



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

Prescrizioni del Garante [art. 154, 1 c) del Codice] - 10 gennaio 2008

Bollettino del n. 90/gennaio 2008, pag. 0

[doc. web n. 1524263]

[v. Prov. generale [17 gennaio 2008](#)]

## **Prescrizioni sulla conservazione dei dati di traffico (Telecom Italia) - 10 gennaio**

### **IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice") e, in particolare, gli artt. 123 e 132;

VISTI i vari accertamenti ispettivi effettuati presso diverse sedi di Telecom Italia S.p.A. (di seguito, "Telecom"), anche al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali nell'ambito della conservazione dei dati di traffico per finalità di accertamento e repressione dei reati;

VISTA la documentazione in atti;

VISTO l'art. 154, comma 1, lett. d) del Codice;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

### **PREMESSO**

Nel 2006 il Garante ha deliberato un programma ispettivo nei riguardi dei principali fornitori di servizi di comunicazione elettronica al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali nell'ambito della conservazione dei dati di traffico per finalità di accertamento e repressione dei reati. Ciò, anche in vista dell'adozione del provvedimento del Garante di cui all'art. 132, comma 5, del Codice.

Nell'ambito di tale iniziativa sono stati svolti nove accertamenti ispettivi sui sistemi utilizzati, per la predetta finalità, da Telecom Italia S.p.A. tesi, fra l'altro, a verificare l'adeguamento alle specifiche prescrizioni impartite dall'Autorità alla società con il provvedimento del 1° giugno 2006, relativo alle misure di sicurezza da implementare a garanzia di un lecito e corretto trattamento dei dati di traffico (doc. web n. [1296533](#), in [www.garanteprivacy.it](http://www.garanteprivacy.it)).

In particolare, sono stati effettuati i seguenti accertamenti: in data 12 luglio 2006 in Roma (per l'acquisizione di notizie sui dati di traffico e sui database), in data 18 e 19 luglio 2006 in Padova (sui sistemi informativi della telefonia mobile), in data 20 e 21 luglio 2006 in Bologna (sui sistemi informativi della telefonia fissa), in data 26, 27 e 28 settembre 2006 in Roma (sui sistemi informativi dell'area magistratura per la telefonia mobile), in data 9, 10 e 12 ottobre 2006 in Roma (sui sistemi informativi dell'area antifrode per la telefonia fissa e mobile), in data 17 e 18 ottobre 2006 in Milano (sui sistemi informativi dell'area magistratura per la telefonia fissa), in data 20, 24 e 25 ottobre in Roma (sui sistemi informativi dell' "area business intelligence" per la telefonia fissa), in data 22 novembre 2006 in Bologna (sui sistemi informativi della telefonia fissa in relazione all'adeguamento alle prescrizioni impartite dal Garante con il provvedimento del 1° giugno 2006) e, infine, in data 23 novembre 2006 in Roma (sui sistemi informativi della telefonia mobile in relazione all'adeguamento alle prescrizioni impartite dal Garante con il citato provvedimento del 1° giugno 2006).

Sulla base di tali accertamenti, il presente provvedimento attiene unicamente al rispetto, da parte della società, della normativa sulla protezione dei dati personali in riferimento alla conservazione dei dati di traffico telematico di cui all'art. 132 del Codice. Tale disposizione prescrive ai fornitori di servizi di comunicazione elettronica di conservare, per finalità di accertamento e repressione di reati, oltre ai dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, i dati relativi al traffico telematico, escludendone i "contenuti".

\*\*\*

Nel quadro delle attività di controllo sopraindicate, l'ispezione del 23 novembre 2006 è stata svolta al fine di verificare il funzionamento del sistema che registra dati di traffico telematico trattati per finalità di accertamento e repressione di reati nell'ambito della telefonia mobile (sistema *Ipms-IP monitoring system*) e, in particolare, per accertare il rispetto di quanto prescritto dal predetto art. 132 del Codice sui limiti alla conservazione dei dati di traffico telematico riconducibili al "contenuto" della comunicazione.

Nel corso del medesimo accertamento sono state rese alcune dichiarazioni per conto della società e si è precisato, in particolare, che: *"il sistema [Ipms] è alimentato da log file di tutto il traffico IP proveniente dalla rete e generato dai clienti della telefonia mobile, nonché dagli utilizzatori dei servizi resi tramite il portale di Tim. Il sistema è deputato*

anche all'attivazione, a richiesta dell'autorità giudiziaria, della duplicazione della posta elettronica, del fax via web ed all'attivazione di un trigger di segnalazione della connessione ai servizi Internet di un cliente di telefonia mobile" (v. dichiarazioni dell'ing. Carlo Benedetti, in qualità di addetto alla funzione di gestione applicativa, nell'ambito del verbale di operazione compiute il 23 novembre 2006).

