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. 1484758]
[V. Provv. generale 17 gennaio 2008]

Prescrizioni sulla conservazione dei dati di traffico (Vodafone) - 10 gennaio 2008

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");

Visto il provvedimento in tema di nuove misure di sicurezza presso i fornitori di servizi di comunicazione elettronica adottato dall'Autorità in data 15 dicembre 2005 (di seguito "provvedimento 15 dicembre 2005", in *www.garanteprivacy.it*, doc. *web* n. 1203890);

Vista la nota del 3 luglio 2006 con la quale Vodafone Omnitel N.V. (di seguito "Vodafone") ha fornito riscontro alla richiesta dell'Autorità di comunicare le misure e gli accorgimenti adottati in conformità al predetto provvedimento;

Visto l'ulteriore provvedimento adottato dal Garante il 20 settembre 2006, con il quale l'Autorità ha prorogato di novanta giorni il termine per l'integrale adozione delle misure e degli accorgimenti indicati nel provvedimento 15 dicembre 2005 che, allo stato, non risultavano attuati. Ciò, nei termini indicati nel prospetto riassuntivo del 19 settembre 2006 per la parte attinente a Vodafone (in *www.garanteprivacy.it*, doc. *web* nn. 1341009 e 1348670);

Vista la nota del 22 dicembre 2006 con la quale la società ha fornito riscontro in merito all'adeguamento alle predette prescrizioni;

Vista la nota del 7 febbraio 2007 con la quale l'Autorità ha preso atto delle dichiarazioni rese per conto della società, rilevanti anche sul piano della responsabilità penale ai sensi dell'art. 168 del Codice;

Vista l'ulteriore nota del 23 novembre 2007 con la quale, per conto della società, sono state rese ulteriori dichiarazioni ai fini del rispetto della normativa sulla protezione dei dati personali, con riferimento ai trattamenti svolti per finalità di accertamento e repressione dei reati;

Vista la documentazione in atti;

Visto l'art. 154, comma 1, lett. *c*) 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 dott. Giuseppe Fortunato;

Premesso:

Nel 2006 il Garante ha deliberato un programma ispettivo nei confronti 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 tre accertamenti ispettivi sui sistemi utilizzati per la predetta finalità dall'operatore di telefonia mobile Vodafone, in data 4 ottobre 2006, nel periodo 4–6 dicembre 2006 e nel periodo 6–8 febbraio 2007.

Sistemi utilizzati per l'"area magistratura"
Dalle risultanze istruttorie è emerso che la società effettua trattamenti dei dati di traffico per finalità di accertamento e repressione dei reati tramite un'area operativa dedicata (c.d. "area magistratura") che si occupa di gestire le richieste dell'autorità giudiziaria volte all'acquisizione di dati anagrafici dei clienti e di dati di traffico telefonico e telematico, nonché all'attivazione di intercettazioni telefoniche e telematiche.

In particolare, all'interno di tale area, il sistema preposto all'acquisizione, alla gestione e alla comunicazione delle richieste provenienti dall'autorità giudiziaria concernenti sia i dati di traffico storico, sia le intercettazioni, è denominato *Sds Web*.

I sistemi informativi che contengono i dati di traffico storico risultano essere:

- *Rts*, recante i dati di traffico telefonico mobile;

- *Ecs*, contenente i dati di traffico telematico mobile.

Per quanto riguarda la semplice richiesta di dati anagrafici risulta utilizzata l'applicazione denominata *Ag-Web*.

Per ciò che concerne l'attivazione delle intercettazioni telefoniche e telematiche (deviazione del traffico verso i punti di ascolto), risulta utilizzato il sistema *Modico Md-Cts*, attraverso le sue componenti:

- *Df2g*, apparato deviatore di traffico telefonico;
- *Lig*, apparato deviatore di traffico telematico;
- *Tec*, banca dati nella quale viene tenuta traccia delle utenze oggetto di intercettazione sia telefonica sia telematica, nonché dei corrispondenti punti di ascolto; tramite la stessa viene anche realizzato il controllo e la configurazione delle prestazioni sugli apparati *Df2g* (*provisioning*).

