2080353_NUOPRO.book Page 153 Wednesday, June 18, 2008 12:48 PM

CONSERVAZIONE DEI DATI INFORMATICI E PROSPETTIVE EUROPEE (1)

DI

STEFANO ATERNO

DOCENTE DI INFORMATICA FORENSE E CRIMINOLOGIA INFORMATICA – UNIVERSITÀ DEGLI STUDI DI ROMA – LA SAPIENZA

Il *data retention*, assume oggi un'importanza rilevante in tema di investigazioni e riservatezza della persona.

La conservazione dei dati di traffico è importante sotto molti profili: è importante per gli investigatori, è importante per la difesa, è importante per il cittadino che con la conservazione *sine die* dei dati teme l'affievolimento del diritto alla riservatezza della sua sfera privata.

La disciplina che riguarda il *data retention*, e tutti gli aspetti relativi alla conservazione, è di recente applicazione. Sono ormai alcuni anni che si discute a livello nazionale e a livello europeo sull'importanza, ai fini di indagine, dei dati di traffico telefonico e telematico e sulle implicazioni rispetto alla privacy degli individui.

Ad oggi, 25 gennaio 2008, tra Italia ed Europa la partita del *data retention* non è ancora giunta al termine.

Le norme di riferimento in vigore nell'ordinamento italiano sono sostanzialmente: l'articolo 132 del codice privacy e le norme del cd decreto Pisanu, dl 144/2005 convertito in legge nell'agosto del 2005 (l. 155/2005).

A livello europeo è da sottolineare la presenza della direttiva europea 2006/24/CE del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (pubblicata

(1) Testo rivisto dall'autore ed aggiornato – nelle note – agli interventi normativi in materia immediatamente successivi al Convegno (febbraio-marzo – aprile 2008).

2080353_NUOPRO.book Page 154 Wednesday, June 18, 2008 12:48 PM

sulla GUCE n. L105 del 13 aprile 2006). Questa direttiva che riduce di molto il tempo massimo di conservazione è stata introdotta in Italia con la legge comunitaria n. 13 del 6 febbraio 2007 (ossia la legge comunitaria 2006) e il nostro Paese avrebbe dovuto recepirla entro il 15 settembre 2007. Mentre si scrive, non è stata ancora recepita, anche se lo schema di decreto legislativo è stato già deliberato dal Consiglio dei Ministri ed ha ottenuto il parere del Garante Privacy e delle competenti Commissioni della Camera e del Senato della Repubblica. Si attende nei prossimi giorni la deliberazione definitiva e l'emanazione del Presidente della Repubblica.

Ma, in attesa del recepimento della normativa comunitaria, in Italia, per quanto tempo quindi si conservano i dati?

Da diversi anni l'Italia si è dotata di una normativa in materia di conservazione dei dati di traffico (telefonico e telematico) per accertamento e repressione di taluni reati. Stiamo parlando dell'art. 132 del codice privacy che prevede, almeno per il momento e per alcuni reati, un periodo di tempo massimo di 4 anni per i dati telefonici e di 1 anno per i dati telematici.

L'articolo 132 del TU privacy è stato introdotto nel codice privacy del giugno del 2003 ed è entrato in vigore il 1 gennaio 2004 (Dlgs n. 196/2003) sostanzialmente modificato rispetto al testo originario a causa di delicate esigenze investigative nazionali che hanno imposto un'ampliamento dei tempi di conservazione dei dati anziché una loro cancellazione come orginariamente il Legislatore era intenzionato a fare (2).

Lo Stato italiano era impegnato in indagini contro il terrorismo delle Brigate Rosse che avevano ucciso a Roma il prof. Massimo D'antona, e continuava ad essere impegnato, come sempre, contro la criminalità mafiosa.

L'Italia fu uno dei primi stati europei a dotarsi di una normativa così rigorosa in materia di conservazione di dati di traffico cd «esterni» (escluso il contenuto delle comunicazioni). Nonostante vi fossero già alcuni principi indicati nella direttiva 2002/58/CE, l'ampliamento dei termini di conservazione sembrava del tutto necessario visto che l'Italia era ed è ancora, purtroppo, l'unico paese

(2) In relazione a queste modifiche e comunque in termini critici, si veda SAVIOTTI, SALVI, «Tabulati telefonici e traffico via internet · norme coerenti per la lotta al terrorismo», in *Guida al Diritto*, n. 14 del 10 aprile 2004, p. 11.

