



Il Secolo della Rete

For a Free Knowledge Society

Protesta contro il decreto "Grande Fratello"

di Fiorello Cortiana e Monica Frassoni *

"Il decreto legge del governo, che raddoppia i tempi di conservazione dei tabulati telefonici e di internet per tutti i cittadini nel nome della lotta al terrorismo, mette in discussione in modo indiscriminato diritti fondamentali garantiti costituzionalmente. L'**art.15** della costituzione afferma l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione, l'estensione assoluta della limitazione di queste libertà non trova rispondenza nella lotta al terrorismo. Un provvedimento di questo genere non si prende attraverso un decreto alla vigilia di natale, e' **un amaro regalo per la costituzione**, per il parlamento e per tutti i cittadini italiani. Alla ripresa dei lavori interesseremo il parlamento italiano ed europeo e gli organismi di tutela internazionale della privacy e dei diritti costituzionali, affinché il governo italiano modifichi il provvedimento nel rispetto delle garanzie fondamentali".

** Intergruppo sull'innovazione tecnologica e cittadinanza telematica e Co-presidente dei verdi al Parlamento Europeo)*

Petizione

*All'attenzione di **Marcello Pera** (Presidente del Senato), **Pierferdinando Casini** (Presidente della Camera), **Silvio Berlusconi** (Presidente del Consiglio).*

Con la presente, intendo protestare per il decreto che il consiglio dei ministri ha improvvisamente varato lo scorso 23 dicembre. Ritengo che la **conservazione coatta** dei siti che visito, dei destinatari delle mie telefonate e delle mie email per un periodo non inferiore ai **5 anni** costituisca una **violazione inaccettabile** dei diritti inviolabili che mi spettano in quanto cittadino, così come sancito dall'art. 15 della Costituzione. Ritengo inoltre che una decisione così importante avrebbe meritato un ampio dibattito pubblico, e non una scelta unilaterale ed improvvisa. Auspico quindi che il Parlamento possa correggere i punti del decreto nel rispetto del nuovo codice della Privacy. Diversamente, mi servirò solo di provider che sfruttano server e connessioni residenti all'estero.

Roma - C'è chi sorride dinanzi al decreto legge varato dal Governo in queste ore, una normativa che riguarda internet e i cittadini italiani e che è riuscita nell'arco di 24 ore a scatenare un'ondata di polemiche come raramente si è visto. Il sorriso, in effetti, è espressione della natura umana quando viene posta, all'improvviso e inaspettatamente, dinanzi ad una enormità come quella presentata a Palazzo Chigi da due ministri: Castelli (Giustizia) e Stanca (Innovazione).

Il testo varato dal Governo concretizza con pochi semplici concetti un quadro orwelliano paventato dai più pessimisti all'alba della rivoluzione digitale. I provider internet e gli operatori di telefonia devono **conservare fino a cinque anni tutti i dati del traffico**, quello internet, appunto, e quello telefonico. Per dati di traffico si intendono i contatti, chi manda o spedisce un messaggio, a chi viene fatta una telefonata e da chi, e quando. Dati che l'autorità giudiziaria potrà richiedere alla bisogna a provider ed operatori. La giustificazione di tutto questo è quella di sempre: *sicurezza* e *anti-terrorismo*. Non si intendono, come si era creduto in un primo tempo, **i contenuti delle email o delle telefonate**. Nella [conferenza stampa di presentazione](#) Stanca ha sottolineato che "è importante registrare che mi sono collegato, che mi sono collegato a quella persona, per questo periodo di tempo, in quella data, a quell'ora, eccetera". Ed è stata esplicitamente **esclusa la registrazione** dei contenuti delle comunicazioni.

Il progettino che vuol essere progettone appare ai più fallato.

Il primo problema, evidenziato ieri da una nota diffusa da [AIIIP](#) e [Assoprovider](#), le due associazioni di settore, sono le strutture necessarie a registrare i dati di traffico. Gli oneri per archiviare la mole di dati richiesta, per garantirle la giusta sicurezza e integrità, sarebbero presto eccessivi per operatori che oggi conservano quei dati per soli pochi giorni esclusivamente per rispondere a problemi di instradamento.

Ma soprattutto c'è il problema della **privacy**. Il [Garante della privacy](#) in seduta collegiale subito dopo il varo del provvedimento ha emesso - fatto rarissimo - una nota in cui sottolinea come possa confliggere con il dettato costituzionale che protegge la segretezza e la libertà delle comunicazioni. Il Garante si attende che il Parlamento metta pesantemente mano al provvedimento non appena giungerà alla sua attenzione per l'esame e l'eventuale successiva traduzione del tutto in legge dello Stato. L'iniziativa governativa, peraltro, arriva a pochi giorni dall'introduzione del nuovo Codice della privacy che ne esce, evidentemente, stravolto.

"Ogni ulteriore estensione della fattispecie di dati raccolti - scrivono ancora i provider a questo proposito - deve essere soppesata con estrema cautela, sia sotto il profilo della quantità di dati da memorizzare, sia e soprattutto perché comporterebbe la creazione di archivi dai quali si potrebbe risalire (...) alla cerchia di relazioni di ciascun utente creando, nei fatti un dossier a carico di ciascun cittadino da cui rimarrebbero esclusi, in una sorta di paradossale digital divide alla rovescia, solo coloro che ancora non usano la rete".

