

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PROVVEDIMENTO 17 gennaio 2008

Conservazione dei dati di traffico: misure e accorgimenti a tutela dell'interessato in attuazione dell'articolo 132 del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali. (G.U. n. 30 del 5.02.2008)

IL PRESIDENTE

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, 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 (decreto legislativo 30 giugno 2003, n. 196, di seguito, «Codice»);

Visti in particolare gli articoli 17, 123 e 132, comma 5, del Codice;

Vista la deliberazione del 19 settembre 2007 con la quale l'Autorita' ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, riguardante «Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalita' di accertamento e repressione di reati» e pubblicato, unitamente alla medesima deliberazione, sul sito web dell'Autorita';

Visti i commenti e le osservazioni pervenuti a questa Autorita' a seguito della consultazione pubblica per la quale era stato fissato il termine del 31 ottobre 2007;

Considerate le risultanze dei diversi incontri, anche di carattere tecnico, intercorsi con alcune associazioni di categoria che lo avevano richiesto;

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

Premesso:

1. Considerazioni preliminari.

Il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le liberta' fondamentali, nonche' per la dignita' dell'interessato.

Tali informazioni hanno una natura particolarmente delicata e la loro impropria utilizzazione puo' avere importanti ripercussioni sulla sfera personale di piu' soggetti interessati; possono avere un'«accentuata valenza divulgativa di notizie caratterizzanti la personalita' dell'autore» e la loro conoscibilita' richiede adeguate garanzie (cfr., fra l'altro, Corte cost. 11 marzo 1993, n. 81 e 14 novembre 2006 n. 372).

I dati relativi al traffico telefonico e telematico dovrebbero peraltro riguardare solo alcune caratteristiche esteriori di conversazioni, chiamate e comunicazioni, senza permettere di desumerne i contenuti.

Inoltre, le stesse caratteristiche esteriori permettono di individuare analiticamente quando, tra chi e come sono intercorsi contatti telefonici o per via telematica, o sono avvenute determinate attivita' di accesso all'informazione in rete e persino il luogo dove si trovano i detentori di determinati strumenti.

L'intensita' dei flussi di comunicazione comporta la formazione e, a volte, la conservazione di innumerevoli informazioni che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali, e di formare anche

delicati profili interpersonali. Cio', specie quando i dati sono conservati massivamente dai fornitori per un periodo piu' lungo di quello necessario per prestare servizi a utenti e abbonati, al fine di adempiere a un distinto obbligo di legge collegato a eccezionali necessita' di giustizia.

Per le comunicazioni telematiche, poi, si pongono ulteriori e piu' specifiche criticita' rispetto alle comunicazioni telefoniche tradizionalmente intese, in quanto il dato apparentemente «esterno» a una comunicazione (ad es., una pagina web visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: puo' permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati.

Eventuali abusi (quali quelli emersi nel recente passato, allorché sono stati constatati gravi e diffusi fatti di utilizzazione illecita di dati), possono comportare importanti ripercussioni sulla sfera privata degli individui o anche violare specifici segreti attinenti a determinate attivita', relazioni e professioni.

Emerge quindi la necessita', in attuazione di quanto previsto per legge, di assicurare che la conservazione di tali dati da parte dei fornitori, laddove essa sia necessaria per prestare un servizio o in quanto imposta dalla legge, avvenga comunque in termini adeguati per garantire una tutela maggiormente efficace dei diritti e delle liberta' delle persone.

Per tali motivi, a prescindere dalle garanzie previste in termini piu' generali nell'ordinamento anche sul piano costituzionale e processuale, il legislatore all'art. 132 del Codice ha demandato al Garante per la protezione dei dati personali l'individuazione delle misure e degli accorgimenti che i fornitori dei servizi di comunicazione elettronica devono adottare a fronte della conservazione dei dati di traffico telefonico e telematico, allo stato prescritta per finalita' di accertamento e repressione dei reati.

Il presente provvedimento e' rivolto appunto a individuare le elevate cautele che devono essere osservate dai fornitori nella formazione e nella custodia dei dati del traffico telefonico e telematico.

Prima di indicare quali cautele risultano necessarie a seguito del complesso procedimento di accertamento curato dal Garante, sono opportune alcune altre premesse sull'attuale quadro normativo, sui fornitori e sui dati personali coinvolti.

2. Quadro di riferimento.

2.1. Normativa comunitaria.

La direttiva europea n. 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, impone agli Stati membri di proteggere la riservatezza delle comunicazioni elettroniche e vieta la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, a eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima.

