

Sicurezza delle informazioni: come difendersi dalle nuove forme di attacco

“Le ultime novità normative in materia di Data Retention”
Il D.Lgs 30/05/2008, (In attesa di pubblicazione)

Roma 11 giugno 2008

Avv. Prof. Stefano Aterno

Università La Sapienza di Roma

www.studioaterno.it



data retention oggi

nella terra di nessuno
tra

diritto, politica e sicurezza



La normativa OGGI in vigore:

- art. 132 del Dlgs 196/2003 (codice privacy)
 - modificato dalla l. 48 del 2008 e dal D.Lgs 30/05/2008, (In attesa di pubblicazione);
- art. 6 decreto Pisanu (L. 155/2005) prorogato dal dl 248/2007
 - abrogazione art. 6 al momento della entrata in vigore del D.Lgs 30/05/2008 (in attesa di pubblicazione)
- Direttiva europea 2006/24/CE :
 - attuata dal D.Lgs 30/05/2008, (In attesa di pubblicazione)
- il *comma 4 ter* al 132 introdotto dalla L. 48 del 5 aprile 2008

OGGI
Con l'art. 6 della L. 155/2005 (cd Pisanu)

I dati si devono conservare:

- art. 132 dlgs 196/2003:

- telefonico 24 + 24 mesi

- telematico 6 mesi + 6 mesi

Art. 6 L. 155/05 per motivi antiterrorismo e criminalità organizzata I
DATI NON SI CANCELLANO dall'estate del 2005
(decreto legge milleproroghe aveva prorogato al 31.12.08):

Telefonici: più di 7anni1/2

Telematici: più di 4 anni e 1/2

Perché conservare i dati per tanto tempo ?

- Indagini(**utilità dati esteriori delle comunicazioni**)
- **Riscontri** dei collaboranti
- Le chiamate senza risposta “sono segnali convenzionali:
(vedi indagini BR su riscontro presenza su luogo delitto)
- Localizzazione geografica(approssimativa)chiamante/ato
- Indagini VOIP:possibile utilizzo dati(sequestro Roveraro)
- Per indagini sulle BR = dopo 2 anni e mezzo dai fatti
importante utilità dei dati

Perché NON bisogna conservare i dati
per tanto tempo ...

Aiuto, qualcuno ci spia !



.....bene...attenzione a non buttare il
bambino con l'acqua sporca...

Con l'attuazione della direttiva avremo un art.132 più o meno così...

- Fermo restando quanto previsto dall'articolo 123, comma 2, 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***
 - *per **dodici mesi***
1. *“1-bis. I dati di cui all'articolo 132-bis relativi alle chiamate senza risposta trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione sono conservati per **trenta giorni**.”.*
- 2. 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.
 - 3. Entro il termine di cui al comma 1, 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.

- 4. Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi 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.
- 4-bis. 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.».
- 4 ter(6).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. (6).

- **4-quater.(6).Il fornitore o l'operatore di servizi informatici o telematici** cui è rivolto l'ordine previsto dal comma **4-ter 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**. (6).
- **4-quinquies.(6).I provvedimenti adottati ai sensi del comma 4-ter 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. (6).

NOTA: problema di competenza del Pubblico Ministero dell'esecuzione:

- **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

- 5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, *volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a:* (5)
- a. prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'Allegato B);

(b.) ABROGATA (5) [disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;]

(c.) ABROGATA (5) [individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al comma 4 e all'articolo 7;]

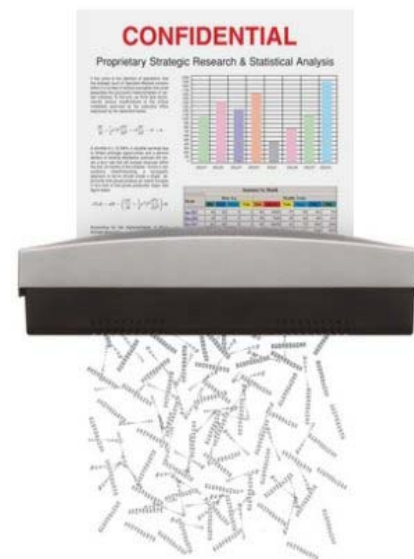
d. indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui *al comma 1* . (5)

abrogazione art. 6 L. 155 dell'agosto 2005

il termine del 31.12.2008
NON C'E' PIU'

