RELAZIONE AVVOCATO STFANO ATERNO

SALA CONGRESSI
HOTEL SOLARA

OTRANTO 8 E 9 OTTOBRE 2004

CONVEGNO NAZIONALE

"FIRME ELETTRONICHE E DIGITALI PER IL COMMERCIO ELETTRONICO E L'E–GOVERNEMENT. L'IMPRESA, LA PUBBLICA AMMINISTRAZIONE E IL PROFESSIONISTA TRA FALSI INFORMATICI ED ESIGENZE DI CERTEZZA"

@

"DATI ESTERNI, ESIGENZE INVESTIGATIVE E TUTELA DEI DATI PERSONALI"

Mi unisco ai ringraziamenti per la gentile ospitalità ed in particolare ringrazio i colleghi Andrea Lisi e Daniele Minotti che mi hanno invitato.
Tempi duri per il *right to be alone* noto come "diritto ad essere lasciati soli" tanto caro fin dal 1890 a BRANDEIS e WARREN, e tempi duri anche per il diritto alla riservatezza dei dati personali che discende direttamente dal primo. Le aspettative nate dal Dlgs 196/2003 erano certamente diverse soprattutto per quanto riguarda gli aspetti legati alla conservazione dei dati sia del traffico telefonico sia del traffico internet.
La prima stesura dell'art. 132 del decreto legislativo 30 giugno 2003, così come pubblicato in Gazzetta ufficiale il 29 luglio dello stesso anno, indicava sinteticamente che i dati relativi al traffico telefonico dovevano essere conservati dal fornitore per trenta mesi per finalità di accertamento e repressione dei reati fermo restando quanto previsto dall'art. 123 comma 2 della stessa normativa per il trattamento dei dati ai fini della fatturazione.
Apparve subito evidente che tale norma mal si conciliava con le esigenze dettate dal periodo critico che il paese attraversava nella lotta al terrorismo interno ed internazionale per non parlare delle repressione di reati come la pedo-pornografia su Internet ed i reati informatici.
Pochi mesi dopo ed esattamente con decreto legge del 24 dicembre 2003 n. 354, il Legislatore è corso ai ripari modificando l'art. 132 al comma 1 con l'eliminazione della parola "telefonico" comprendendo quindi anche i dati di traffico internet, e aggiungendo il comma 2 che aumenta di altri trenta mesi il periodo di conservazione seppur entro i limiti dei delitti di cui all'art. 407 comma 2 lett. a) e dei delitti in danno di sistemi informatici o telematici. Il tutto subordinando però l'acquisizione degli ulteriori trenta mesi di traffico ad una richiesta che il Pubblico Ministero ed il difensore devono fare al Giudice al quale spetta l'autorizzazione o meno con decreto motivato all'acquisizione dei dati.
Nel caso del difensore, il Giudice, una volta decisa l'acquisizione procede anche d'ufficio.
La modifica pone qualche problema ma gli organi investigativi sono per lo più soddisfatti ed i risultati di molte indagini non subiscono danni. Il problema si verifica in sede di conversione in legge in quanto vengono apposte modifiche sostanziali (vedi G.U.

n. 45 del 27.2.04) concernenti la re-introduzione della parola "telefonico" relativamente al traffico da conservare ed una riduzione del periodo da 30 mesi a 24 mesi sia al comma 1 sia al comma 2 dell'art. 132.
In relazione ad un una possibile conservazione dei dati di traffico Internet per finalità di fatturazione richiamata dall'art. 123 comma 2 al quale lo stesso art. 132 fa riferimento, appare importante sottolineare che ormai è molto frequente il ricorso a contratti di abbonamento ad Internet gratuiti o comunque con servizi "flat" su linea dedicata che non sembrano rientrare nel disposto dell'art. 123 comma 2 e quindi non rilevare ai sensi dell'art. 132 in quanto il corrispettivo non è in rapporto alla durata della connessione o al volume dei dati trasmessi. Illustrare qui le altre tipologie di servizi e di connessione alla rete rapportate alla fatturazione ci porterebbe lontano, pertanto, a tutto voler considerare, comunque il termine di conservazione previsto per la fatturazione appare di soli 6 mesi e non obbliga i gestori e gli ISP (internet service provider) alla conservazione dei dati di traffico internet oltre tale termine.
Chiaramente tale modifica finisce per scontentare tutti ed ha sollevato la protesta della Procure della Repubblica impegnate in indagini delicate contro il terrorismo e la criminalità organizzata.
In un immaginario scontro tra queste ultime ed il Garante dei dati personali quest'ultimo sembra però aver vinto ai punti. D'altronde negli ultimi tempi l'individuo è sempre più sottoposto a controlli e monitoraggi di ogni tipo i quali non sempre sono motivati da esigenze di sicurezza anzi spesso tradiscono motivazioni commerciali.
Le modifiche apportate in sede di conversione non soddisfano coloro che ritengono prioritarie le esigenze di sicurezza nazionale e di tutela dalle minacce del terrorismo e di lotta alla criminalità. E' la stagione delle grandi indagini contro i terroristi delle Brigate Rosse per gli omicidi D'antona e Biagi caratterizzate da numerose ed importanti indagini informatiche, telematiche e telefoniche, è il periodo della nascita del CNAIPIC ovvero del Centro Anticrimine Informatico per Infrastrutture Critiche presso i Centri specializzati della Polizia di Stato e delle Telecomunicazioni, è il momento in cui vengono resi esecutivi i progetti relativi alla messa in orbita di satelliti italiani militari e commerciali. E' un periodo in cui l'esigenza di sentirsi sicuri è molto diffusa.
Assistiamo ad una sorta di "tiro alla fune", da una parte continue spinte verso una migliore e completa tutela della sfera di riservatezza dell'individuo che finisce per impedire la conservazione dei dati di traffico telefonico oltre i limiti di tempo stabiliti dalla norma e dall'altra parte continue richieste di ampliamento dei poteri nella formazione di banche dati per esigenze di sicurezza e di ordine pubblico.
Allo stato, la disposizione prevista all'art. 132 dlgs. 196/2003 non soddisfa le esigenze sopra richiamate e vedrete che ben presto si tornerà a parlare di questa norma nel momento in cui, a livello europeo, si darà attuazione al progetto discusso al vertice dei ministri dell'Interno dell'Unione Europea il 25 marzo 2004 scorso a Bruxelles e che prevede la realizzazione urgente di banche dati (passaporti rubati, impronte digitali degli inquisiti per terrorismo, dati dei passeggeri aerei) e la conservazione dei dati di traffico telefonico e del traffico via Internet al fine di contrasto del terrorismo.
Problemi seri si pongono anche per i difensori degli imputati (anche se attenzione deve essere posta da avvocati impegnati in ogni settore e non solo in quello penale) chiamati

