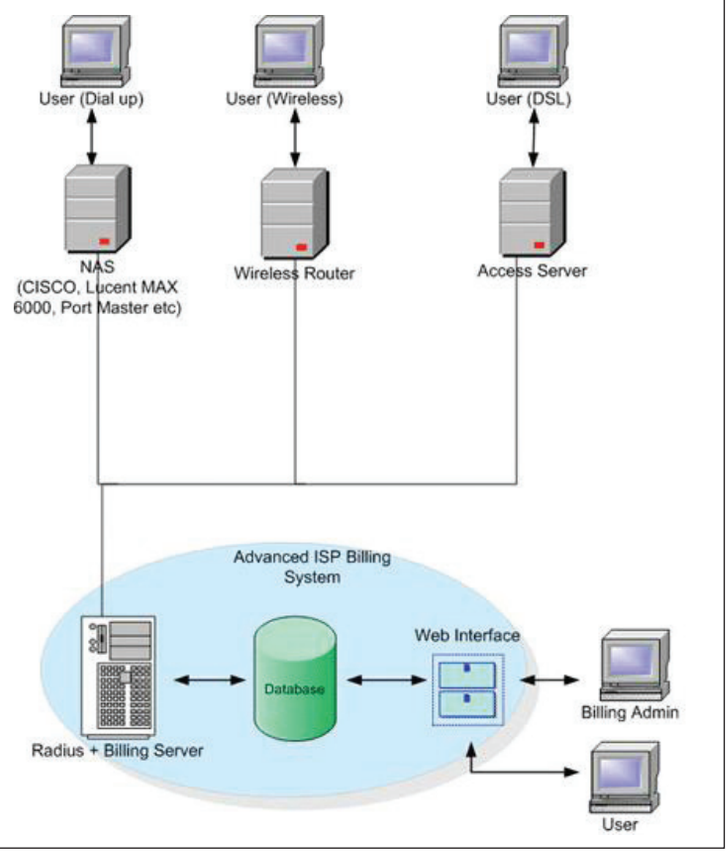
L'esigenza del legislatore quella di identificare, in modo certo, tutti gli utenti che effettuano l'accesso alla rete Internet attraverso un locale pubblico o Hot-Spot. Inoltre si ha l'esigenza di associare a questi utenti i dati salienti della loro navigazione in rete. Questa operazione equivalente a quella oggi già effettuata dagli operatori di telefonia che conservano il nostro traffico telefonico. Pertanto i "dati di traffico" da memorizzare sono: la data e l'ora della comunicazione, "con chi" l'utente dell'Internet Point ha comunicato e in che modalità. Si noti che è assolutamente escluso il contenuto della comunicazione, ovvero il contenuto delle mail, cosa l'utente abbia trasmesso o ricevuto. L'utente deve essere identificato, tramite documento di riconoscimento, prima di cominciare la comunicazione. Questo implica che il gestore del locale/Internet Point deve acquisire tutte queste informazioni, sia quelle sull'identità degli utenti sia quelle sulla loro navigazione, in forma elettronica. Il gestore dovrà inoltre conservare queste informazioni inalterate e inaccessibili a terzi, per la durata prevista dalla legge, salvo presentarle a richiesta alle autorit che hanno il titolo per esaminarle.