2080353_NUOPRO.book Page 155 Wednesday, June 18, 2008 12:48 PM

europeo a dover fare i conti con il fenomeno della criminalità organizzata di tipo mafioso e proprio in quegli anni con la recrudescenza del terrorismo politico.

Nel 2005, a cavallo tra luglio e agosto, la presenza sul territorio italiano di un terrorista fuggito dopo gli attentati di Londra ha portato lo Stato italiano ad introdurre un decreto legge (dl n. 144/2005, il cd decreto Pisanu) che ha sospeso i diritti di cancellazione di tutti i dati fino al 31.12.2007 e introdotto, solo per motivi antiterrorismo, la possibilità di acquisizione da parte della Magistratura dei dati di traffico oltre i termini previsti dall'art. 132 ovvero oltre i 48 mesi per i telefonici e 12 mesi per i telematici.

Il termine di conservazione dei dati è infatti cosi ripartito e strutturato : i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore per ventiquattro mesi, per finalità di accertamento e repressione di reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi.

Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore per ulteriori ventiquattro mesi e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per ulteriori sei mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

Entro il termine di cui al comma 1 (24 mesi), i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391*quater* del codice di procedura penale.

Dopo la scadenza del termine indicato al comma 1 (24 mesi), il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo

2080353_NUOPRO.book Page 156 Wednesday, June 18, 2008 12:48 PM

407, comma 2, lettera a), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

Nei casi di urgenza, quando vi e' fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che e' comunicato immediatamente e comunque non oltre ventiquattro ore al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.

Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti anche a prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione agli accessi, disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1, individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento e indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.

Il cd decreto Pisanu (legge n. 155 del 2005, dl 144/2005) che appunto ha modificato l'art. 132, ha anche aggiunto, all'art. 6, che fino al 31 dicembre 2007 e' sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonche', qualora disponibili, dei servizi, debbono essere conservati fino a quella data dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto-legge, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.

2080353_NUOPRO.book Page 157 Wednesday, June 18, 2008 12:48 PM

In sintesi, si sottolinea quindi che per le finalità del cd decreto Pisanu i dati telefonici e telematici devono essere conservati fino al 31 dicembre 2007. Nei casi non previsti dal decreto possono essere messi a disposizione dell' Autorità Giudiziaria solo i dati acquisiti entro il termine previsto dal comma 1 e 2 dell'art. 132 codice privacy.

Pertanto, se la conservazione dei dati di traffico è 24 mesi più 24 mesi (telefonico) e 6 mesi più 6 mesi (telematico), è evidente che oggi in Italia abbiamo un periodo di conservazione ben al di sopra degli *standard* europei richiesti dalle direttive degli anni passati e in ultimo dalla direttiva 2006/24/CE del 15 marzo 2006 recepita con legge comunitaria nel febbraio del 2007 (l. n. 36 del febbraio 2007).

Questo lungo periodo di conservazione ha sempre preoccupato l'Autority per la privacy che fin dal 2005 (in realtà fin dal giugno del 2003 con il Dlgs 196/2003) ha cercato di contenere le istanze degli inquirenti e delle forze di polizia volte ad ampliare i termini di conservazione. Ultimamente, la proroga dei termini del Pisanu ha fatto attivare nuovamente e in modo deciso il Garante della Privacy italiano, il quale, in una recente intervista, rilasciata agli organi di stampa e finita anche sul web, ha sottolineato come in Italia la situazione stava superando i limiti in quanto, di fatto, si stavano conservando i dati telefonici per un periodo di quasi 8 anni e per un periodo di quasi 5 anni per i telematici (3).

Al di là delle perplessità suscitate dall'intervista, il calcolo fatto dal Garante appare un calcolo possibile soltanto facendo le considerazioni che seguono.