Ad attaccare a spada tratta il provvedimento sono anche riferimenti storici per la rete italiana, come [Alcei](#), l'associazione per le libertà digitali, che in una nota ricorda come "l'accumulazione preventiva del traffico internet ha una scarsissima efficacia investigativa e non aggiunge sostanziale valore all'operato della polizia giudiziaria. Le attuali tecniche di indagine di cui dispone la magistratura, insieme alla cooperazione offerta dagli internet provider e dagli operatori telefonici già consentono, infatti, di svolgere investigazioni di polizia senza bisogno di emanare norme pericolose che, a parte la discutibilità tecnica, danno *licenza di spiare* tutto e tutti".

"Solo in caso di indagine - ha spiegato ieri Stanca - abbiamo consentito alla magistratura l'accesso ai dati della comunicazione telefonica e internet. È un esempio, perché tutti i paesi si stanno muovendo in questa direzione". Lui lo chiama "un altro passo avanti".

Telefonate ed email: bisogna conservare i dati per 5 anni
Un decreto del consiglio dei ministri raddoppia i tempi
di archiviazione della comunicazione telematica.
Soddisfazione della direzione Antiterrorismo
ma il Garante parla di schedatura dei cittadini

23 dicembre 2003

di Stefano Porro

ROMA. Da qualche giorno siamo tutti più sorvegliati. Lo scorso 23 dicembre il governo ha varato un decreto legge che obbliga i gestori di traffico telefonico e i provider che forniscono accesso a Internet a conservare la memoria del traffico generato dai loro utenti per un periodo non inferiore a 5 anni. Un profluvio di dati relativi a telefonate, sms ed email inviati o ricevuti, e persino ai siti che visitiamo, sarà d'ora in poi accuratamente archiviato per essere messo a esclusiva disposizione dei magistrati che indagano su reati di eversione e di criminalità organizzata.

Soddisfazione per il provvedimento è stata espressa dal pm Pietro Saviotti, titolare dell'**inchiesta sulle nuove Brigate Rosse**, secondo il quale la normativa faciliterà il lavoro di indagine della magistratura, soprattutto nel campo dell'anti-terrorismo. Il decreto infatti recepisce le richieste avanzate tempo fa dalla Direzione nazionale antimafia e dai distretti antiterrorismo che potranno investigare su dati e comunicazioni effettuate in un periodo di 60 mesi. Nonostante il **ministro della Giustizia Castelli** abbia precisato che il monitoraggio delle attività compiute su Internet riguarda solo i dati esterni (orario di connessione, mittente e destinatario delle email) e non i contenuti (il corpo del messaggio o gli allegati), il garante della privacy Stefano Rodotà paventa il rischio di una fascicolazione sociale dei cittadini.

"La posta elettronica e i dati sulla navigazione di Internet contengono informazioni sensibili attraverso cui è possibile ricostruire le preferenze delle persone, conoscere qual è il loro stato di salute o credo politico, e addirittura indagare sulle loro relazioni sociali" precisa Rodotà. "Basta analizzare quali siti frequento o a chi scrivo email con maggiore frequenza per tracciare un mio profilo di base. In questo modo si trasformano i cittadini in potenziali sospetti".

Di tutt'altro parere il ministro dell'Innovazione Tecnologica Lucio Stanca che ha definito la nuova normativa una "soluzione bilanciata tra l'esigenza prioritaria della libertà e della privacy individuale ed i problemi della sicurezza che, in alcuni momenti critici, è funzionale all'esercizio della libertà".

La patata bollente passa a questo punto ai provider, i quali dovranno affrontare ingenti investimenti per gestire le nuove metodologie di archiviazione. Secondo Daniele Manini, responsabile dell'associazione di categoria Assoprovider, "è tecnologicamente impossibile soddisfare le richieste del governo. Al giorno d'oggi 24 milioni di italiani usano Internet. Se ipotizziamo che ciascuno di questi riceva (solo) 1 megabyte di posta al giorno, la conservazione di questo traffico per 5 anni genererebbe un archivio di circa 80 milioni di CD-Rom. Una massa di dati impossibile da gestire".

La polemica è più che mai aperta, e c'è da giurare che non si placcherà facilmente. Al Parlamento toccherà il difficile compito di stabilire un equilibrio tra la necessità di garantire protezione e sicurezza ai cittadini senza intaccarne l'inviolabile diritto alla libertà e alla segretezza della comunicazione, così come sancito dall'art. 15 della Costituzione. Altrimenti, l'anno nuovo si aprirà sotto l'egida del Grande Fratello.

<http://www.assoprovider.net/page-news-on-line.phtml?ID=173>

23 Dicembre 2003

[AIIP ED ASSOPROVIDER ALLARMATE PER LA VENTILATA ESTENSIONE DELLA ARCHIVIAZIONE DEI DATI DI TRAFFICO INTERNET.](#)

L'AIIP, Associazione Italiana Internet Provider e AssoProvider, Associazione Provider Indipendenti esprimono estrema preoccupazione per le dichiarazioni rilasciate dal dott. Saviotti nell'intervista pubblicata sul Corriere della Sera di oggi 23 dicembre 2003.