Risultanze istruttorie
Al fine di una completa analisi delle risultanze istruttorie è necessario dare in primo luogo sintetica evidenza, nel presente provvedimento, dei numerosi e complessi accertamenti ispettivi e, in secondo luogo, delle ulteriori dichiarazioni rese da ultimo per conto della società, con nota del 23 novembre 2007, con la quale si è attestata l'adozione di alcune significative implementazioni che hanno determinato il superamento di talune criticità in precedenza riscontrate.

Nella seguente lettera A) vengono riassunti i soli profili critici emersi negli accertamenti ispettivi che riguardano: l'adozione delle misure minime di sicurezza, il rispetto delle prescrizioni impartite con il provvedimento 15 dicembre 2005 e, più in generale, della normativa in materia di protezione dei dati personali. Nella successiva lettera B) vengono invece analizzate le implementazioni adottate dalla società e comunicate con la predetta nota del 23 novembre 2007. Di seguito, sono formulate alcune valutazioni conclusive sulla base dell'esame congiunto di tutti i predetti aspetti.

A) Criticità rilevate nel corso degli accertamenti ispettivi.
Nel corso degli accertamenti ispettivi è stata riscontrata la mancata attuazione di alcune misure minime di sicurezza e, segnatamente, l'omesso aggiornamento del documento programmatico sulla sicurezza (dps), l'utilizzo di credenziali di accesso condivise, nonché di *password* non soggette a scadenza.

Su tale profilo, l'Autorità ha avviato un separato procedimento e ha già trasmesso gli atti alla competente autorità giudiziaria, con nota del 10 settembre 2007, inoltrata ai sensi e per gli effetti di cui all'art. 169 del Codice.

* * *

Inoltre, sono emerse alcune carenze con riferimento all'adeguamento alle prescrizioni impartite dal Garante con il provvedimento 15 dicembre 2005. In particolare, si sono potute rilevare:

1. la comunicazione per mezzo di posta elettronica non certificata
Nel corso degli accertamenti è emerso che la società si è dotata dal 23 dicembre 2006 di indirizzi di posta elettronica certificata (*Pec*).

Si è rilevato, inoltre, che le richieste dell'autorità giudiziaria risultano prevalentemente pervenire tramite posta elettronica non certificata transitando, quindi, attraverso sistemi non sicuri. Le risposte della società agli uffici giudiziari risultano, invece, inviate sempre attraverso il sistema di posta elettronica certificata (*Pec*). Tuttavia, nell'ipotesi in cui i destinatari non utilizzino la posta elettronica certificata, la società chiede loro di emettere un apposito provvedimento che autorizzi un nuovo inoltro degli esiti di quanto richiesto, in deroga alle prescrizioni impartite con il provvedimento 15 dicembre 2005 (come risulta dal verbale delle operazioni compiute l'8 febbraio 2007);

2. la mancanza di *log* di tracciamento delle operazioni e l'inaffidabilità delle registrazioni
Per quanto riguarda il sistema *Rts* (contenente i dati di traffico telefonico mobile) è emerso che le operazioni effettuate da amministratori di sistema o da amministratori di basi di dati non risultano adeguatamente tracciate (come risulta dall'allegato al verbale delle operazioni compiute a Corsico (Mi) il 7 febbraio 2007).

Analogamente, in relazione al sistema operativo, i *file* di tracciamento risultano modificabili dagli amministratori di sistema (come emerge dall'ultimo documento citato).

Per quanto riguarda il sistema *Modico Md-Cts* (che consente la deviazione del traffico verso i punti d'ascolto), è emersa la possibilità di attivare le intercettazioni telefoniche anche agendo direttamente su apparati di rete e sistemi di gestione potendo, pertanto, eludere le procedure di *audit* previste per detto sistema (come risulta dal verbale delle operazioni compiute a Milano il 6 febbraio 2007);

3. l'assenza di procedure di cifratura dei dati giudiziari
Dagli accertamenti è emersa, inoltre, l'assenza di procedure di cifratura dei dati giudiziari. A tal riguardo, si è rilevato che in alcuni sistemi i dati di traffico telefonico o telematico o riguardanti le utenze sotto intercettazione non sono sottoposti a cifratura e sono, quindi, visualizzabili agli operatori o agli amministratori. In particolare, per:

- *Rts*: i dati di traffico telefonico sono cifrati solo nel momento della loro trasmissione agli uffici giudiziari e non anche nella fase di loro presenza nel sistema informatico;
- *Ecs*: i dati di traffico telematico non sono sottoposti a cifratura e sono visualizzabili con l'indicazione di indirizzi Ip e numeri telefonici (come risulta dal verbale delle operazioni compiute in Milano il 7 febbraio 2007);
- *Df2g*: i file vocali, temporaneamente memorizzati nel sistema a causa dell'indisponibilità del punto di ascolto, non sono sottoposti a cifratura, ma gli stessi sono codificati in un formato della Urmet (come risulta dal verbale delle operazioni compiute in Milano il 6 febbraio 2007);

- *Tec*: i dati presenti non sono cifrati, ma vi è un'iniziativa aziendale in corso rivolta alla cifratura (come risulta dal verbale delle operazioni compiute l'8 febbraio 2007).

* * *

Dagli accertamenti ispettivi sono emerse, poi, ulteriori criticità. In particolare, si sono potute rilevare:

4. la conservazione di dati di traffico telematico in violazione dell'art. 132 del Codice
Nel corso degli accertamenti (come risulta dal verbale delle operazioni compiute in Milano il 7 febbraio 2007) è stato verificato il funzionamento del sistema che contiene i dati di traffico telematico trattati per scopi di accertamento e repressione di reati (sistema *Ecs*). In particolare è emerso che:

- nel sistema *Ecs* sono conservati solo i dati relativi al traffico telematico dei clienti che usano *connect card* Vodafone o il telefono mobile come *modem* per la navigazione in Internet;
- il sistema *Ecs* effettua la correlazione tra l'indirizzo Ip assegnato al numero del cliente che attiva la connessione e l'indirizzo Ip di destinazione;
- in tale sistema sono registrati l'indirizzo Ip dell'origine della comunicazione associato al numero del cliente Vodafone (Msisdn-*Mobile Station Integrated Services Digital Network*), la data, l'ora e la durata della comunicazione, nonché l'indirizzo Ip di destinazione e il numero di porta;
- non è raccolta la *Url* di destinazione;

5. l'assenza di alcuna indicazione di tempi di conservazione dei dati anagrafici estratti per prestazioni obbligatorie non remunerate
Il sistema *Ag-Web*, preposto all'acquisizione, gestione e comunicazione di dati anagrafici relativi a prestazioni obbligatorie non remunerate conserva tali dati, estratti dai sistemi della società, per il periodo in cui sono messi a disposizione dell'ufficio giudiziario richiedente, pari a tre mesi (come risulta dal verbale delle operazioni compiute il 5 dicembre 2006). Successivamente, una volta fornito il riscontro all'organo procedente, la richiesta e la risposta vengono conservate a tempo indeterminato in un'apposita banca dati, non essendo stati ancora determinati i tempi di conservazione;

6. la vulnerabilità dei sistemi *server* e i flussi di trasmissione dati non sicuri.
Su alcuni sistemi *server* utilizzati nell'area magistratura a supporto delle applicazioni indicate, sono state riscontrate carenze di configurazione e prassi d'uso inidonee di seguito elencate:

- *Sds-Web*: ricorso a protocolli *web* non cifrati (*http*) in luogo di connessioni sicure Ssl (come risulta dall'allegato al verbale delle operazioni compiute l'8 febbraio 2007);
- *Rts*: attivazione di servizi di rete Tcp/Ip non necessari e non cifrati (come risulta dal verbale delle operazioni compiute in Corsico (Mi) il 7 febbraio 2007);
- *Ecs*: configurazione di meccanismi di equivalenza tra utenze che consentono l'accesso a utenze privilegiate (c.d. diritti di *super user*) e attivazione di servizi di rete Tcp/Ip non necessari e non cifrati (come risulta dal verbale delle operazioni compiute in Milano il 7 febbraio 2007);
- *Df2g*: accessibilità con protocolli Tcp/Ip non sicuri (come risulta dal verbale delle operazioni compiute in Milano il 6 febbraio 2007);
- *Lig*: attivazione di servizi di rete Tcp/Ip non necessari e non cifrati e insicura modalità di trasmissione degli *mms* (come risulta dal verbale delle operazioni compiute in Milano il 7 febbraio 2007);
- *Tec*: attivazione di servizi di rete Tcp/Ip non necessari e non cifrati e accesso interattivo al sistema con protocollo insicuro e con utenze privilegiate (c.d. *super user*) (come risulta dal verbale delle operazioni compiute l'8 febbraio 2007).