La direttiva riguarda (art. 3) il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. I dati relativi al traffico sono definiti, in questa sede, quali quelli sottoposti a trattamento «ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione» (cfr. art. 2 e considerando n. 15 della direttiva 2002/58/CE).

La medesima direttiva, nell'imporre agli Stati membri l'adozione di

disposizioni di legge nazionali che assicurino la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, pone l'accento sui dati di traffico generati dai servizi medesimi (art. 5); tali dati, trattati e memorizzati dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione, fatte salve alcune tassative eccezioni (cfr. art. 6, paragrafo 2, 3 e 5 e art. 15, paragrafo 1; v., fra gli altri, il Parere n. 1/2003 sulla memorizzazione ai fini di fatturazione dei dati relativi al traffico, adottato il 29 gennaio 2003 dal Gruppo dei garanti europei per la tutela dei dati personali).

L'art. 15, paragrafo 1, della direttiva consente che gli Stati membri possano adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui ai predetti articoli 5 e 6 solo quando tale restrizione costituisca «una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica». A tal fine, gli Stati membri possono, tra l'altro, adottare misure legislative le quali prevedano che, per tali motivi, i dati siano conservati per un periodo di tempo limitato.

2.2. Normativa nazionale.

La direttiva 2002/58/Ce è stata recepita con il Codice in materia di protezione dei dati personali (Titolo X («Comunicazioni elettroniche»); cfr. art. 184). Nel Capo I di tale Titolo, intitolato «Servizi di comunicazione elettronica», è stata introdotta una nuova disciplina sulla conservazione dei dati di traffico telefonico.

Da un lato, l'art. 123 del Codice ha ridotto a sei mesi il previgente limite temporale per la conservazione dei dati di traffico telefonico per finalità di fatturazione, pagamenti in caso di interconnessione e di commercializzazione di servizi, termine che era in precedenza individuabile nella misura massima di cinque anni in base a quanto previsto dal decreto legislativo n. 171/1998.

Dall'altro, l'art. 132 del medesimo Codice, modificato prima della sua entrata in vigore (decreto-legge 24 dicembre 2003, n. 354, convertito in legge, con modificazioni, dall'art. 1 della legge 26 febbraio 2004, n. 45) ha introdotto un distinto obbligo per i fornitori di servizi di comunicazione elettronica di conservare per finalità di accertamento e repressione dei reati dati di traffico telefonico relativi ai servizi offerti.

Tutto ciò, sullo sfondo del principio cardine in materia secondo cui i dati non devono essere formati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio (articoli 3 e 11 del Codice).

Dal contesto sopra riassunto emerge che è stata nel complesso vietata una conservazione generalizzata dei dati relativi al traffico (art. 123, comma 1, cit.), con le seguenti eccezioni:

è stato consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2) o, previo consenso dell'abbonato o dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto (art. 123, comma 3);

è stata però prescritta in termini distinti la conservazione

temporanea dei dati di traffico telefonico per esclusive finalita' di accertamento e repressione dei reati per due periodi di ventiquattro mesi ciascuno (art. 132 del Codice).

Un successivo provvedimento d'urgenza del 2005 (decreto-legge 27 luglio 2005, n. 144, convertito in legge, con modificazioni, dall'art. 1 della legge 31 luglio 2005, n. 155) ha poi introdotto, tra l'altro:

- a) l'obbligo di conservare i dati di traffico telematico, escludendone i contenuti, per due periodi di sei mesi ciascuno;
- b) l'obbligo di conservare dati relativi alle chiamate telefoniche senza risposta;
- c) con riferimento ai primi ventiquattro mesi di conservazione dei dati del traffico telefonico e ai primi sei mesi di conservazione dei dati del traffico telematico, la previsione che la richiesta giudiziaria volta ad acquisirli, rivolta al fornitore, venga effettuata dal «pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private e non già dal giudice su istanza del pubblico ministero»;
- d) un regime transitorio in virtu' del quale e' stata sospesa temporaneamente l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati di traffico, anche se non soggetti a fatturazione (termine originariamente stabilito al 31 dicembre 2007, ma successivamente prorogato al 31 dicembre 2008 con l'art. 34 del recente decreto-legge 31 dicembre 2007, n. 248, in fase di conversione in legge);
- e) per i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie, che si limitino a porre a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, alcuni specifici obblighi di identificazione e monitoraggio delle operazioni compiute dai clienti (cfr. anche il decreto ministeriale 16 agosto 2005, in Gazzetta Ufficiale 17 agosto 2005, n. 190, attuativo di tale previsione).

Il decreto-legge del 2005 ha quindi, da un lato, emendato l'art. 132 del Codice (punti a), b) e c) sopra indicati) e, dall'altro, ha introdotto un regime transitorio per la conservazione dei dati, nonche' la predetta disciplina speciale applicabile solo a determinati soggetti.