L'ipotesi, ventilata nell'intervista, di una archiviazione coatta di tutte le E-mail (e relativi allegati) scaricate dagli utenti italiani di Internet si scontra con la realtà fisica e con l'articolo 15 della costituzione ed avrebbe l'effetto di far dirottare il traffico di posta elettronica verso paesi più rispettosi della dignità della persona.

Sotto il profilo della realtà fisica, assumendo che nella media, i 24 milioni di utenti internet italiani ricevono

(solo) 1 Mbyte di posta al giorno, la conservazione di questo traffico per 5 anni genererebbe un archivio di circa 80 milioni di CD-Rom.

Sotto il profilo costituzionale, l'articolo 15 recita: La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge." Esclude quindi qualsiasi forma di intercettazione generalizzata e preventiva della E-mail, sia pure solo di quelle effettivamente scaricate dal destinatario, e di qualsiasi altra forma di traffico internet.

Allo stato delle cose, i Provider di accesso alle rete Internet, nel rispetto delle norme di sicurezza imposte dalla vigente regolamentazione, mantengono un registro delle assegnazioni temporanee o permanenti dei numeri di IP assegnati a propri clienti. Con il codice di autoregolamentazione "internet e minori", allo scopo di agevolare l'identificazione indiretta degli autori della immissione in rete su server condivisi tra più utenti e nel rispetto del principio dell'anonimato protetto (si all'anonimato per le attività lecite, no all'impunità per quelle illecite), hanno assunto anche l'obbligo di mantenere un registro dei numeri di IP utilizzati per la pubblicazione anonima di contenuti in rete. I dati (header) necessari per l'instradamento della E-mail sono conservati solo per il tempo necessario (pochi giorni) a rispondere all'interessato della eventuale mancata esecuzione del servizio.

Come dimostra la cospicua attività di contrasto e repressione del crimine informatico attuata dalla Polizia delle Comunicazioni e dalle altre forze dell'ordine, questi dati, lecitamente raccolti per l'esecuzione del servizio, si sono sinora dimostrati adeguati alla esecuzione di indagini anche complesse.

Ogni ulteriore estensione della fattispecie di dati raccolti deve essere soppesata con estrema cautela, sia sotto il profilo della quantità di dati da memorizzare, sia e soprattutto perché comporterebbe la creazione di archivi dai quali si potrebbe risalire agli interessi culturali, sociali, politici, religiosi, sessuali etc., nonché alla cerchia di relazioni di ciascun utente creando, nei fatti un dossier a carico di ciascun cittadino da cui rimarrebbero esclusi, in una sorta di paradossale digital divide alla rovescia, solo coloro che ancora non usano la rete.

La violazione fatta sistema della privacy dei cittadini irreprensibili, rappresenta un onere sociale ed economico che deve essere soppesato prima di una eventuale fuga in avanti: occorre verificare attentamente se in luogo di un "giro di vite" generalizzato, non sia piuttosto il caso di verificare quali smagliature nelle misure di sicurezza già in atto hanno in qualche caso agevolato l'uso delittuoso della rete.

In conclusione AIIP ed AssoProvider, evidenziano la dubbia costituzionalità del provvedimento oggi in discussione al Consiglio dei Ministri e manifestano estrema preoccupazione per gli effetti sociali ed economici dei provvedimenti ventilati.

Decreto-legge 24 dicembre 2003, n. 354

Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia

(GU n. 300 del 29-12-2003)

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 77 e 87 della Costituzione;

Vista la VI disposizione transitoria della Costituzione;

Ritenuta la straordinaria necessità ed urgenza di riorganizzare la giurisdizione dei tribunali regionali e del Tribunale superiore delle acque pubbliche all'esito delle declaratorie di illegittimità costituzionale di cui alle sentenze della Corte costituzionale numeri 305 e 353 del 2002, in attesa della complessiva riforma della disciplina concernente il governo delle acque pubbliche e degli impianti elettrici, che attualmente risale al testo unico approvato con regio decreto 11 dicembre 1933, n. 1775;

Ritenuta, in attesa della riforma organica della magistratura onoraria, la straordinaria necessità ed urgenza di assicurare la proroga dell'esercizio delle funzioni da parte dei giudici onorari di tribunale e dei vice procuratori onorari, di imminente scadenza;

Ritenuta la straordinaria necessità ed urgenza di disciplinare le modalità di conservazione dei dati di traffico connesso ai servizi di comunicazione telefonica e via internet, così da prevenirne la perdita nell'ipotesi in cui ne risulti necessaria l'acquisizione ai fini della repressione di reati di particolare gravità;

Sentito l'Ufficio del Garante per la protezione dei dati personali;

Ritenuta la straordinaria necessità ed urgenza di assicurare il funzionamento del Consiglio di giustizia amministrativa per la Regione siciliana, nonché di intervenire sulla disciplina del contratto di leasing finanziario per garantirne la corretta applicazione in ipotesi di procedure concorsuali, al fine di evitare il pregiudizio all'affidamento collegato alla cartolarizzazione dei relativi crediti;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 23 dicembre 2003;