Se la norma dell'art. 132 codice privacy è stata modificata nell'agosto del 2005 e da quel giorno si è fissato obbligatoriamente un termine di conservazione di 24 + 24 è evidente che da quel giorno i gestori non hanno potuto cancellare i dati che conservavano fin dal 2001. Cosi per i dati telematici rispetto al termine massimo del 2004. Quindi il calcolo del Garante si basa su tali date : agosto 2001 e agosto 2004 e quindi, ad oggi, 7 anni e mezzo per i telefonici e 4 e mezzo per i telematici.

(3) Si veda l'intervista del Garante e ai fini del calcolo si tenga presente il termine massimo di conservazione presupponendo anche che alla data del luglio del 2005 i gestori conservavano ancora (fatturazione?) i dati del 2001 e che pertanto oggi ancora non sono stati cancellati.

2080353_NUOPRO.book Page 158 Wednesday, June 18, 2008 12:48 PM

Ciò è vero però se diamo per scontato ciò che scontato forse non è per tutti ovvero che dati di traffico in possesso a tutti i gestori effettivamente sin dal 2005 risalivano ed erano conservati nelle loro banche dati sin dal 2001.

Ciò detto e considerata anche una certa flessibilità di calcolo, è comunque palese che in Italia si stanno superando i limiti che la direttiva 2006/24/CE ha imposto a tutti gli Stati membri.

In Italia però la situazione investigativa, della sicurezza e dell'ordine pubblico inteso come lotta alla criminalità mafiosa non sembra consentire una rinuncia al termine di conservazione massimo ovvero fino al 31 dicembre 2007 per tutti i dati ed infatti con il decreto legge chiamato anche «mille proroghe» del 28 dicembre 2007 (4), il Governo italiano sposta al 31 dicembre 2008 il termine dei gestori per la cancellazione dei dati di traffico (5).

Siamo nei primi giorni di gennaio 2008, la direttiva europea 2006/24/CE non sembra costituire una preoccupazione, non è stata recepita nè sembra all'ordine del giorno dell'esecutivo, il quale, nel frattempo incontra alcuni problemi di ordine politico ed è costretto a dimettersi. La proroga del «decreto pisanu» (nel decreto legge cd mille proroghe) sembra salva in quanto si ritiene verrà certamente (vedremo poi invece erroneamente) convertita in legge.

In realtà la proroga dei termini di conservazione ha riacceso gli animi e le proteste di quanti ritengono che allo stato attuale in Italia siano in pericolo le libertà fondamentali dell'individuo. E' molto frequente il dibattito sulla portata applicativa delle norme sulla privacy dei consumatori e degli utenti dei gestori telefonici e telematici, complice anche un clima da grande fratello introdotto a causa delle recenti e note indagini contro importanti manager di una nota società per azioni del comparto telefonico.

(4) Tipico decreto legge di fine anno con il quale vengono prorogati tutti i decreti in scadenza.

(5) Nel decreto milleproroghe, dl 31 dicembre 2007, n. 248, viene prorogata la scadenza del termine di conservazione per motivi antiterrorismo e antimafia fino al 31 dicembre 2008 con proroga delle sospensioni circa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi, *nonche', qualora disponibili*, dei servizi, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del decreto-legge, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.

2080353_NUOPRO.book Page 159 Wednesday, June 18, 2008 12:48 PM

Il Garante della privacy italiano, è molto attivo nel periodo tra il dicembre e la fine di febbraio e forte anche di una consultazione pubblica terminata il 31 ottobre 2008, proprio nei giorni che seguono l'intervista, si pronuncia sulla tipologia dei dati di traffico e sulle garanzie da fornire all'interessato (6) ed emana alcuni provvedimenti *ad hoc* verso alcuni gestori di telefonia mobile che conservano dati di traffico comprensivi del cd *Internet protocol destination* in relazione alle connessioni internet.

Il Garante in questi provvedimenti, del tutto legittimi e motivati, di fatto svolge anche una funzione interpretativa che va un po' al di là delle sue prerogative.

Egli in relazione ad alcune definizioni, tra le quali anche quella di *Internet protocol di destinazione* (7), anticipa interpretativamenete concetti che saranno oggetto di modifiche del codice privacy ai sensi della direttiva e nel fare ciò, impone di fatto fin da subito ai gestori destinatari dei provvedimenti e incidentalmente anche a tutti gli addetti del settore, la cancellazione di alcuni dati perché detenuti in contrasto con le su richiamate definizioni essendo essi stessi ritenuti dal Garante «contenuto di comunicazioni».