Fermo restando il predetto regime, che prevede temporaneamente la conservazione (lett. d) sopra citata), la vigente normativa di riferimento prescrive ai fornitori di servizi di comunicazione elettronica di conservare comunque, per finalita' di accertamento e repressione di reati, i dati relativi al traffico telefonico (inclusi quelli concernenti le chiamate senza risposta) e quelli inerenti al traffico telematico (esclusi i contenuti delle comunicazioni), rispettivamente per ventiquattro e sei mesi (art. 132, comma 1, del Codice).

La stessa normativa prescrive inoltre, ai medesimi fornitori, di conservare tali dati per un periodo ulteriore, rispettivamente di ventiquattro e sei mesi, per l'accertamento e la repressione dei delitti tassativamente individuati dall'art. 407, comma 2, lettera a), c.p.p., nonche' dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2).

Infine, prevede che la conservazione dei predetti dati sia effettuata nel rispetto di specifici accorgimenti e misure a garanzia degli interessati. L'individuazione di tali cautele, oggetto del presente provvedimento, e' stata appunto demandata al Garante per la

protezione dei dati personali (cfr. articoli 17 e 132, comma 5, del Codice).

2.3. Altra disciplina comunitaria: la direttiva 2006/24/CE.

Al fine di armonizzare le disposizioni degli Stati membri sul tema della conservazione dei dati di traffico per finalità di accertamento e repressione di reati e' poi intervenuta la direttiva n. 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, che doveva essere recepita entro il 15 settembre 2007.

Tale direttiva contiene specifiche indicazioni sul risultato convenuto a livello comunitario con riferimento sia ai tempi di conservazione dei dati di traffico (minimo sei mesi e massimo due anni), sia alla corretta e uniforme individuazione delle «categorie di dati da conservare» (analiticamente elencate nell'art. 5 della direttiva medesima); cio', in relazione agli specifici servizi ivi enucleati, ovvero di telefonia di rete fissa e di telefonia mobile, di accesso a Internet, di posta elettronica in Internet e di telefonia via Internet.

In questo quadro risulta necessario tenere conto di tali indicazioni anche nell'ambito del presente provvedimento. Cio', anche in considerazione del fatto che nell'attuale quadro normativo interno, pur sussistendo una definizione generale di «dati relativi al traffico» (art. 4, comma 2, lettera h) del Codice), tali dati non vengono enumerati, ne' vengono distinti espressamente i dati relativi al traffico «telefonico» da quelli inerenti al traffico «telematico». Tale distinzione risulta, invece, necessaria in considerazione del fatto che il legislatore italiano, diversamente da quello comunitario, ha individuato due diversi periodi di conservazione in relazione alla natura «telefonica» o «telematica» del dato da conservare.

Cio' comporta l'esigenza di specificare l'ambito soggettivo di applicazione del presente provvedimento rispetto all'obbligo di conservazione dei dati.

3. I fornitori tenuti a conservare i dati di traffico.

Il «fornitore» sul quale incombe l'obbligo di conservare i dati di traffico ai sensi del citato art. 132 del Codice e' quello che mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione; per «servizi di comunicazione elettronica» devono intendersi quelli consistenti, esclusivamente o prevalentemente, «nella trasmissione di segnali su reti di comunicazioni elettroniche» (art. 4, comma 2, lettera d) e e), del Codice).

Cio', deriva:

a) dalla collocazione del menzionato art. 132 all'interno del titolo X, capo I, del Codice e da quanto disposto dall'art. 121 del medesimo Codice il quale, nell'individuare i «Servizi interessati», chiarisce che le disposizioni del titolo X «si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni»;

b) da quanto stabilisce il citato decreto-legge 27 luglio 2005, n. 144 nella parte in cui, nell'imporre la conservazione dei dati per il predetto regime transitorio, si riferisce ai «fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico».

Devono ritenersi quindi tenuti alla conservazione dei dati ai sensi del medesimo art. 132 i soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non

discriminazione (cfr. anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (c.d. direttiva quadro) e d.lg. n. 259/2003 recante il Codice delle comunicazioni elettroniche).