Sulla proposta del Presidente del Consiglio dei Ministri e del Ministro della giustizia, di concerto con i Ministri dell'interno, per la funzione pubblica, per l'innovazione e le tecnologie e dell'economia e delle finanze;

Emana

il seguente decreto-legge:

Art. 1. Riorganizzazione dei tribunali delle acque

(omissis)

Art. 2. Proroga dell'incarico dei giudici onorari di tribunale e dei vice procuratori onorari prossimi alla scadenza

(omissis)

Art. 3. Modifiche all'articolo 132 del decreto legislativo n. 196 del 2003

1. L'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, è sostituito dal seguente:

«Art. 132 (Conservazione di dati di traffico per altre finalità)

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione dei reati.

2. Decorso il termine di cui al comma 1, i dati sono conservati dal fornitore per ulteriori trenta mesi e possono essere richiesti esclusivamente per 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 dell'autorità giudiziaria, d'ufficio o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. 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 pubblico ministero richiede al giudice, che decide con decreto motivato, l'autorizzazione ad acquisire i dati. Tale disposizione si applica anche al difensore dell'imputato o della persona sottoposta alle indagini che intenda acquisire direttamente i dati dal fornitore. Il

giudice procede all'acquisizione, con decreto motivato, anche d'ufficio.

5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto di particolari misure e di accorgimenti, nel determinare i quali si tiene comunque conto dei seguenti principi:

- a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato b);
- b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;
- c) individuare le modalità di accesso ai dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'accesso sia consentito 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 ai commi 1 e 2.

6. Le modalità di trattamento dei dati di cui al comma 5 sono individuate con decreto del Ministro della giustizia, di concerto con il Ministro dell'interno, con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, su conforme parere del Garante.».

Art. 4. Modifiche all'articolo 181 del decreto legislativo n. 196 del 2003

1. All'articolo 181 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali è aggiunto, in fine, il seguente comma: «6-bis. Fino alla data del 31 dicembre 2005 per la conservazione del traffico si osserva il termine della prescrizione di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171.».

Art. 5. Modifiche all'articolo 183 del decreto legislativo n. 196 del 2003

1. All'articolo 183 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, al comma 1, la lettera f) è sostituita, dalla seguente: «f) il decreto legislativo 13 maggio 1998, n. 171, ad eccezione dell'articolo 4, comma 2, la cui abrogazione decorre dal 1° gennaio 2006;».

Art. 6. Disposizioni in materia di giustizia amministrativa

(omissis)

Art. 7. Disposizioni in tema di effetti delle procedure concorsuali sui contratti di locazione finanziaria

(omissis)

Art. 8. Norma finanziaria

1. Per l'attuazione delle disposizioni del presente decreto è autorizzata la spesa complessiva di 743.960 euro a decorrere dall'anno 2004; al relativo onere si provvede mediante utilizzo delle proiezioni dello stanziamento iscritto, ai fini del bilancio triennale 2003-2005, nell'ambito dell'unità previsionale di base di parte corrente «Fondo speciale» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2003, allo scopo parzialmente utilizzando l'accantonamento medesimo. 2. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 9. Entrata in vigore

1. Le disposizioni degli articoli 1, 6 e 8 del presente decreto entrano in vigore il 1° gennaio 2004. Le altre entrano in vigore lo stesso giorno della pubblicazione del decreto nella Gazzetta Ufficiale della Repubblica italiana. Il presente decreto sarà presentato alle Camere per la conversione in legge.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 24 dicembre 2003

CIAMPI

Berlusconi, Presidente del Consiglio dei Ministri

Castelli, Ministro della giustizia

Pisanu, Ministro dell'interno

Quando è lecito spiare i cittadini?
di Manlio Cammarata - 30.10.03

Nelle cronache degli ultimi giorni sulla cattura dei brigatisti rossi che avrebbero ucciso il professor D'Antona e forse anche il professor Biagi è stato dato grande rilievo agli aspetti tecnologici delle indagini, dall'esame dei computer palmari all'elaborazione dei "tabulati" delle conversazioni telefoniche degli indagati, risalenti ad alcuni anni fa. Gli investigatori hanno sottolineato che, se fosse stato già in vigore il decreto legislativo 196/03 (che all'[art. 132](#) limita a trenta mesi la conservazione dei dati) non sarebbe stato possibile giungere alla ricostruzione dei fatti e alla cattura dei presunti responsabili.

L'osservazione è di quelle che fanno riflettere, perché riguarda il tema del bilanciamento tra la protezione della riservatezza e le esigenze della sicurezza. Una contrapposizione di grande rilevanza, per la quale è stata proposta una soluzione che dovrebbe mettere tutti d'accordo e che è stata accettata in linea di principio dallo stesso Rodotà: conservare sì i dati per cinque anni, ma affidandoli a un soggetto che dia la massima garanzia di riservatezza (e che potrebbe essere lo stesso Garante per la protezione dei dati personali).