Ciò purtroppo è vero in parte in quanto in molti casi, non distinti né analizzati con precisione dal Garante stesso, i dati conservati pur essendo *IP destination* non individuano alcun contenuto di comunicazione (8).

---

(6) Provvedimento del Garante privacy, a carattere generale del 17 gennaio 2008, «Sicurezza dei dati di traffico telefonico e telematico», con il quale, si rivolge ai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, ma oltre ad affrontare il problema della sicurezza dei dati ed l'aumento del livello fino alla *strong authentication*, esplicitamente, il Garante rileva incidentalmente *che i dati di traffico relativi alla comunicazione (come, ad esempio, la c.d. «navigazione web» e le pagine visitate di un sito Internet) spesso identificano o rivelano nella sostanza anche il suo contenuto e pertanto l'eventuale conservazione di tali dati si porrebbe, in violazione di quanto disposto dall'art. 132 del Codice (come modificato dal citato d.l. n. 144/2005), laddove esclude dalla conservazione per finalità di giustizia i «contenuti» della comunicazione (cfr., in tal senso, anche l'art. 1, comma 2, della direttiva 2006/24/Ce, nella parte in cui esclude dal proprio ambito di applicazione la conservazione del «contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche»*.

(7) Da non confondere con l'IP address (ovvero identificativo del nominativo dell'Utente connesso).

(8) E' il noto problema delle reti nattate ovvero il problema che molto chiaramente è stato oggetto di una nota di ASSTEL del 10 marzo 2008 : riguardante gli adempimenti richiesti ai fornitori concernenti l'assegnazione «univoca» dell'indirizzo di protocollo internet (IP Address) ad una comunicazione elettronica.

Con il decreto proposto dal legislatore (schema di decreto) che recepisce *«la Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura dei servizi di comunicazione elettronica accessibili*

2080353_NUOPRO.book Page 160 Wednesday, June 18, 2008 12:48 PM

Nel frattempo, siamo alla metà di gennaio 2008, in commissione parlamentare, in occasione della conversione in legge del decreto milleproroghe, il relatore (9) di maggioranza inserisce una modifica al testo del decreto legge modificando sostanzialmente la proroga e vincolandola all'imminente recepimento della direttiva europea (10).

La modifica sostanzialmente stabilisce il termine massimo di conservazione dei dati e quindi oltre i limiti previsti dal 132 codice privacy (oltre i 24 mesi più 24) fino al recepimento della direttiva 2006/24/CE e comunque non oltre il 31 dicembre 2008.

Se la direttiva, come sembra, verrà recepita entro il 31.12.2008 i dati conservati oltre i 2 anni dovranno essere cancellati con buona pace della lotta al terrorismo, alla pedopornografia ma soprattutto alla criminalità mafiosa.

Nel frattempo lo schema di decreto legislativo che dovrebbe recepire la direttiva viene deliberato in via preliminare dal Governo proprio con uno dei suoi ultimi atti urgenti prima dell'inzio della campagna elettorale per le elezioni politiche anticipate (11).

---

al pubblico o di reti pubbliche di comunicazione» si richiede ai fornitori del servizio di accesso ad internet di **assegnare a ciascuna comunicazione telematica un indirizzo IP univoco** (cfr. art. 3 comma 2.1) che consenta l'identificazione univoca dell'utente o abbonato (cfr. art. 5 comma 2).

La formulazione attuale della normativa, imponendo al fornitore l'assegnazione univoca, per ciascun utente, di un indirizzo IP pubblico, introduce delle criticità difficilmente risolvibili allo stato:

a) Ogni fornitore si dovrebbe dotare di un numero di indirizzi IP elevato, stimabile, per difetto, ad una intera classe A (che consente per chi ne è proprietario di possedere 2^24 indirizzi IP pubblici differenti). Con l'attuale versione del protocollo internet IPv4, il piano di indirizzamento disponibile (2^32 indirizzi univoci per tutto il mondo internet) non è certamente compatibile con tale scenario; ad avvalorare questa tesi si fa presente che:

– l'IPv4, proprio per la **limitazione del piano di indirizzi supportabile**, sarà in futuro sostituito con la nuova versione IPv6 che costruisce gli indirizzi con 128 bit anziché 32;

– per risolvere la limitazione del protocollo IPv4, ed evadere le continue richieste di accessi ad internet, sono state adottate tecniche di NAT/PAT (Network & Port Address Traslation) volte a risparmiare prefissi di rete, ovviando alla scarsità di indirizzi IP pubblici allocati per ogni paese.

b) Le tecniche utilizzate per razionalizzare l'utilizzo degli indirizzi IP pubblici (ovvero il NAT/PAT) rendono i sistemi informatici e telematici non direttamente raggiungibili da internet, accrescendo il livello di sicurezza delle reti in termini di integrità.

In virtù di quanto sopra, ASTEL suggerisce di integrare la definizione di «*Indirizzo di protocollo internet (IP) univocamente assegnato*» (art. 1 comma 1.g – Definizioni) come segue: Indirizzo di protocollo (IP), abbinato ad altri aspetti tecnici qualificanti la connessione (data, ora della connessione, porta sorgente pubblica), che consentono l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica.

(9) *http://www.camera.it*.

(10) Sul punto, inseguito ad una attenta ricerca e lettura dei lavori parlamentari, iniziati intorno al 10 gennaio e che hanno portato poi all'approvazione il 30 marzo 2008 della legge di conversione del decreto legge milleproroghe, non si nota alcuna discussione parlamentare sul punto *http://www.camera.it*.

(11) Mentre si completa questa relazione per il convegno la materia del data retention è di estrema attualità ed in continuo cambiamento e.

2080353_NUOPRO.book Page 161 Wednesday, June 18, 2008 12:48 PM

Sembra che la volontà legislativa sia in contrasto con quella degli organi inquirenti e qualche settimanale ipotizza conflitti tra organi istituzionali (12).

Soprattutto però sembra che alcune norme (13), sulle quali il Garante privacy non si è espresso negativamente, rendano applicabile un regime sui dati ancor più severo, rigido e liberticida di quanto non faccia lo stesso decreto Pisanu o l'attuale articolo 132 ai commi 2, 3 e 4.

Nel caso del comma *4ter* del 132 codice privacy (di prossima emanazione (14)) si nega addirittura alla difesa (comma 3) la possibilità di avere accesso ai dati telematici per i quali una forza di polizia ha ordinato il «congelamento» (solo per i telematici); a tal proposito non si consente neanche un vaglio del giudice (ma solo del Pubblico Ministero del luogo dell'esecuzione) in tema di convalida di tale ordine a fronte di richieste di forze di polizia straniere e in presenza

(12) Si veda il settimanale L'Espresso, del 17 aprile 2008, pag. 21

(13) Si veda per esempio anche il comma 4 ter dell'articolo 132 del codice privacy che sta per essere recepito nella legge di ratifica della Convenzione di Budapest 2001 sul Cybercrime : Art. 10, (*Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196*).

1. Dopo il comma *4bis* dell'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sono inseriti i seguenti :

«*4ter*. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma *4ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.

4quinquies. I provvedimenti adottati ai sensi del comma *4ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

(14) Mentre di scrive, si segnala che è entrato in vigore il 5 aprile del 2008, con al legge n. 48.

2080353_NUOPRO.book Page 162 Wednesday, June 18, 2008 12:48 PM

di indagini preventive (rectius : intercettazioni preventive) che per loro natura sono particolarmente invasive.

E' chiaro che si tratta di una normativa in controtendenza, caratterizzata addirittura da alcune note di schizofrenia legislativa, rispetto invece alla sempre decantata tutela della riservatezza e dei diritti fondamentali dell'individuo.

Controtendenza che si nota anche in alcune sanzioni particolarmente pesanti (si potrebbero definire «punitive») stabilite normativamente a carico dei gestori telefonici e telematici che non dovessero ottemperare ai numerosi obblighi imposti dalle recenti leggi.

In linea di principio generale *nulla questio* rispetto ad un criterio generale di applicazione a tutti del principio di responsabilità. Ma appunto un criterio che dovrebbe applicarsi a tutti.