Al contrario non rientrano, ad esempio, nell'ambito applicativo del presente provvedimento:

i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nella definizione generale di «servizi di comunicazione elettronica», non possono essere infatti considerati come «accessibili al pubblico». Qualora la comunicazione sia instradata verso un utente che si trovi al di fuori della c.d. «rete privata», i dati di traffico generati da tale comunicazione sono invece oggetto di conservazione (ad es., da parte del fornitore di cui si avvale il destinatario della comunicazione, qualora si tratti di un messaggio di posta elettronica; cfr. documento di lavoro «Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line», adottato dal Gruppo di lavoro per la tutela dei dati personali il 21 novembre 2000);

i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico;

i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale;

i gestori dei siti Internet che diffondono contenuti sulla rete (c.d. «content provider»). Essi non sono, infatti, fornitori di un «servizio di comunicazione elettronica» come definito dall'art. 4, comma 2, lettera e) del Codice. Tale norma, infatti, nel rinviare, per i casi di esclusione, all'art. 2, lettera c) della direttiva 2002/21/Ce cit., esclude essa stessa i «servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica [...]». Deve rilevarsi, inoltre, 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 decreto-legge 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»);

i gestori di motori di ricerca. I dati di traffico telematico che essi trattano, consentendo di tracciare agevolmente le operazioni compiute dall'utente in rete, sono, comunque, parimenti qualificabili alla stregua di «contenuti».

4. I dati di traffico che devono essere conservati

L'obbligo di conservazione riguarda i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta,

nonche' i dati inerenti al traffico telematico, esclusi comunque i contenuti delle comunicazioni (art. 132 del Codice). In particolare, sono oggetto di conservazione i dati che i fornitori sottopongono a trattamento per la trasmissione della comunicazione o per la relativa fatturazione (art. 4, comma 2, lettera h), del Codice).

Pertanto, i fornitori (come individuati nel precedente paragrafo 3) devono conservare, per esclusive finalita' di accertamento e repressione di reati, solo i dati di traffico che risultino nella loro disponibilita' in quanto derivanti da attivita' tecniche strumentali alla resa dei servizi offerti dai medesimi, nonche' alla loro fatturazione. Cio', in ossequio anche ai principi di pertinenza e non eccedenza stabiliti dagli articoli 3 e 11 del Codice.

In tal senso, si esprime anche il citato decreto-legge 27 luglio 2005, n. 144 che, all'art. 6, riconduce l'obbligo di conservazione alle «informazioni che consentono la tracciabilita' degli accessi, nonche', qualora disponibili, dei servizi». La direttiva 2006/24/CE ribadisce che tale obbligo sussiste soltanto se i dati sono stati «generati o trattati nel processo di fornitura dei [...] servizi di comunicazione» del fornitore (cfr. considerando 23 e art. 3, paragrafo 1, della direttiva 2006/24/CE cit.).

L'art. 5 di tale direttiva contiene, poi, un'elencazione specifica delle informazioni da conservare e individua diverse categorie di dati di traffico, specificandone i contenuti a seconda che si tratti di traffico telefonico o telematico.

Nell'ambito dei servizi di comunicazione elettronica, occorre infatti distinguere i servizi «telefonici» da quelli «telematici».

Nei primi sono ricompresi:

le chiamate telefoniche, incluse le chiamate vocali, di messaggia vocale, in conferenza e di trasmissione dati tramite telefax;

i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata;

la messaggia e i servizi multimediali, inclusi i servizi di messaggia breve-sms.

Nei secondi sono ricompresi:

l'accesso alla rete Internet;

la posta elettronica;

i fax (nonche' i messaggi sms e mms) via Internet;

la telefonia via Internet (cd. Voice over Internet Protocol/VoIP).

Per quanto concerne specificamente la conservazione dei dati di traffico telefonico relativo alle «chiamate senza risposta», fermo restando allo stato quanto indicato dalla direttiva 2006/24/CE al considerando 12 (laddove esclude dal proprio ambito di applicazione i «tentativi di chiamata non riusciti»), il fornitore, in forza delle modifiche apportate dal decreto-legge n. 144/2005 all'art. 132 del Codice, deve conservare solo i dati generati da chiamate telefoniche che sono state collegate con successo, ma non hanno ottenuto risposta oppure in cui vi e' stato un intervento del gestore della rete (cfr. art. 2, comma 2, lettera f), direttiva 2006/24/CE).

5. Finalita' perseguibili.

Il vincolo secondo cui i dati conservati obbligatoriamente per legge possono essere utilizzati solo per finalita' di accertamento e repressione di reati (individuati specificamente per legge in riferimento al predetto, secondo periodo di conservazione) comporta una precisa limitazione per i fornitori nell'eventualita' in cui essi ricevano richieste volte a perseguire scopi diversi.

Ad esempio:

a) i medesimi fornitori non possono corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una

controversia civile, amministrativa e contabile;

b) sono tenuti a rispettare il menzionato vincolo di finalita' anche l'interessato che acceda ai dati che lo riguardano esercitando il diritto di accesso di cui all'art. 7 del Codice (e che puo' utilizzare quindi i dati acquisiti solo in riferimento alle predette finalita' penali), nonche', nel procedimento penale, il difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private (art. 132, comma 3, del Codice).