Tra la proposta e la sua realizzazione pratica si possono intuire non poche difficoltà tecniche e organizzative, tuttavia superabili. Ma i problemi dei trattamenti di dati personali in funzione della prevenzione e repressione dei reati e della sicurezza nazionale non si esauriscono con i tabulati telefonici e pongono in ogni momento la questione del bilanciamento tra le esigenze della sicurezza dello Stato e il diritto alla riservatezza dei cittadini. Forse la difficoltà di risolvere questa inevitabile contrapposizione tra chi difende l'ordine pubblico e chi protegge la privacy è all'origine del ritardo nella pubblicazione dell' "Allegato C" del codice della protezione dei dati personali. Anche se il titolo "Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia" fa nascere la curiosità di sapere se ci sono o ci saranno regole anche per i "trattamenti occasionali".

Il fatto è che ci sono archivi delle forze dell'ordine che contengono una quantità enorme di informazioni personali: pensiamo alla registrazione delle presenze negli alberghi o alle verifiche di identità compiute durante i controlli casuali sul territorio, per fare i primi esempi che vengono alla mente e per non parlare della nascente banca di dati della carta d'identità elettronica, che di fatto comporterà una schedatura totale dei cittadini.

E non dimentichiamo gli ormai onnipresenti sistemi di videosorveglianza, anche questi spesso di vitale importanza per le attività di contrasto al crimine.

Nessun cittadino di buon senso può negare l'utilità di queste raccolte di dati e, anzi, trovarsi in un luogo pubblico sotto l'occhio di una telecamera può essere in qualche caso rassicurante. Non è difficile accettare qualche limitazione alla propria riservatezza, se essa si traduce realmente in una maggiore tranquillità. Ma il problema è che spesso non sappiamo chi raccoglie queste informazioni, per quanto tempo le conserva, chi può accedervi. E' necessaria una maggiore trasparenza, occorrono garanzie che oggi non ci sono o appaiono insufficienti.

Certo, non è realistico pensare di affidare questa enorme massa di dati in mano pubblica a qualche autorità di garanzia, ma sono necessarie regole meno vaghe e, soprattutto, si devono adottare strumenti efficaci per controllarne l'applicazione.

Tutto questo, però, riguarda l'ambito pubblico nel senso più lato. Dall'uso delle reti pubbliche di telecomunicazioni al transito nelle strade o in altri luoghi aperti a tutti, si può avere la consapevolezza dei controlli e accettarli in funzione della sicurezza collettiva, purché con adeguate garanzie. Ma quando si passa all'ambito individuale, al controllo di comportamenti privati senza la giustificazione dell'ordine pubblico, il discorso cambia. Le norme sulla protezione dei dati personali non sono più in conflitto con superiori esigenze di tutela della collettività, ma solo, in molti casi, con gli interessi economici di qualche settore commerciale. E qui la legge c'è, è chiara e va applicata senza riserve.

Per chi non lo avesse capito, stiamo parlando di un problema che abbiamo sollevato più volte e continueremo a richiamare fino a quando non sarà stato risolto: quello dei controlli mediante software spioni che inviano a qualcuno informazioni che ci riguardano, e magari anche all'estero, in palese violazione della normativa nazionale e comunitaria sul trattamento dei dati personali (vedi [Attenzione: il software ci spia!](#) di due settimane fa).

Qualche forma di controllo sulla vita privata dei cittadini da parte delle autorità costituite può essere accettabile, con limiti ben definiti e solo nei casi in cui i danni dell'invasività non siano più pesanti dei vantaggi, come nel caso della documentazione del traffico telefonico.

Il controllo operato dalle multinazionali commerciali non ha giustificazioni: nelle forme attuali viola quello che è ormai riconosciuto come un diritto fondamentale della persona e deve essere ricondotto nell'ambito della legalità.

Dati del traffico: chi-conserva-cosa?
di Andrea Monti - 08.01.04

Il [decreto-legge 354/03](#) contiene significative modifiche al [DLgs 196/03](#) "Codice in materia di trattamento di dati personali", del quale viene integralmente riscritto l'[art. 132](#) (conservazione dei dati di traffico per altre finalità).

La vecchia formulazione della norma stabiliva, laconicamente, che "fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione di reati, secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante". Mentre il nuovo testo (molto più articolato) si compone di ben sei commi che, essenzialmente, allungano i tempi di conservazione dei dati di traffico fino a cinque anni, oltre a definire i criteri soggettivi, tecnici e procedurali per la conservazione e l'accesso.

Qui ci occupiamo specificamente del nuovo art. 132 comma 1 del DLgs 196/03 secondo cui, "fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione dei reati."

L'identificazione dei dati di traffico rilevanti a norma del DL 354/03

Dal tenore letterale della norma si capisce che i "dati di traffico" dei quali è obbligatoria la conservazione sono esclusivamente quelli finalizzati alla fatturazione. E dunque verrebbero esclusi i log dei servizi (come http, ftp, mail, news) che si trovano a un livello più alto dello stack TCP/IP (vedi [Decreto legislativo 196/03: l'internet non è una rete](#)).