***Tra qualche giorno gli operatori
dovranno cancellare i dati
telefonici/telematici eccedenti***

***ogni giorno !!
(ogni 30 gg)***



Per gli Stati europei

Art. 6

direttiva 2006/24

Gli Stati membri provvedono affinché le categorie di dati di cui all'art. 5 siano conservate per periodi non inferiori a **sei mesi** e non superiori ai **due anni** dalla **data di comunicazione**

Alcune anomalie del sistema, delle norme e delle relazioni tra istituzioni

- Il decreto ha introdotto nuove definizioni MA non ha modificato l'art. 4 del codice privacy (definizioni)...
- Mancata attuazione entro i termini direttiva
- Ritenuta deroga (mai esistita...)
- PROROGA del termine ex decreto Pisanu e sua ABROGAZIONE in sordina e in “zona Cesarini” senza discussione tra le parti interessate né discussione parlamentare
- Provvedimenti per alcuni e non per tutti...
- Norme emanate da Parlamento senza una reale discussione/conoscenza parlamentare

IL decreto ha introdotto nuove definizioni MA non ha modificato l'art. 4 del codice privacy (definizioni)...

Art. 2

1. Ai fini del presente decreto si intende :

- a) per "utente": qualsiasi persona fisica o giuridica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, senza esservi necessariamente abbonata;
- b) per "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, **ivi compresi i dati necessari per identificare l'abbonato o l'utente;**
- c) per "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude;
- d) per "traffico telefonico": le chiamate telefoniche, incluse le chiamate vocali, di messaggia vocale, in conferenza **e quelle basate sulla trasmissione dati,** purché fornite da un gestore di telefonia, i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata, la messaggia e i servizi multimediali, inclusi i servizi di messaggia breve, servizi mediali avanzati e servizi multimediali;
- e) per "chiamata senza risposta": la connessione istituita da un servizio telefonico accessibile al pubblico, non seguita da un'effettiva comunicazione, in quanto il destinatario non ha risposto ovvero vi è stato un intervento del gestore della rete;
- f) per "identificativo dell'utente": l'identificativo unico assegnato a una persona al momento dell'abbonamento o dell'iscrizione presso un servizio di accesso Internet o un servizio di comunicazione Internet;
- g) per "**indirizzo di protocollo internet (IP) univocamente assegnato**": indirizzo di protocollo (IP) che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica.

- 2. Ai fini del presente decreto si applicano, altresì, le ulteriori definizioni, non ricomprese nel comma 1, elencate nell'art. 4 del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante il codice in materia di protezione dei dati personali, di seguito denominato "Codice".

Schizofrenia normativa e regolamentare:

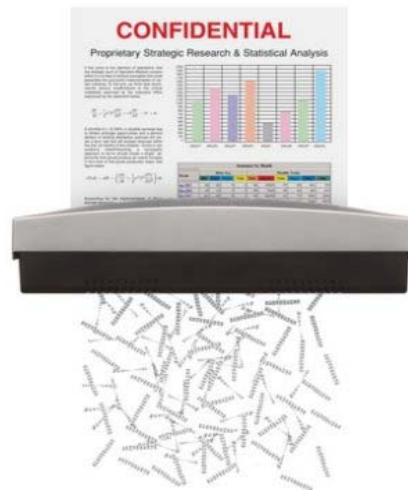
- una certa ignoranza delle norme da parte del Legislatore
- una certa superficialità di molte parti in causa
- una eccessiva contrapposizione tra le diverse posizioni

Con le contrapposizioni tra “integralisti”
non si risolve nulla.....