6. Modalita' di acquisizione dei dati.

Il Codice individua le modalita' con le quali possono essere acquisiti i dati di traffico conservati dai fornitori prescrivendo, con riferimento al primo periodo di conservazione (i primi ventiquattro mesi e sei mesi, rispettivamente per il traffico telefonico e telematico), che la richiesta sia formulata 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» (art. 132, comma 3, del Codice). Al difensore dell'imputato o della persona sottoposta alle indagini e' riconosciuta la facolta' di richiedere, direttamente, al fornitore i dati di traffico limitatamente ai dati che si riferiscano «alle utenze intestate al proprio assistito». La richiesta deve essere effettuata «con le modalita' indicate dall'art. 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'art. 8, comma 2, lettera f), per il traffico entrante» (art. 132, comma 3, cit.). Tale ultimo riferimento ai presupposti previsti dal Codice per l'accesso alle chiamate in entrata comporta, anche per i fornitori, la necessaria valutazione preliminare della circostanza che dalla mancata conoscenza dei dati richiesti possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397. A tale riguardo si richiama quanto rilevato nel provvedimento adottato dal Garante in materia il 3 novembre 2005, consultabile sul sito dell'Autorita' (doc. web n. 1189488).

In relazione al secondo periodo di conservazione, l'art. 132, comma 4, prevede che i dati conservati possano essere acquisiti soltanto in presenza di un decreto motivato del giudice che autorizzi l'acquisizione qualora ritenga sussistenti sufficienti indizi di uno o piu' delitti previsti dall'art. 407, comma 2, lettera a), c.p.p. o in danno di sistemi informatici o telematici.

7. Misure e accorgimenti da prescrivere.

Come premesso, il Garante e' stato preposto per disposizione di legge a individuare accorgimenti e misure da porre a garanzia degli interessati nell'ambito della conservazione dei dati di traffico telefonico e telematico per finalita' di accertamento e repressione di reati (art. 132, comma 5, del Codice).

A tal fine, il Garante ha curato preliminarmente diversi approfondimenti tecnici con esperti del settore, nonche' numerosi accertamenti ispettivi presso primari fornitori di servizi di comunicazione elettronica; ha, infine, indetto una specifica consultazione pubblica su un articolato documento indicante le misure e gli accorgimenti ritenuti idonei per la conservazione dei dati di traffico per finalita' di giustizia.

Le cautele ipotizzate in sede di consultazione pubblica hanno trovato conforto all'esito della stessa, non essendo pervenuti all'Autorita' sostanziali rilievi critici da parte dei soggetti interessati.

Tutte le riflessioni e commenti pervenuti sono stati comunque oggetto di specifica analisi e considerazione nell'elaborazione del presente provvedimento.

Nell'individuare le seguenti cautele che il Garante prescrive ai fornitori interessati al presente provvedimento, l'Autorita' ha tenuto conto dei parametri indicati negli articoli 17 e 132, comma 5, del Codice, nonché:

- a) dell'esigenza normativa volta a prevedere specifiche cautele rapportate alla quantità e qualità dei dati da proteggere e ai rischi indicati nell'art. 31 del Codice, rischi che i fornitori devono già oggi prevenire rispettando i comuni obblighi di sicurezza collegati alle misure non solo minime previste dal Codice (articoli 31 e seguenti; Allegato B);
- b) dell'opportunità di individuare, allo stato, misure protettive per i trattamenti svolti da tutti i fornitori interessati che siano verificabili anche in sede ispettiva, ai fini di una più incisiva messa in sicurezza dei dati di traffico telefonico e telematico;
- c) della necessità di tenere in considerazione i costi derivanti dall'adozione delle misure e degli accorgimenti prescritti con il presente provvedimento, anche in ragione della variegata capacità tecnica ed economica dei soggetti interessati;
- d) del contesto europeo di riferimento, specie alla luce dei pareri resi dal Gruppo per la tutela dei dati personali (cfr. pareri nn. 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE; 3/2006 sulla direttiva 2006/24/CE del Parlamento europeo e del Consiglio 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 che modifica la direttiva 2002/58/CE; 8/2006 sulla revisione del quadro normativo per le reti ed i servizi di comunicazione elettronica, con particolare attenzione alla direttiva relativa alla vita privata e alle comunicazioni elettroniche);
- e) dello stato dell'evoluzione tecnologica, alla luce del quale le seguenti prescrizioni devono pertanto ritenersi soggette ad aggiornamento periodico.