Si perviene a questa conclusione considerando che il comma 1 dell'art.132 del DLgs 196/03 richiama espressamente il comma 2 dell'[art.123](#) dello stesso provvedimento, secondo cui "il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale."

Però l'art.123 comma II va coordinato con la parte dell'[art. 2 della direttiva 2002/58](#) che, alla lettera b, definisce dati relativi al traffico "qualsiasi dato sottoposto a trattamento ai fini della relativa fatturazione". In realtà la norma definisce il dato di traffico in relazione a due ambiti: quello della fatturazione, di cui si dice nel testo, e quello della trasmissione di una comunicazione su una rete di comunicazione elettronica. Che però, in questo caso, non rileva, in quanto l'art.123 comma 2 del DLgs 196/03 fa esplicito riferimento ai trattamenti per sole finalità di fatturazione.

Nella normativa attuale non c'è più l'elenco dettagliato dei dati, che era presente nella direttiva 97/66/CE e nel [DLgs 171/98](#) (abrogati). Ma per capire la norma può avere senso "resuscitare" l'[allegato alla direttiva 97/66](#) che individuava i dati il cui trattamento, ai sensi dell'art. 6, è finalizzato alla fatturazione per l'abbonato ovvero ai pagamenti tra fornitori di reti in caso di interconnessione, vale a dire:

- a) il numero o l'identificazione della stazione dell'abbonato;
- b) l'indirizzo dell'abbonato e il tipo di stazione;
- c) il numero dell'abbonato chiamato;
- d) il numero totale degli scatti da considerare nel periodo di fatturazione;
- e) il tipo, l'ora di inizio e la durata delle chiamate effettuate e il volume dei dati trasmessi;
- f) la data della chiamata o dell'utilizzazione del servizio;
- g) altre informazioni concernenti i pagamenti.

Ma fra i dati indicati dall'allegato alla direttiva 97/66, l'internet service provider può conoscere con ragionevole certezza solamente quelli indicati nelle lettere d), e) ed f), mentre gli altri sono al di fuori del suo controllo o irrilevanti a fini di fatturazione e quindi non trattati.

Appartiene alla prima categoria (dati fuori dal controllo dell'ISP) il numero dell'abbonato (lett. a) visto che il servizio di accesso alla rete è di natura puramente logica e non prevede alcuna fruibilità del servizio basata sull'associazione univoca del numero chiamante all'abbonato. Dunque, l'ISP non ha modo di sapere se il CLI utilizzato dal proprio cliente appartenga a quest'ultimo o a terzi, che ne consentono l'utilizzo. L'unico ad avere il dato e a trattarlo a fini di fatturazione è l'operatore telefonico.

Anche l'indirizzo dell'abbonato (lett. b) non è sempre disponibile all'ISP, come nel caso di servizi "alla Dino Sauro". Cioè sostanzialmente anonimi e basati solo sull'identificazione del numero chiamante (che non necessariamente coincide con quello del "materiale utente" del servizio).

Il numero dell'abbonato chiamato (lett. c) e le altre informazioni relative al pagamento (lett. g)) sono del tutto irrilevanti visto che nel primo caso, il numero chiamato è sempre quello dell'ISP e nel secondo non è l'ISP che gestisce la fatturazione diretta.

Ora è chiaro che questo elenco non ha alcun valore precettivo dal punto di vista giuridico, ma tecnicamente individua in modo preciso quali sono i dati rilevanti quantomeno per i servizi di accesso e quindi non può essere ignorato.

Un ragionamento analogo può valere per i dati di traffico relativi ai servizi internet, sempre a condizione che siano soggetti a fatturazione specifica e differenziata da quella per il mero accesso alla rete). E dunque dovrebbero essere conservati i dati che identificano l'abbonato, il tipo di servizio utilizzato (web, posta, ecc.), data e ora della connessione, IP assegnato all'abbonato, IP raggiunti dall'abbonato, volume di dati generati.

Soggetti e servizi tenuti all'osservanza del provvedimento

Il problema interpretativo più serio, nella definizione di "dato di traffico trattato a fini di fatturazione" sta nel fatto che la normativa comunitaria e quella nazionale via via entrata in vigore trattano ancora (magari "inconsapevolmente") i servizi di comunicazione elettronica come se fossero i vecchi "servizi di telecomunicazioni" cioè, sostanzialmente, fonia e trasmissione dati.

E' quindi evidente che il DL 354/03 e le norme cui si richiama sono palesemente "ritagliate" sui fornitori di servizi di telefonia e ai carrier, ma con maggiori difficoltà sono applicabili agli ISP.

Tipicamente, infatti, questi ultimi non sono proprietari dell'infrastruttura fisica di trasmissione e la utilizzano per fornire servizi che, pur "appoggiandosi" sul trasporto di dati, hanno una fatturazione differenziata che prescinde, in molti casi, dalla "registrazione" dell'accesso. Come nel caso di housing, hosting, posta elettronica, antispam, antivirus ecc. che, nella misura in cui non sono soggetti a fatturazione basata sul traffico, non sono vincolati agli obblighi di conservazione.

Per quanto riguarda la connettività la situazione è più articolata.