Durante lo stesso accertamento è stato effettuato un accesso informatico al sistema Ipms, che ha consentito di acquisire alcuni file di log, generati dai mail server e dai proxy server della rete Tim. Dall'analisi di tali file di log è emerso che:

- il formato di registrazione dei file di log corrisponde al common log format (Clf) tipico dei sistemi web, riportando indicazione dell'indirizzo Ip dell'utente, della data e dell'ora della connessione, dell'indirizzo del sito visitato in notazione Url (*Uniform Resource Locator*) e di altri parametri tecnici;
- la registrazione degli indirizzi in notazione Url comprende l'indicazione dello specifico contenuto o pagina web visitata, nonché eventuali "parole chiave" o "stringhe di ricerca" utilizzate dagli utenti durante le sessioni Internet (tranne quelle svolte con protocolli di cifratura Ssl-*Secure socket layer*).

### CIÒ PREMESSO IL GARANTE OSSERVA

1. Nel rispetto del principio secondo il quale i dati non devono essere formati e conservati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio, i fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica possono formare e conservare soltanto i dati di traffico telematico che devono essere necessariamente generati e che devono rimanere temporaneamente nella loro disponibilità, essendo necessariamente correlati ad attività tecniche strumentali alla resa dei servizi offerti e alla loro eventuale fatturazione (artt. 3, 11 e 123 del Codice).

Il fornitore di accesso, "mediatore" della comunicazione, deve conservare esclusivamente i dati di traffico telematico funzionali a fornire ad abbonati e utenti e a fatturare il servizio di connessione alla rete.

Il fornitore di accesso non deve quindi conservare in qualunque forma informazioni sui siti visitati dagli utenti.

La necessità del pieno rispetto del predetto principio, derivante dalla funzione stessa svolta dal gestore e dai suoi limiti, va evidenziata anche alla luce della constatazione che il trattamento dei dati di traffico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, stante la natura particolarmente delicata delle informazioni trattate la cui conoscenza può avere importanti ripercussioni sulla sfera personale di più soggetti interessati. Tali dati richiedono, per la loro conoscibilità, adeguate garanzie, considerata la loro "accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore" (cfr., fra l'altro, Corte cost., 26 febbraio-11 marzo 1993, in G.U. 17 marzo 1993 e Corte cost., 14 novembre 2006, n. 372).

Per il traffico telematico, peraltro, vista la particolarità delle informazioni trattate, si pongono specifiche criticità rispetto alle comunicazioni telefoniche, potendosi non di rado riscontrare una sostanziale identificazione fra il dato esteriore della comunicazione elettronica e il contenuto della stessa. Alcuni dati di traffico telematico, apparentemente "esterni" alla comunicazione elettronica (come, ad esempio, le pagine web visitate o gli indirizzi Ip di destinazione), coincidono di fatto, nella maggior parte dei casi, con il "contenuto" della comunicazione medesima, consentendo, tra l'altro, di ricostruire direttamente o indirettamente relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

In questo quadro, a prescindere dalle garanzie previste in termini più generali nell'ordinamento anche sul piano costituzionale e processuale, va anche tenuto specificamente conto del fatto che l'art. 132 del Codice, nel prescrivere la conservazione temporanea dei dati di traffico per finalità di accertamento e repressione di reati, specifica puntualmente, con riferimento al traffico telematico, che devono essere esclusi dalla conservazione "i contenuti delle comunicazioni" (art. 132 del Codice, come modificato dal d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155 e successivamente prorogato con d.l. 31 dicembre 2007, n. 248).

2. Dall'esame delle risultanze emerse dai predetti accertamenti relativi al sistema Ipms, nonché dall'analisi della documentazione in atti, è emerso che Telecom Italia S.p.A. effettua un trattamento illecito e non corretto dei dati di traffico telematico degli utenti che usufruiscono dei servizi di accesso alla rete Internet, erogati con tecniche Gsm (*Global System for Mobile Communications*), Gprs (*General Packet Radio Service*), Edge (*Enhanced Data rates for Gsm Evolution*), Umts (*Universal Mobile Telecommunications System*) e Hsdpa (*High Speed Downlink Packet Access*).