Sembra piuttosto avere la meglio una certa schizofrenia legislativa perché poi, in concreto e in applicazione della normativa dell'art. 167 del codice privacy, non tutti rispondono così gravemente in caso di trattamento illecito dei dati personali e non si comprende perché la gravità di reati e di sanzioni debba colpire i gestori che mal custodiscono e non chi commette dei reati di trattamento illecito.

Sembra quasi che il problema da risolvere sia prevenire il trattamento illecito perché in caso di violazione scarsi saranno i mezzi e gli strumenti sanzionatori... (è sotto gli occhi di tutti l'inutilità dell'articolo 169 del codice privacy (misure di sicurezza) e dell'art. 167 che lega la punibilità ad un nocumento che deve essere un pregiudizio apprezzabile patrimonialmente.

Queste sono con tutta evidenza norme che di fatto non spaventano nessuno in un paese dove però si ha molta paura del Grande Fratello.

Nulla questio, appunto, se non si trattasse di una legislazione che invece dall'altra parte cancella dati utilissimi alle indagini e alla lotta contro pedofilia e criminalità organizzata.

Questa sembra più che altro confusione e schizofrenia normativa senza alcun tipo di raziocinio.

Il testo previsto nella bozza del decreto prevede il termine di 24 mesi per i dati di traffico telefonico e 12 mesi per la conservazione del traffico telematico.

2080353_NUOPRO.book Page 163 Wednesday, June 18, 2008 12:48 PM

Questo testo ad oggi, mentre si scrive, non è ancora ritornato alla Presidenza del Consiglio e si ritiene che verrà deliberato probabilmente dal prossimo Governo.

Questi provvedimenti normativi turbano le notti di molti inquirenti e di coloro che ritengono in pericolo le indagini antimafia, antipedofilia e antiterrorismo.

Non è un mistero che la criminalità organizzata (anche e soprattutto mafiosa) ha incominciato già da qualche tempo ad utilizzare la telefonia VOIP su telefoni mobili e su Personal computer (telefonata quindi basata su trasmissione di dati di pacchetto e pertanto da considerarsi telematica ma soprattutto criptata per le caratteristiche del prodotto *software*) per non essere intercettabile e per consentire una comunicazione che faccia letteralmente perdere le tracce delle proprie chiamate (15).

Non è solo il problema della conservazione dei dati di traffico telematico che preoccupa gli investigatori. E' infatti ormai noto che i dati telefonici sono serviti in questi anni per trovare riscontri alle dichiarazioni dei cd pentiti di giustizia ovvero collaboranti con l'autorità Giudiziaria. In seguito al pentimento e al racconto di tanti episodi di vita mafiosa, tra i quali anche le telefonate, si andavano a trovare i riscontri in relazione alle telefonate fatte, alle persone chiamate e alle telefonate ricevute.

Non solo, anche le indagini contro il terrorismo politico delle Brigate Rosse hanno utilizzato e messo a frutto le preziose indicazioni rese dai dati di traffico telefonico e, visti i risultati ottenuti, non si può dar torto a coloro che in queste ore si dicono preoccupati dall'entrata in vigore della normativa così come pensata dal Legislatore italiano.

E' evidente che la soluzione mediatrice sembra essere quella dei termini previsti dalla direttiva ma proprio perché sembrano non essere sufficienti a questo punto sono doverose alcune precisazioni.

La direttiva 2006/24 prevede all'art. 6 che «*Gli Stati membri provvedono affinchè le categorie di dati di cui all'art. 5 siano conservate*

(15) La telefonata effettuata con sistema Skype è criptata e non intercettabile, almeno in via di principio generale. Si veda un caso in Italia (processo per il sequestro e l'uccisione dell'imprenditore Roveraro) dove attraverso strumenti di intercettazione telematica si è tentato e in parte riusciti ad intercettare i responsabili.

2080353_NUOPRO.book Page 164 Wednesday, June 18, 2008 12:48 PM

per periodi non inferiori a ***sei mesi*** *e non superiori a* ***due anni*** *dalla data di comunicazione*».