I servizi flat su linea dedicata non sembrano rientrare nell'ambito di applicazione dell'art. 132 del DLgs 196/03 perché, non essendo il corrispettivo rapportato alla durata della connessione o al volume di dati trasmessi, non è possibile parlare di "dati di traffico" trattati "a fini di fatturazione".

Analogo discorso vale per i servizi in dial-up tramite rete commutata, considerato che i dati rilevanti li genera e custodisce l'operatore telefonico che raccoglie la chiamata e poi fattura direttamente in bolletta (mentre l'ISP fattura il solo canone per l'utilizzo della propria infrastruttura e del gateway verso l'internet).

L'obbligo sussiste, invece, per i servizi in dial-up su numerazione 702xx, nei quali l'ISP percepisce la *reverse interconnection* e dunque deve trattare i dati relativi alla durata della connessione per poter regolare i conti con il carrier. Ma anche in questo caso è necessario effettuare un distinguo.

Come è noto, con la reverse interconnection il gestore telefonico "retrocede" all'ISP una percentuale del traffico telefonico generato da chi si collega a determinati archi di numerazione. Dal punto di vista del gestore telefonico, è irrilevante se il titolare dell'utenza telefonica coincida o meno con l'abbonato dell'ISP. Perché conta il fatto che un certo numero di telefono abbia generato traffico su una certa numerazione, a prescindere da chi si sia materialmente collegato ai servizi dell'ISP.

Siamo di fronte, quindi, a rapporti giuridici distinti e separati che non interferiscono fra loro. Il primo intercorre fra gestore telefonico e abbonato ai servizi di telefonia per l'uso della linea telefonica. Il secondo fra ISP e abbonato a servizi internet per navigazione, mail e via scorrendo. Il terzo (al quale sono del tutto estranei sia l'abbonato al gestore, sia quello all'ISP) riguarda il gestore telefonico e l'ISP per la "spartizione" della bolletta.

Proviamo ora, in ipotesi, a metterci nella condizione di un ISP che deve applicare il DL 354/03 e dunque registrare i dati di traffico dei propri abbonati, cioè di chi ha sottoscritto un contratto con l'ISP in questione. Se l'abbonato dell'ISP usa la propria linea telefonica, egli è contemporaneamente abbonato dell'operatore telefonico e dell'ISP. In questo caso la registrazione dei dati di traffico è a carico di entrambi e non sorgono particolari problemi.

Se, invece, l'abbonato dell'ISP si serve di una linea altrui (come nel caso di chi si connetta, usando proprie userID e password, da casa di amici, ad esempio) la situazione cambia sensibilmente perché i rapporti giuridici si separano e l'abbonato dell'operatore telefonico è persona diversa da quello dell'ISP.

In questo scenario, l'operatore telefonico registra i dati relativi alla chiamata telefonica e addebita gli scatti all'intestatario della linea. Mentre l'ISP registra il collegamento, relativo ai servizi forniti, effettuato dal proprio abbonato (riconosciuto tramite userID e password) e il CLI del chiamante (con il quale non ha alcun rapporto giuridico e che, dunque, non può considerare "proprio" abbonato). In pratica, "abbonato" ai sensi del DL 354/03 è il cliente dell'ISP e non il titolare della linea (che è abbonato del gestore telefonico).

Considerato che la reverse interconnection è quantificata sulla base del traffico generato su una linea, e non dai servizi che ci passano sopra, l'ISP tratta a fini di fatturazione i dati della linea chiamante che però, non essendo intestata al proprio abbonato connesso, non rientra nelle ipotesi del decreto. E quindi non scatta l'obbligo di conservazione per trenta più trenta mesi. Tratta invece i dati relativi alla chiamata, che però arriva da un soggetto con il quale non ha alcun rapporto giuridico. E dunque non è obbligato a conservare questi

dati. D'altra parte non è possibile sostenere l'esistenza di un contratto concluso "al momento", perché mancano gli elementi essenziali di un contratto come, per lo meno, la volontà dell'interessato dell'utenza telefonica di intrattenere un rapporto giuridico con l'ISP e la consapevolezza sul contenuto dell'obbligazione.

L'aspetto paradossale della situazione creata dal DL 354/03 è che, in rapporto ai servizi internet, l'obbligo di conservazione per gli ISP si configura a seconda della tipologia di commercializzazione dei prodotti. Se housing, hosting, mail e via discorrendo sono fatturati a canone fisso, non c'è obbligo di conservazione. Se gli stessi servizi sono fatturati a tempo o a volume i dati di traffico vanno conservati. E' facile immaginare che, se questo decreto legge dovesse essere convertito così com'è, gli ISP dovranno rivedere profondamente la propria offerta commerciale. O addirittura, valutare la possibilità di uscire da questo mercato. Il che, per certi versi, favorirebbe anche l'opera degli investigatori, che avrebbero così a che fare con un numero ridotto di interlocutori.

Ma non farebbe certo bene al sistema-paese.

E' finita la privacy per i navigatori italiani

Un decreto blitz di fine anno del Governo obbliga tutti i gestori telefonici e gli Internet Provider a conservare i "dati di traffico" dei loro clienti degli ultimi 5 anni. Il Garante della Privacy protesta.