Le problematiche tecniche

Vediamo ora cosa ci comporti dal punto di vista operativo e quali problematiche possono insorgere. Il primo problema è quello della univoca identificabilità dell'apparato che origina la comunicazione e dell'utente che la genera. È risaputo che i computer di un Internet Point o di un locale pubblico utilizzano indirizzi IP privati e si presentano sulla rete pubblica con un solo IP legato all'organizzazione. Questa operazione si chiama NAT (*Network Address Translation*) e nasconde all'esterno le identità dei singoli computer posti nella rete privata. Il gestore, dunque, non può ottemperare del tutto alla normativa in quanto non è in grado di poter identificare univocamente chi abbia effettuato una certa operazione in rete nel caso in cui vi sia coincidenza di azioni da parte di più computer locali. Sul traffico di posta elettronica occorre tenere a mente che, generalmente, negli Internet Point/locali pubblici non è quasi mai consentito l'utilizzo di client locali. In genere, infatti, da questi luoghi i server di posta vengono raggiunti utilizzando un' interfaccia Web. Chiaramente questa modalità di accesso si presenta agli apparati di rete come una normale pagina Web, non permettendo in questo modo di capire se l'utente stia leggendo o inviando una mail, a meno di non intercettare il contenuto della sessione, cosa per non consentita dalla legge. Occorrerà poi mantenere questi dati "con modalità che ne garantiscano l'inalterabilità e la non accessibilità da parte di persone non autorizzate". In questo caso o l'applicativo che gestisce i log dispone di queste funzionalità, oppure può essere sufficiente registrare periodicamente questi su CD per garantirsi l'inalterabilità.

Sulle reti wireless il problema è sicuramente più arduo, questo poiché, la norma impone la preventiva identificazione di tutti coloro che accedono ad un sistema Wi-Fi pubblico. Come sappiamo, gli Hot-Spot permettono l'accesso alla rete ad utenti non identificati a priori.
Si pensi, ad esempio, agli Hot-Spot esistenti negli aeroporti, od a quelli in fase di installazione in molti luoghi aperti e pubblici delle nostre città: non è facile identificare praticamente e preventivamente questa tipologia di utenti. Per adempiere alla legge occorre pertanto conservare come minimo tutti i log forniti dal dispositivo di connessione (non il contenuto, solo le sessioni attivate) nonché l'associazione fra l'indirizzo IP interno associato ad ogni computer locale e l'identità della persona che lo ha utilizzato in un dato intervallo di tempo. Questi log devono essere conservati in modalità fisicamente sicura sino al **31/12/2007**.

FIGURA 3 Schema che illustra la modalità di funzionamento della piattaforma della Advanced ISP Billing.



Chi è soggetto alla legge?

Sorge spontanea una domanda: chi è soggetto alla legge? Sembrerebbe di poter dire che il legislatore volesse normare tutte quelle forme di accesso pubblico estemporaneo, quindi non la clientela residenziale degli ISP né quella delle aziende. Vediamo comunque cosa dice la normativa: *le norme si applicano ai titolari o gestori di un esercizio pubblico o di un circolo privato di qualsiasi specie nel quale sono posti a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale*. Pertanto la discriminante è l'apparato terminale che il gestore mette a disposizione del pubblico, come tipicamente avviene negli Internet Point e locali simili. Laddove, quindi, non ci sia il terminale, la legge non si applica, anche se esiste la possibilità di accedere ad Internet con un proprio terminale.
Occorre porre attenzione però, poiché nella circolare del Ministero dell'interno n. 557/2005 si legge: "…*In particolare, gli obblighi di identificazione e registrazione devono essere assolti anche dagli esercenti attività ricettive, laddove vengano offerti alle persone ospitate servizi di connessione alle reti telefoniche e telematiche, anche se gratuiti, ma ciò non esclude che l'identificazione avvenga contestualmente a quella richiesta a norma dell'art. 109 del T.U. delle leggi di P.S.*" (Quest'ultima normativa è quella che impone l'obbligatorietà di identificazione ai fini di pubblica sicurezza dei clienti delle strutture ricettive). Inoltre, come si detto precedentemente, l'identificazione e la registrazione dei log è obbligatoria qualora si offrano servizi di connettivit wireless.
Pertanto dovranno adeguarsi a questa normativa tutti coloro che offrono connettivit pubblica ad Internet via Wi-Fi o che mettano a disposizione terminali o totem. Inoltre, secondo me, consigliabile che anche chi offre questi servizi senza mettere terminali a disposizione si adegui alla normativa. Chiaramente si sta parlando di accesso pubblico, quindi Internet Point, alberghi, biblioteche, università ecc