B) Dichiarazioni rese successivamente agli accertamenti ispettivi
Con nota del 23 novembre 2007, la società ha reso da ultimo alcune dichiarazioni ai fini della verifica dell'attuale rispetto della normativa in materia di protezione dei dati personali con riferimento ai trattamenti svolti nell'area magistratura.

Dall'analisi di tali nuovi elementi emergono alcune modifiche alle misure e agli accorgimenti adottati a protezione dei dati personali trattati nell'ambito dei sistemi dell'area magistratura.

L'idoneità delle misure e degli accorgimenti adottati in ottemperanza alle prescrizioni impartite da questa Autorità a seguito della contestazione della violazione delle misure minime di sicurezza deve essere invece effettuata in altra sede, da questa Autorità e dall'autorità giudiziaria, stante la pendenza di un procedimento penale.

Per gli altri profili, in questa sede va preso quindi atto delle dichiarazioni rese per conto della società, rilevanti anche ai fini della responsabilità penale ai sensi dell'art. 168 del Codice, in ordine solo ai seguenti aspetti:

- **cifratura dati**: sono stati cifrati i *database* dei seguenti sistemi: *Sds*, *Rts*, *Ag-Web*, *Mdcts*, *Tec*, *Df2g*; sono stati altresì cifrati i *file* dei seguenti sistemi: *Tec*, *Lig*, *Df2g*;
- ***user access mangement***: "*tutti i sistemi rilevanti per le attività di AG sono stati integrati con il workflow aziendale (Uam) di autorizzazione e revisione dei diritti di accesso degli utilizzatori. Questo permette il monitoraggio del personale che per ragioni inerenti la propria attività accede ad informazioni riconducibili alla categoria "banca dati giudiziaria*" *consentendo ai responsabili una verifica periodica*";
- **messa in sicurezza dei canali di accesso ai sistemi**: "*l'autenticazione a tutti i sistemi AG avviene dietro procedure di strong authentication, sviluppate mediante l'utilizzo di certificati digitali e* username *nominative. Per rafforzare maggiormente la protezione di tali sistemi, entro il primo semestre del 2008, salvo imprevisti tecnici, per poter autenticarsi ed accedere alle interfacce applicative dovranno utilizzare una connessione via VPN, la quale permette di cifrare il traffico passante tra la postazione* client *dell'utilizzatore ed il* server";
- **interfaccia applicativa unica**: "*tutte le attività legate all'erogazione delle prestazioni obbligatorie sono gestite utilizzando un unico sistema, SDS-Web, che consente una maggiore verifica delle attività svolte dagli incaricati autorizzati al trattamento dei dati giudiziari. Su tale sistema, in esercizio già dal mese di dicembre 2006, sono state implementate le misure di cifratura e logging delle attività svolte dagli utenti applicativi*";
- **adeguamento applicativo online per richieste dell'autorità giudiziaria**: il sistema Ag-Web consente all'autorità giudiziaria di accedere in modo sicuro (*https*), tramite un'interfaccia *web*, a un portale per l'invio e la ricezione delle anagrafiche dei clienti. Il *database* di tale sistema, contenente i *log* delle richieste da parte degli

ufficiali di polizia giudiziaria è stato cifrato in modo da non rendere disponibili tali informazioni al personale tecnico; tale soluzione è operativa dal mese di febbraio 2007;

- **adeguamento sistema tracciamento navigazione *web* (clienti)**: "*il sistema Ecs consente il tracciamento dei dati di navigazione internet effettuata dai clienti tramite rete mobile, effettuando una correlazione tra Msisdn, indirizzo Ip sorgente (assegnato dalla società al cliente) ed indirizzo Ip destinatario. È in corso di sviluppo un'iniziativa che prevede la cifratura del database, con rilascio operativo programmato, salvo imprevisti tecnici, per la fine di aprile 2008*";
- **adeguamento sistema *Tec, Lig* e *Rts***: "*gli adempimenti (gestione degli accessi, delle credenziali e del* logging*) alle prescrizioni notificate in data 25 settembre 2007 relativi ai sistemi indicati sono stati implementati*".