Nell'impostazione della società, la fornitura del servizio di accesso alla rete Internet implica il trattamento di dati di traffico telematico raccolti tramite sistemi di "transparent proxying" che vengono interposti tra l'utente e i siti della rete ai quali questi accede. Tale azione tecnica, non necessaria per l'instradamento della comunicazione, né per la sua fatturazione, determina un'ingente raccolta di dati personali in forma di log file relativi alle connessioni effettuate nel corso della c.d. navigazione web. Ciò, anche con riferimento a siti esterni alla rete del fornitore di accesso, rispetto ai quali Telecom agisce da "mediatore" della connessione, ovvero quale fornitore del canale trasmissivo attraverso cui si sviluppa la comunicazione elettronica.

Tale raccolta di dati, realizzata sui percorsi di navigazione degli utenti, è risultata peraltro assai capillare, interessando tutti gli utenti di rete mobile e prevedendo la tenuta di dettagliati "log file", recanti indicazioni complete sugli indirizzi in notazione Url delle risorse richieste (indirizzi dettagliati delle pagine web e di ogni oggetto in esse compreso o richiamato), sugli indirizzi Ip del client che ha richiesto una determinata risorsa, sulla data e sull'ora della richiesta, insieme ad altri parametri tecnici tipici della tecnologia web la cui registrazione è possibile sulla base dei protocolli di rete in uso (http).

3. Alla luce di quanto rilevato al precedente punto 1, non risulta lecito e deve, pertanto, essere oggetto di divieto, il trattamento effettuato dalla società consistente nell'interposizione non necessaria per la fornitura del servizio di accesso alla rete Internet di sistemi di "transparent proxying" tra l'utente e i siti della rete ai quali questi accede; tali sistemi determinano un'ingente raccolta di dati personali in forma di log file relativi alle connessioni effettuate nel corso della navigazione web, anche con riferimento a siti esterni alla rete della società.

Non risulta altresì lecita e deve essere, parimenti, vietata la raccolta con conseguente conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche quando esse siano specificate con notazione Url o con mero indirizzo Ip di destinazione. I dati già trattati illecitamente dovranno essere cancellati al più presto dando riscontro a questa Autorità dell'avvenuta cancellazione entro, e non oltre, il termine che appare congruo stabilire in sessanta giorni dalla ricezione del presente provvedimento.

4. Come si è detto, il presente provvedimento riguarda solo i dati di traffico telematico.

Con riferimento agli ulteriori profili oggetto di accertamento ispettivo, l'Autorità si riserva ogni altra determinazione, anche all'esito di eventuali nuovi accertamenti volti a verificare la veridicità delle dichiarazioni rese per conto della società (rilevanti anche sul piano della responsabilità ai sensi dell'art. 168 del Codice), in ordine all'integrale recepimento delle prescrizioni impartite dall'Autorità, sia con il provvedimento del 15 dicembre 2005 (in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. [1203890](#)), sia con il citato provvedimento del 1° giugno 2006, il cui termine per l'attuazione delle prescrizioni è stato differito al 31 marzo 2007 (Prov. 7 dicembre 2006, doc. web n. [1371041](#)).

#### PER QUESTI MOTIVI IL GARANTE

A) vieta, ai sensi dell'art. 154, comma 1, lett. d) del Codice a Telecom Italia S.p.A., avente sede in Milano, Piazza Affari n. 2, ogni ulteriore trattamento di dati personali consistente:

1. nell'interposizione di sistemi informatici tra l'utente e i siti della rete ai quali questi accede, nella misura in cui i medesimi sistemi non siano strumentali alla resa del servizio di accesso alla rete Internet e determinino una raccolta di dati eccedente e non necessaria per la fornitura del servizio stesso o per la sua eventuale fatturazione;

2. nella raccolta e nella conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche quando esse siano specificate con notazione Url o con mero indirizzo Ip di destinazione. Ciò, in riferimento sia al sistema relativo alla telefonia mobile denominato *Ipms-Ip monitoring system*, sia ad ogni altro sistema in cui gli stessi, o altri analoghi dati di traffico vengano formati;

B) dispone, conseguentemente, la cancellazione dei dati trattati illecitamente al più presto, dando riscontro a questa Autorità dell'avvenuta cancellazione entro e non oltre il termine di sessanta giorni dalla data di ricezione del presente provvedimento.

Roma, 10 gennaio 2008

IL PRESIDENTE  
Pizzetti

IL RELATORE  
Pizzetti

IL SEGRETARIO GENERALE  
Buttarelli

stampa

chiudi