nelle ipotesi di delitti informatici o commessi a mezzo di sistemi informatici ad indagini difensive che comportano conoscenze tecniche che troppo spesso mancano.
Sono per lo più avvocati poco preparati dal punto di vista tecnico –informatico che non conoscono le modalità di acquisizione della prova informatica ed i principi posti a fondamento dell'informatica forense (in inglese:computer forensics).
Tali lacune comportano spesso errori nelle strategie processuali e durante le fasi delle indagini preliminari e dell'acquisizione degli elementi di prova, errori che potrebbero essere evitati con una conoscenza più approfondita e con una preparazione seria e attenta in questa materia insieme ad una maggiore umiltà nel ricorrere al consulente tecnico di parte.
Vista la diatriba tra i sostenitori della necessità di maggiore controllo e di maggiore sicurezza all'interno della rete e coloro che spingono invece verso uno spazio libero da vincoli, controlli ed imposizioni, sorge spontanea la domanda : da quale parte stare ?
Entrambi gli interessi sono così importanti che non si può propendere per l'una o per l'altra ipotesi in senso assoluto.
E' invece necessario ed importante portare l'attenzione sul piano della punibilità degli abusi. La ricerca di un giusto contemperamento degli opposti interessi e delle diverse esigenze passa per un forte rispetto delle regole, controlli su eventuali abusi, sanzioni certe e veloci.
Controlli e sanzioni quindi su chi commette abusi nella conservazione e nel trattamento dei dati per finalità di sicurezza e di indagine e su coloro che detengono questi dati oltre il limite consentito dalle norme. Forse solo così potremo garantire ancora l'esistenza di una disciplina che tuteli la riservatezza dei dati personali in tutti gli altri casi.
Il timore di un Pubblico Ministero che può acquisire i dati o di un ISP piuttosto che di un gestore di telefonia che conservano i dati per lungo tempo, non hanno motivo di esistere se ci sono effettivi controlli e sanzioni severe che puniscono gli eventuali abusi.
Il timore concreto e giustificato di coloro che sostengono come oggi si stia sempre più attaccando la tranquillità dell'individuo e violando il suo diritto ad essere lasciato solo (direi anche …in pace) è dettato dalla consapevolezza di una sostanziale incapacità di perseguire eventuali abusi.
E' qui invece che, a mio modesto parere, bisogna puntare per cercare un equilibrio. Aumentare gli sforzi per rendere certa la punizione di abusi e dall'altra parte consentire che per certe esigenze di primaria importanza vengano trattati e conservati i dati aumentando i limiti oggi previsti.
La limitazione della normativa penale in tema di illecito trattamento dei dati con l'inserimento del nocumento come condizione obiettiva di punibilità (o secondo altri come elemento costitutivo del reato) che limita rispetto al passato il ricorso alla fattispecie penale in materia di trattamento illecito non giova alla ricerca di una soluzione. Se mancano gli strumenti di tutela o sono carenti di effettività, certezza e chiarezza difficilmente la norma viene osservata ed è più facile riscontrare violazioni.
Purtroppo negli ultimi anni è stato chiaro a tutti che la strada verso la tranquillità dell'individuo ed una sua tutela all'interno della propria sfera di intimità si sta interrompendo bruscamente per fare spazio ad una esigenza (a volte esagerata) di sicurezza e di controlli invasivi della persona.

E’ forse una conclusione amara ma non sembra molto distante dalla realtà, ritenere che oggi il diritto ad essere lasciati soli è un lusso che non possiamo permetterci.