Occorre trovare un **EQUILIBRIO** tra le diverse posizioni



1) alcune critiche per gli Integralisti della riservatezza assoluta



Contraddizioni emergenti, come i pareri emessi per:

- Comma 4 ter del 132 Codice privacy (inserito dalla L. 48 del 2008)
- L'art. 167 codice privacy è scritto male (il problema del documento)
- Sparisce il vaglio del Giudice ex art. 132 codice privacy

Seguono critiche e contraddizioni....

-provvedimento del Garante sui dettagli chiamate
effettuate sulle bollette
(marzo 2008)
(a richiesta ..tutti in chiaro - nessun omissis)

*Ci vuole un genio per capire che così l'intestatario dell'utenza
controllerà*

il coniuge/compagna o i figli maggiorenni ?

*...nelle case degli italiani
nasce il "piccolo fratello" !!!*

Segue bollette in chiaro...

Qualcuno sostiene..... l'intestatario
dell'utenza deve "avvertire" i componenti
della famiglia

avvertire ???

Stai a vedere che se vuole verificare se la
moglie ha l'amantel'avverte!!!

Pensate che il Grande Fratello sui dati
conservati per i soli 24 mesi (12)

NON ci sarà più ?

il Rischio ? = zero

Il gioco vale ancora la candela = continuerà
ad esserci per i dati di 24 mesi !!!

2 anni sono come 8 anni.....ti ricatto lo stesso, sarà più
difficile....aumenterà il prezzo....

2)

Note dolenti anche sul fronte opposto
a cui sta tanto a cuore la sicurezza del Paese.....
Essi sono infatti rei di..



- di non aver chiesto fino a 2 anni i telematici (lo prevede la direttiva 2006/24/Ce
- di non essersi accorti o aver fatto rilievi a livello Parlamentare o sollevato discussioni più ampie
- di non aver chiesto l'attuazione dell'art. 30 TCE che consente agli Stati membri di discostarsi dalla normativa per particolari motivi (tra i quali ordine pubblico)
- di non richiedere e/o aver richiesto entro il termine del 15 settembre "FUTURE MISURE" ai termini di cui alla direttiva....(art. 12)

infatti....

PER CIRCOSTANZE PARTICOLARI e per
periodi limitati lo Stato membro può esercitare la
facoltà di prorogare i termini di conservazione
(art. 12 direttiva 2006/24)

Comunicare (motivando) alla Commissione tale
termine più lungo

mesi 6 e poi “silenzio assenso”

Le misure nazionali si considerano approvate

Il rischio serio

è che la bilancia penda troppo da una parte....

non è auspicabile una sproporzione
neanche se pende dalla parte della privacy

La conseguenza è l'eccessiva e repentina
alternanza tra due beni giuridici di pari grado

per i cittadini:

- in 5 minuti e con un tratto di penna la privacy potrebbe essere cancellata o soppressa (per motivi urgenti) per periodi di tempo
(vedi estate 2005)

per la sicurezza del Paese:

- non si è in grado di fare strategie preventive e siamo sempre a rincorrere...

La soluzione ?

tra due beni giuridici di pari grado

Sicurezza e riservatezza

L'equilibrio è determinato dalla

prevenzione

ed eventuale punizione (vera)

degli abusi (DA UNA PARTE E DALL'ALTRA)

Altrimenti.....

Tra i due litiganti....

nella terra di nessuno

ci stiamo dimenticando

la storia

delle leggi dell'emergenza

Esse ci privano del bene giuridico

invece di cercare un equilibrio sulla

bilancia.....

Parafrasando Albert Einstein

Non so ancora bene cosa c'è scritto sul decreto in pubblicazione in questi giorni....

Ma so cosa ci sarà scritto sul prossimo....

“da oggi ed a tempo indeterminato sono sospesi di diritti previsti dal Dlgs 196 del 2003 (codice privacy)”

eppure

“la storia insegna agli uomini...”

...o almeno dovrebbe



Grazie dell'attenzione !
sono a disposizione per le vostre domande



Avv. Prof. Stefano Aterno

www.studioaterno.it

s.aterno@studioaterno.it