Di seguito, sono indicati gli accorgimenti e le misure prescritti dal Garante.

Per effetto del presente provvedimento:

7.1. Sistemi di autenticazione.

Il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito solo agli incaricati del trattamento e unicamente sulla base del preventivo utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti.

Per i dati di traffico conservati per esclusive finalità di accertamento e repressione dei reati (cioè quelli generati da più di sei mesi, oppure la totalità dei dati trattati per queste finalità se conservati separatamente dai dati trattati per le altre finalità fin dalla loro generazione), una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento.

Tali modalita' di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore.

Limitatamente a tali addetti tecnici, circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni hardware e software, aggiornamento e riconfigurazione dei sistemi, possono determinare la necessita' di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di autenticazione biometrica o di strong-authentication per operazioni che comportano la presenza fisica dell'addetto che procede all'intervento in prossimita' del sistema di elaborazione (per esempio, per lo svolgimento di operazioni di amministrazione da console locale che implicano la disabilitazione dei servizi di rete e l'impossibilita' di gestire operazioni di input/output tramite dispositivi accessori come quelli utilizzabili per la strong authentication).

In caso di accesso da parte degli addetti tecnici nei termini anzidetti, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice e, per quanto concerne i trattamenti di dati di traffico telefonico per esclusive finalita' di giustizia, quanto specificato al successivo paragrafo 7.3, dovra' essere tenuta preventivamente traccia in un apposito »registro degli accessi« dell'evento, nonche' delle motivazioni che lo hanno determinato, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

7.2. Sistemi di autorizzazione.

Relativamente ai sistemi di autorizzazione devono essere adottate specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Tali differenti funzioni non possono essere attribuite contestualmente a uno stesso soggetto.

I profili di autorizzazione da definire e da attribuire agli incaricati devono differenziare le funzioni di trattamento dei dati di traffico per finalita' di ordinaria gestione da quelle per finalita' di accertamento e repressione dei reati distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice), dagli incaricati abilitati anche al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice).

Conseguentemente, un incaricato cui sia attribuito un profilo di autorizzazione abilitante ad esempio al trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice) non puo' accedere, per cio' stesso e direttamente, a dati il cui trattamento richieda il possesso del profilo di autorizzazione relativo all'intero periodo di conservazione obbligatoria (art. 132, comma 2, del Codice).

Questa suddivisione non implica la moltiplicazione degli addetti ai servizi per scopi di giustizia; i fornitori hanno infatti la facoltà di utilizzare, per i loro incaricati, il profilo di autorizzazione che abilita al trattamento dei dati relativi al primo periodo o quello che abilita al trattamento dei dati relativi all'intero periodo di conservazione per scopi di giustizia.

7.3. Conservazione separata.

I dati di traffico conservati per esclusive finalità di accertamento e repressione di reati vanno trattati necessariamente tramite sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia nell'immagazzinamento dei dati (storage).

Più specificamente, i sistemi informatici utilizzati per i trattamenti di dati di traffico conservati per esclusiva finalità di giustizia devono essere differenti da quelli utilizzati anche per altre funzioni aziendali (come fatturazione, marketing, antifrode) ed essere, altresì, protetti contro il rischio di intrusione mediante idonei strumenti di protezione perimetrale a salvaguardia delle reti di comunicazione e delle risorse di memorizzazione impiegate nei trattamenti.

I dati di traffico conservati per un periodo non superiore a sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità, per l'elaborazione con sistemi dedicati a questo specifico trattamento.

Questa prescrizione lascia ai fornitori la facoltà di scegliere, sulla base di propri modelli organizzativi e della propria dotazione tecnologica, l'architettura informatica più idonea per la conservazione obbligatoria dei dati di traffico e per le ordinarie elaborazioni aziendali; permette infatti che i dati di traffico conservati sino a sei mesi dalla loro generazione possano essere trattati, per finalità di giustizia, con sistemi informatici non riservati esclusivamente a tali elaborazioni; oppure, che gli stessi dati vengano duplicati per effettuare un trattamento dedicato esclusivamente al perseguimento delle finalità di giustizia. In quest'ultimo caso le misure e gli accorgimenti prescritti per i dati conservati per esclusive finalità di giustizia si applicano sin dall'inizio del trattamento.

Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali.

Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico.

Nell'ambito dei trattamenti per finalità di accertamento e repressione di reati, una volta decorso il termine di cui al comma 1 dell'art. 132 del Codice, i dati di traffico devono essere trattati con modalità che consentano l'accesso differenziato su base temporale, provvedendo a forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti e

l'efficacia dei profili di autorizzazione definiti.