Privacy e legge 155/05

L'adeguamento alle misure richieste dalla legge anti terrorismo implica che il gestore di Internet Point / locale pubblico che acquisisce i dati dell'utente che utilizza il servizio e registrandone i log, ricade pienamente nella definizione di "titolare" di un trattamento di dati personali ai sensi della Legge sulla Tutela dei Dati Personali (DLgs 196/03) ed è tenuto, pertanto, a rispettare le norme sull'informativa, il consenso, la conservazione e la sicurezza dei dati.

a. Informativa
E' necessario fornire al cliente l'informativa che contenga le indicazioni previste dall'art. 13 del DLgs 196/03.

b. Consenso
In questo caso il consenso non è necessario, dal momento che il trattamento è previsto da norme di legge. Il rifiuto dell'interessato a conferire i propri dati obbliga il titolare a non concedere il servizio.

c. Notificazione
Come si evince dall'art. 37 del DLgs 196/03, il trattamento svolto da un fornitore di servizi di telecomunicazioni non rientra tra quelli che devono essere notificati al Garante.

d. Misure di sicurezza
Si consiglia di applicare gli art. 33 e 34 DLgs 196/03, inclusa la redazione del documento programmatico sulla sicurezza, poiché dai log del traffico potrebbero emergere dati sensibili ovvero idonei a rivelare idee politiche, religiose, tendenze sessuali ecc.

Soluzioni

Per ottemperare a questa disposizione occorre inserire un server di autenticazione e quindi prevedere dei meccanismi di autenticazione, come ad esempio un server RADIUS. La società svedese Clavister offre Security Gateway che includono strumenti di auditing, reportistica e monitoraggio che permettono la tracciabilità degli accessi alla rete. Tutti i Gateway Clavister offrono supporto Radius server ed Active Directory per l'autenticazione degli utenti. Laddove fosse troppo onerosa l'implementazione di un server Radius, vi è la possibilità di utilizzare il database locale degli apparati, che

in grado di gestire sino a 500 utenti. La società ha realizzato inoltre un plug-in con interfaccia web denominato Hot-Spot Manager (**Figura 2**) per consentire la gestione di ambienti di connettività che offrono accessi ad Internet in luoghi o locali pubblici, come Hot-Spot (wireless) o Internet Point (wired), nonchè la gestione delle utenze che vi accedono.
Un altro prodotto interessante è la piattaforma della Advanced ISP Billing: in questo caso si tratta di un server Radius avanzato che permette non solo l'identificazione degli utenti, ma anche la gestione della loro tariffazione (**Figura 3**). Questo prodotto permette la gestione di ambienti wireless (Hot-Spot) e prevede inoltre una interessante suite per la gestione e tariffazione del VOIP.
La piattaforma integrata con i Security Gateway di Clavister e supporta inoltre Quintum, Cisco, Huawei, Lucent, Nortel e MERA. Il prodotto gira su sistemi operativi Microsoft, Unix, Linux e Solaris. Sul loro sito è riportata la documentazione completa ed è possibile scaricare la demo del prodotto.

Conclusioni

Gestori ed utenti protestano, trovando il provvedimento eccessivo. I gestori di Internet Point e locali pubblici fanno notare che saranno prodotte decine di migliaia di copie di carte di identità e passaporti, e nessuno ne garantirà la sicurezza.
Inoltre si dovranno archiviare sino al 31/12/2007 tonnellate di informazioni. Molte grosse catene si sono organizzate ed ha avuto vita facile chi si era già attrezzato per profilare i clienti.
È evidente comunque che queste misure potrebbero essere particolarmente onerose per le piccole realtà.

Bibliografia e riferimenti

[1] Advanced ISP Billing www.advancedispbilling.com
[2] Clavister AB www.clavister.it
[3] Ministero degli Interni www.interno.it

Note Biografiche

Nicola Sotira si occupa di progettazione e sicurezza delle reti presso la società Exwai. Membro della *Association for Computing Machinery* lavora da diversi anni nel settore della sicurezza informatica, con particolare attenzione alle problematiche di sicurezza perimetrale, VPN e controlli di accesso basati su biometria e smartcard. Recentemente si sta occupando di sicurezza su reti wireless e WiMAX.