Essendo ricompresi nell'art. 5 anche i dati relativi alla telefonia via internet, avvenendo questo tipo di telefonata attraverso dati di pacchetto (trattasi quindi di dati telematici), vista anche l'importanza e l'utilità assunta recentissimamente da questi dati di telefonia via Internet (16), sarebbe opportuno pensare di aumentare a due anni anche il termine di cancellazione dei dati telematici. Ciò, come si può notare è comunque un termine consentito dalla direttiva e non occorre una specifica autorizzazione in quanto rientra tra le facoltà di ogni Stato membro che all'interno dell'arco di tempo di cui all'art. 6 può oscillare con discrezionalità.

Il punto è che oggi sembra essere tardi per ogni protesta o recriminazione contro l'ondata anti-*data retention* che sembra prevalere sulle esigenze antiterrorismo e lotta alla criminalità. Il Legislatore italiano e del resto anche le forze e le istituzioni che hanno come compito istituzionale quello di tutelare la sicurezza del Paese, non sono riusciti a recepire la direttiva nei termini di cui all'art. 15 della 2006/24/CE (15 settembre 2007). Il recepimento gli avrebbe consentito di avvalersi, se opportunamente richiesto nei termini, della proroga speciale di cui all'art. 12 che avrebbe consentito all'Italia di superare il periodo massimo di conservazione e, seppur per un periodo limitato, di far fronte alle difficili esigenze investigative (17).

A ben vedere l'art. 12 sembra pensato più che altro per momenti di emergenza e per affrontare circostanze particolari che giustificano una proroga; ad esempio ciò potrebbe accadere quando ven-

(16) Si veda, unica indagine sino ad ora, l'utilità avuta dai dati del traffico telefonico via Internet (VOIP) per la soluzione del caso del sequestro Roveraro, in seguito ad indagini particolarmente tecnologiche portate avanti dai carabinieri dei ROS sotto la direzione del Pubblico Ministero di Milano, dott. Nobili.

(17) Art. 12 della direttiva 2006/24/CE : 1. Uno Stato membro che si trovi ad affrontare circostanze particolari che giustificano una proroga, per un periodo limitato, del periodo massimo di conservazione di cui all'articolo 6, può adottare le necessarie misure. Lo Stato membro notifica immediatamente alla Commissione e informa gli altri Stati membri delle misure adottate in virtù del presente articolo, motivandone l'introduzione.

2. Entro sei mesi dalla notifica di cui al paragrafo 1, la Commissione approva o respinge le misure nazionali in questione, dopo aver accertato se costituiscano un mezzo di discriminazione arbitraria o di restrizione occulta degli scambi fra gli Stati membri e se rappresentino un ostacolo al funzionamento del mercato interno. In assenza di decisione da parte della Commissione entro tale periodo, le misure nazionali si considerano approvate.

3. Quando le misure nazionali di uno Stato membro in deroga alle disposizioni della presente direttiva sono approvate conformemente al paragrafo 2, la Commissione può valutare se proporre una modifica della presente direttiva.

2080353_NUOPRO.book Page 165 Wednesday, June 18, 2008 12:48 PM

gono commessi particolari atti di terrorismo o vi è un chiaro attacco alla alle istituzioni democratiche da parte della criminalità mafiosa. In quel momento lo Stato membro trovandosi ad affrontare un momento particolare che giustifica una proroga, può chiederla adottando le necessarie misure. Ma se questo è vero è anche vero che è stato pensato sulla base delle esigenze di tutti gli Stati membri.

La domanda che sorge spontanea è se l'Italia può essere paragonata, nel suo essere malata di criminalità mafiosa, a tutti gli altri membri.

La normativa di cui all'art. 12 può esser sufficiente in ipotesi di attentati terroristici come quelli che purtroppo hanno ucciso tante vite innocenti in Spagna o a Londra, dove le organizzazioni criminali seppur operanti sul territorio non hanno le caratteristiche tipiche della criminalità mafiosa radicatasi negli anni in intere regioni del paese.

L'articolo 12 può essere utile nel bloccare la cancellazione dei dati da quel momento emergenziale in avanti e di dati di cui si disporrà saranno comunque relativi a due anni e 1 giorno perché quelli precedenti saranno stati cancellati dai gestori che rispondono, con sanzioni amministrative pensanti, direttamente al Garante della privacy.