La differenziazione puo' essere ottenuta:
mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure mediante separazione logica, ovvero intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione.

Devono essere adottate misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni.

7.4. Incaricati del trattamento.

Gli incaricati che accedono ai dati di traffico conservati per le finalita' di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo, devono essere designati specificamente in rapporto ai dati medesimi.

Il processo di designazione deve prevedere la frequenza di una periodica attivita' formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilita'. L'effettiva partecipazione al corso deve essere documentata.

Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico (menzionate anche nell'art. 132, comma 5, lettera c)), nei limiti in cui cio' e' consentito ai sensi dell'art. 8, comma 2, lettera f) del Codice, il titolare del trattamento deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identita' del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo.

7.5. Cancellazione dei dati.

Allo scadere dei termini previsti dalle disposizioni vigenti, i dati di traffico sono resi non disponibili per le elaborazioni dei sistemi informativi e le relative consultazioni; sono altresì cancellati o resi anonimi senza alcun ritardo, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente, documentando tali operazioni al più tardi entro trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice.

7.6. Altre misure.

Audit log

Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di audit log devono garantire la completezza,

l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi devono essere adottati, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.

Le misure di cui al presente paragrafo sono adottate nel rispetto dei principi in materia di controllo dei lavoratori sull'uso di strumenti elettronici, con particolare riguardo all'informativa agli interessati (cfr. Provv. 1° marzo 2007, doc. web n. 1387522).

7.7. Audit interno Rapporti periodici.

La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati.

I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione.

L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

L'esito dell'attività di controllo deve essere comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.

7.8. Documentazione dei sistemi informativi.

I sistemi informativi utilizzati per il trattamento dei dati di traffico devono essere documentati in modo idoneo secondo i principi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione.

La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema.

La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalita' di accertamento e repressione di reati.

La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorita' su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico.

7.9. Cifratura e protezione dei dati.

I dati di traffico trattati per esclusive finalita' di giustizia vanno protetti con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. In particolare, devono essere adottate soluzioni che rendano le informazioni, residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei database o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche.

Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, data base administrator e manutentori hardware e software) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate.

Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire, piu' in generale, la sicurezza dei sistemi, evitando di esporli a vulnerabilita' e a rischio di intrusione (a titolo esemplificativo, l'accesso interattivo in modalita' «emulazione di terminale», anche per scopi tecnici, non deve essere consentito su canali non sicuri, cosi' come deve essere evitata l'attivazione di servizi di rete non necessari che si possono prestare alla realizzazione di forme di intrusione).

7.10. Tempi di adozione delle misure e degli accorgimenti.

Valutato il complesso delle misure e degli accorgimenti, tenuto conto del quadro delle cautele che emergono dalle risultanze ispettive essere gia' in atto presso i fornitori, nonche' dei tempi tecnici necessari per completarne l'attuazione, anche alla luce di quanto emerso dalla consultazione pubblica, risulta dagli atti congruo fissare un termine transitorio per i trattamenti di dati in essere, prevedendo che tutti gli adempimenti di cui al presente punto 7 siano completati al piu' presto ed entro, e non oltre, il termine che e' parimenti congruo stabilire per tutti i fornitori al 31 ottobre 2008. Entro tale termine, i fornitori dovranno dare conferma al Garante attestando formalmente l'integrale adempimento al presente provvedimento.

8. Applicazione di alcune misure a dati trattati per altre finalita'.

Le considerazioni svolte sulla natura particolarmente delicata dei dati di traffico, sulla necessita' di garantire una tutela maggiormente efficace dei diritti e delle liberta' delle persone e di prescrivere una piu' incisiva messa in sicurezza di dati rilevano

anche per ogni altro trattamento di dati di traffico telefonico e telematico effettuato dai fornitori di cui al paragrafo 3.

Cio', comporta l'improrogabile esigenza di assicurare che almeno alcuni tra gli accorgimenti e le misure di cui al precedente punto 7, limitatamente a quelli adattabili al caso di specie, siano applicati comunque dai predetti fornitori nell'ambito di analoghi trattamenti di dati di traffico telefonico e telematico effettuati per finalita' non di giustizia, ma di fatturazione, pagamento in caso di interconnessione e commercializzazione di servizi, nel piu' breve periodo temporale indicato nel menzionato art. 123.

Per tali ragioni il Garante, contestualmente e distintamente da quanto va disposto ai sensi dell'art. 132, comma 5, del Codice, prescrive ai fornitori di cui al paragrafo 3, ai sensi dell'art. 17 del medesimo Codice, di adottare nel termine e con la modalita' di cui al paragrafo 7 ottobre le misure e gli accorgimenti indicati nella lettera c) del seguente dispositivo.