Valutazione delle risultanze istruttorie
Dall'esame complessivo delle risultanze istruttorie e tenuto conto, in particolare, delle dichiarazioni da ultimo rese con la predetta nota del 23 novembre 2007, emerge attualmente un quadro di sostanziale adeguamento alle prescrizioni impartite con il provvedimento 15 dicembre 2005, fatta eccezione per la mancanza di *log* di tracciamento delle operazioni e l'inaffidabilità delle registrazioni. Ciò, ferme restando, da un lato, la non liceità della prassi adottata volta a richiedere all'autorità giudiziaria l'adozione di un apposito provvedimento per autorizzare l'inoltro degli esiti di quanto richiesto in "deroga" alle prescrizioni del provvedimento 15 dicembre 2005 e, dall'altro, la necessità per il Garante di acquisire ulteriori elementi conoscitivi in merito alla dichiarata adozione di strumenti di cifratura dei dati trattati nell'area magistratura. Tali elementi dovranno pervenire a questa Autorità entro e non oltre sessanta giorni dalla ricezione del presente provvedimento.

L'Autorità si riserva di acquisire ulteriori elementi conoscitivi in relazione ai dichiarati aggiornamenti relativi a strumenti di *strong authentication*, che allo stato non risultano ancora completati.

Sotto diverso profilo, si dà atto che la società, sebbene dagli accertamenti ispettivi non risultava aver adottato alcune misure minime di sicurezza, ha dichiarato da ultimo di aver adempiuto alle prescrizioni relative alla gestione degli accessi, delle credenziali e del *logging* (come risulta dalla nota del 23 novembre 2007).

* * *

Tuttavia, dagli accertamenti ispettivi compiuti sono emerse ulteriori criticità con riferimento ad altri aspetti della normativa in materia di protezione dei dati personali (indicati nei punti da 4 a 6) e riguardanti specificamente: la conservazione di dati di traffico telematico in violazione dell'art. 132 del Codice, l'assenza di ogni indicazione di tempi di conservazione dei dati anagrafici estratti per prestazioni obbligatorie non remunerate, nonché la vulnerabilità dei sistemi *server* e flussi di trasmissione dati non sicuri.

Con riferimento a tali criticità, questa Autorità ravvisa la necessità di porvi rimedio e prescrive pertanto a tal fine, con il presente provvedimento, l'adozione da parte della società di misure e accorgimenti da adottare a garanzia degli interessati, di seguito indicati nel dispositivo, entro il termine che risulta congruo stabilire in sessanta giorni dalla ricezione del presente provvedimento.

* * *

Con riguardo all'accertata conservazione di dati di traffico telematico in violazione dell'art. 132 del Codice, va disposto il divieto dell'ulteriore trattamento di tali dati, con la conseguente cancellazione al più presto, da documentare a questa Autorità entro il termine che appare congruo stabilire in sessanta giorni dalla data di ricezione del presente provvedimento.

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).

Dall'esame delle risultanze istruttorie dei predetti accertamenti relativi al sistema *Ecs*, nonché dall'analisi della documentazione in atti, è invece emerso che Vodafone, nel fornire il servizio di accesso alla rete Internet, effettua un trattamento di dati di traffico telematico ulteriori rispetto a quelli necessari per l'instradamento della comunicazione o per la sua fatturazione, come sopra specificati. Ciò, anche con riferimento a siti esterni, rispetto ai quali la società agisce da mero intermediatore della connessione, ovvero 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 capillare, interessando tutti gli utenti Vodafone che usano *connect card* o il telefono mobile come *modem* per la navigazione in Internet.

Alla luce dei princìpi sopra indicati non risulta lecita e deve, pertanto, essere oggetto di divieto la conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche quando esse siano specificate 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.