Forse in caso di attentati di questo tipo 2 anni di dati basteranno, ma sicuramente in materia di mafia due anni non bastano. Contro il terrorismo interno delle Brigate Rosse che hanno ucciso Biagi e D'antona sono stati utilizzati (incrocio dei dati di traffico di telefonate intercorse tra alcuni soggetti in un certo spazio geografico nei minuti dell'omicidio) con successo dati di traffico relativi a due anni e mezzo prima. E'evidente a tutti che si utilizzano i dati di traffico quando si riesce a scoprire il numero di telefono delle persone che cerchi... non sempre ciò è immediatamente possibile... e fino al quel momento possono passare anni e anni...

Con l'entrata in vigore della direttiva questi dati non si troveranno più (salvo rare ipotesi di necessità di conservazione per fini di fatturazione ma di regola non presenti nei casi di dati utilizzati dai terroristi o dai mafiosi).

Cosa fare?

Oltre all'applicabilità, nei limiti sopra enunciati, dell'art. 12, se si vuole realmente fare qualcosa per conservare la normativa nazio-

2080353_NUOPRO.book Page 166 Wednesday, June 18, 2008 12:48 PM

nale nella parte in cui prevede termini di conservazione dei dati più lunghi, l'Italia potrebbe adottare la procedura prevista nell'art. 95, par. 4 del TCE. Secondo tale norma: «*allorché, dopo l'adozione da parte del Consiglio o della Commissione di una misura di armonizzazione, uno Stato membro ritenga necessario mantenere disposizioni nazionali giustificate da esigenze importanti di cui all'articolo 30 o relative alla protezione dell'ambiente o dell'ambiente di lavoro, esso notifica tali disposizioni alla Commissione precisando i motivi del mantenimento delle stesse*». A sua volta l'art. 30 del TCE richiama specificatamente i motivi di moralità pubblica, di ordine pubblico, di pubblica sicurezza, di tutela della salute e della vita delle persone e degli animali, di protezione del patrimonio artistico, storico o archeologico nazionale, etc.

E' di tutta evidenza che i delitti di cui agli articoli 416 e 416*bis* cp sono delitti contro l'ordine pubblico.

Gli strumenti sembrano esserci e forse ancora percorribili dal Legislatore italiano al quale spetta, in prima battuta il recepimento della direttiva e poi la ricerca del giusto equilibrio tra privacy e sicurezza del Paese (18).

Oggi, dopo alcuni anni in cui si è cercato di suggerire che il metodo era la ricerca del giusto equilibrio, in un momento, quello attuale nel quale tutti scrivono e dicono di volerlo perseguire, si ha qui la presunzione di suggerire nuovamente che forse si sbagli approccio. Fin qui le forze in campo si sono «scontrate» sul tema del *data retention* cercando ciascuna di far prevalere la propria assoluta volontà.

Il metodo è invece «incontrarsi» e ciò non può non passare per la comprensione delle ragioni dell'altro. Non sembra difficile a parole e pertanto è ancor più deludente il fatto che non vi si riesca.

Ma fino a quando si agirà a livello legislativo «separati» e «contro» invece che «insieme» e «per»... ogni conflitto e scontro istituzionale avrà come unico risultato di mettere in pericolo sia la sicurezza dei

(18) Si consenta di inserire un richiamo ad uno dei primi contributi in materia di equilibrio tra i due opposti interessi, contributo, insieme all'altro nel quale per la prima volta si è parlato di Securacy come punto di equilibrio raggiungibile, in ATERNO, *Profili penali dell'anonimato in rete*, in *A.A.V.V.. Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, 2005, pp. 129 e s., Nyberg edizioni; inoltre si vedano alcuni riferimenti in GNOSIS, *Privacy e sicurezza l'equilibrio è possibile*, n. 1, ottobre-dicembre, Istituto Poligrafico dello Stato, 2004, 136.

2080353_NUOPRO.book Page 167 Wednesday, June 18, 2008 12:48 PM

cittadini del paese sia la sopravvivenza della stessa privacy; un giorno o l'altro essa finirà per soccombere e la bilancia penderà troppo dalla parte di una «emergenza della sicurezza» perché quest'ultima è come il ghiaccio sporco sulle strade... pensi che non ci sia... ma quando ci sei sopra... è già troppo tardi.