Copia del presente provvedimento verra' trasmessa al Ministero della giustizia, anche ai fini della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonche', per opportuna conoscenza, all'Autorita' per le garanzie nelle comunicazioni.

Tutto cio' premesso il Garante:

a) ai sensi degli articoli 17, 123 e 132, comma 5, del Codice, prescrive ai fornitori di servizi di comunicazione elettronica individuati nel paragrafo 3 di adottare nel trattamento dei dati di traffico telefonico e telematico di cui al paragrafo 4 le misure e gli accorgimenti a garanzia degli interessati individuate nel presente provvedimento, provvedendo a (par. 7):

1) adottare specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento, nonche' di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalita', locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Per i dati di traffico trattati per esclusive finalita' di accertamento e repressione dei reati, una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento. Tali modalita' di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore. Relativamente ai soli addetti tecnici indicati al presente punto 1, qualora circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessita' di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di strong authentication, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice, deve essere tenuta traccia dell'evento in un apposito »registro degli accessi«, nonche' delle motivazioni che li hanno determinati, con una successiva descrizione sintetica delle operazioni svolte, anche

mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

2) adottare specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Il fornitore deve definire e attribuire agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice) dagli incaricati abilitati anche al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice);

3) adottare, per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati, sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (storage). I dati di traffico conservati per un periodo non superiore ai sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità. Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali. Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico. Inoltre, nell'ambito dei trattamenti per finalità di accertamento e repressione di reati, una volta decorso il termine di cui al comma 1 dell'art. 132 del Codice, il fornitore deve trattare tali dati con modalità che consentano l'accesso differenziato su base temporale, tramite forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti e l'efficacia dei profili di autorizzazione definiti. Tale differenziazione può essere ottenuta mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure mediante separazione logica, ovvero intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione. Infine, il fornitore deve adottare misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori

a sette giorni;

4) designare specificamente gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo. Il processo di designazione deve prevedere la documentata frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico, nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera f) del Codice, il fornitore deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo;

5) rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti. Il fornitore deve cancellare o rendere anonimi senza ritardo tali dati, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice;

6) adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi il fornitore deve adottare, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;

7) svolgere, con cadenza almeno annuale, un'attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. Tale attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento

e repressione dei reati. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere: comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria;

8) documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i principi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

9) proteggere i dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. Il fornitore deve adottare soluzioni che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei data base o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche. Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, database administrator e manutentori hardware e software) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate. Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in

chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire piu' in generale la sicurezza dei sistemi evitando di esporli a vulnerabilita' e a rischio di intrusione;

b) ai sensi dei medesimi articoli 17, 123 e 132, comma 5 del Codice, nonche' dell'art. 157 del Codice, prescrive ai predetti fornitori titolari del trattamento di effettuare tutti gli adempimenti di cui alla precedente lettera a) al piu' presto e, comunque, entro e non oltre il termine del 31 ottobre 2008, dandone conferma al Garante attestando entro lo stesso termine l'integrale adempimento;

c) ai sensi dell'art. 17 del Codice prescrive ai medesimi fornitori titolari del trattamento di adottare, rispetto ai dati di traffico trattati per le finalita' di cui all'art. 123 del Codice, entro e non oltre il termine del 31 ottobre 2008, dandone ai sensi dell'art. 157 del Codice conferma al Garante e attestando entro lo stesso termine l'integrale adempimento, i seguenti accorgimenti e misure (par. 8):

1) adottare specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento nonche' di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che abbiano la possibilita' concreta di accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalita', locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Qualora circostanze eccezionali, legate a indifferibili interventi per malfunzionamenti, guasti, installazione hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessita' di accesso a sistemi di elaborazione che trattano dati di traffico da parte di addetti tecnici in assenza di strong authentication, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice in materia di protezione dei dati personali, deve essere tenuta traccia in un apposito «registro degli accessi» dell'eventuale accesso fisico ai locali in cui sono installati i sistemi di elaborazione oggetto di intervento e dell'accesso logico ai sistemi, nonche' delle motivazioni che li hanno determinati, con una descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore;

2) adottare procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;

3) rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti, provvedendo alla loro cancellazione o trasformazione in forma anonima, in tempi

tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di conservazione (art. 123 del Codice);

4) adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi il fornitore deve adottare, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;

5) documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i principi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

d) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia anche ai fini della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Roma, 17 gennaio 2008

Il presidente
Pizzetti

Il relatore
Pizzetti
Il segretario generale
Buttarelli