Di Pier Luigi Tolardo

[ZEUS News - www.zeusnews.it - *Prima Pagina*, 29-12-2003]

In genere alla fine dell'anno gli italiani sono molto impegnati a farsi gli auguri, a impacchettare i regali e a cercare di dimenticare l'anno trascorso che il Governo, qualunque sia il suo colore, approfitta della distrazione "natalizia" per rifilare qualche provvedimento negativo e/o impopolare che in un altro momento sarebbe più difficile far passare.

Così è stato anche a fine 2003 con un decreto del Governo Berlusconi che riforma il Codice della Privacy, emanato dallo stesso Governo, solo lo scorso 27 Giugno e non ancora entrato in vigore, perché la sua decorrenza è a partire dal 1 Gennaio 2004.

Il nuovo Codice della Privacy, cambiato prima di entrare in vigore, avrebbe dovuto porre fine alla prassi delle società telefoniche di conservare a fini di documentazione del traffico i dati dei contatti telefonici per ben 5 anni, i contatti significa il numero del chiamante, del chiamato, la data e l'ora e la zona per i telefoni mobili, non i contenuti che rimangono riservati e si devono intercettare apposta, con l'autorizzazione della magistratura o anche senza ma allora è un reato.

Il nuovo Codice della Privacy stabiliva in 30 mesi il termine massimo di conservazione di questi dati, il decreto Berlusconi stabilisce che devono essere conservati fino a 5 anni, ma dopo i 30 mesi, possono essere richiesti da un magistrato solo all'interno di indagini su terrorismo, mafia, rapimenti ed estorsioni.

In pratica il Governo ritorna sui suoi passi rispetto alle telefonate dopo l'allarme gettato dai magistrati del delitto D'Antona a proposito di colpevoli. a cui non sarebbero potuto risalire se la legge avesse limitato a 30 mesi la conservazione dei dati del traffico telefonico, dopo cui devono essere inesorabilmente cancellati. Bisogna, ragionevolmente, chiedersi perché, nel caso del delitto D'Antona, le indagini abbiano girato a vuoto per così tanto tempo ma il Governo ha raccolto questo grido d'allarme e ha reso legge una prassi delle società telefoniche che, invece, aveva deciso di cambiare.

C'è di più però: oltre alla conservazione dei dati del traffico telefonico il Governo introduce un obbligo, a carico degli internet Service Provider, di conservare i dati relativi a tutte le connessioni agli stessi da parte dei loro clienti. A disposizione dei magistrati, ma anche degli avvocati degli indagati, dovranno rimanere per 60 mesi dati come il tragitto di una comunicazione, mittente e destinatario, numero dei caratteri inviati per e-mail.

A differenza però della comunicazione telefonica, nel caso della comunicazione elettronica, sarà molto più difficile distinguere tra contatti e contenuti. E infatti lo stesso Garante per la Privacy Stefano Rodotà ha dichiarato con un suo comunicato ufficiale: *"La nuova disciplina sui dati relativi alle comunicazioni elettroniche e alle utilizzazioni di Internet può anche entrare in conflitto con le norme costituzionali sulla libertà e segretezza delle comunicazioni e sulla libertà delle manifestazioni del pensiero. Il Garante confida in un attento esame del decreto da parte del Parlamento"*.

La preoccupazione che dai file di log si possano ricostruire quali pagine internet sono state visitate, da chi e per quanto tempo, oppure quando è stata spedita una determinata e-mail, quanto pesava, quando è stata scaricata, ricostruendo gli interessi culturali, religiosi, politici, sessuali, la sua cerchia di relazioni, creando dei dossier sui cittadini, tranne naturalmente chi è escluso dalla Rete.

La stessa Assoprovider, l'Associazione che raggruppa gli Internet Provider, è preoccupata anche per i riflessi economici di questo provvedimento, che potranno produrre un aumento di costi per gli utenti stessi e in suo comunicato dichiara: *"Assumendo che nella media i 24 milioni di utenti Internet ricevano solo un megabyte di posta al giorno, la conservazione di questo traffico per 5 anni genererebbe un archivio di circa 80 milioni di Cd-Rom"*.

All'Unione Europea era allo studio una normativa comunitaria sulla conservazione dei dati delle comunicazioni elettroniche che prevedeva un tempo massimo di conservazione di 12 mesi ma la trattativa tra i diversi Paesi si è bloccata perché per alcuni era un tempo *eccessivo*.

Bisogna anche sottolineare che il Governo non tiene in nessun conto il parere delle Authority indipendenti, che pure il Parlamento ha eletto, basta considerare il fatto che i giudizi negativi di Antitrust e Autorità delle Comunicazioni in materia di radio-televisione e telefonia rimangono inascoltati, non solo quello della Privacy e, d'altra parte, né le Authority né un singolo cittadino o un'associazione possono ricorrere alla Corte Costituzionale se ritengono che una legge sia lesiva dei loro diritti costituzionali, ma, fortunatamente, questo diritto riconosciuto presso la Corte Europea dei Diritti dell'Aja.