* * *

L'Autorità si riserva ogni eventuale ulteriore determinazione anche a seguito delle informazioni ulteriori che la società dovrà inviare all'Autorità entro il predetto termine di sessanta giorni.

TUTTO CIÒ PREMESSO IL GARANTE

A) ai sensi dell'art. 154, comma 1, lett. *d*) del Codice dispone, nei termini di cui in motivazione, nei confronti di Vodafone Omnitel N.V., società del gruppo Vodafone Group Plc., con sede in Ivrea (TO), via Jervis n. 13, il divieto dell'ulteriore trattamento, in qualsiasi forma e grado di dettaglio, di dati personali relativi ai siti *web* visitati dagli utenti, anche quando tali dati siano specificati con mero indirizzo Ip di destinazione; dispone, per l'effetto, 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;

B) ai sensi dell'art. 154, comma 1, lett. *c*) del Codice, prescrive a Vodafone Omnitel N.V.:

1. in relazione all'adeguamento alle prescrizioni impartite con il provvedimento adottato dal Garante in data 15 dicembre 2005:

- di adottare, con riferimento alla comunicazione per mezzo di posta elettronica non certificata, "*tecniche di firma digitale per la cifratura dei documenti*", di utilizzare esclusivamente "*strumenti di cifratura basati su firma digitale per la comunicazione all'autorità giudiziaria dei risultati dell'attività strumentale svolta*", nonché di utilizzare la "*posta elettronica Internet esclusivamente nella forma della posta elettronica certificata (Pec)*" (*cfr*. prescrizione di cui alla lett. *b*) punti 2, 3 e 4);
- di adottare, con riferimento alla mancanza di *log* di tracciamento delle operazioni e inaffidabilità delle registrazioni, misure e accorgimenti compatibili con quanto previsto dal predetto provvedimento con riferimento all'adozione di "*strumenti informatici idonei ad assicurare il controllo delle attività svolte da ciascun incaricato sui singoli elementi di informazione presenti nei database utilizzati, con registrazione delle operazioni compiute in un apposito* audit log", (*cfr*. prescrizione di cui alla lett. *c*) punto 1), chiarendo se la dichiarata implementazione dei sistemi *Tec*, *Lig* e *Rts* si estenda agli altri sistemi utilizzati nell'area magistratura, trasmettendo idonea documentazione anche tecnica a supporto delle dichiarazioni rese;
- di chiarire, con riferimento all'assenza di procedure di cifratura dei dati giudiziari nel sistema *Li-Ims*, se, e in quali termini, la dichiarata implementazione di strumenti di cifratura sia compatibile con quanto prescritto nel citato provvedimento in merito all'adozione di "*moderni strumenti di cifratura per la protezione dei dati nel periodo di loro presenza nel sistema informativo del fornitore*" (*cfr*. prescrizione di cui alla lett. *c*) punto 2), trasmettendo idonea documentazione, anche tecnica, a supporto delle dichiarazioni rese;

2. in relazione alle ulteriori criticità rilevate nel corso degli accertamenti ispettivi:

- di adottare, con riferimento all'assenza di ogni indicazione di tempi di conservazione dei dati anagrafici estratti per prestazioni obbligatorie non remunerate, una disciplina interna che contenga l'indicazione di un limite massimo di conservazione dei medesimi dati, nel rispetto dei principi di finalità, di pertinenza e di non eccedenza (art. 11 del Codice), analogamente a quanto previsto dalla prescrizione indicata nel provvedimento del 15 dicembre 2005, relativa alla *"limitazione della persistenza dei dati personali a quanto strettamente necessario per attuare i provvedimenti dell'autorità giudiziaria, prevedendone la cancellazione immediatamente dopo la loro corretta comunicazione all'autorità giudiziaria richiedente"* (*cfr*. lett. *c*) punto 3);
- di adottare, con riferimento alla vulnerabilità dei sistemi *server* e flussi di trasmissione di dati non sicuri, le misure e gli accorgimenti necessari per disabilitare, relativamente ai sistemi operativi e alle basi di dati, la possibilità di accesso interattivo o tramite *web* con protocolli insicuri;

C) ai sensi dell' art. 154, comma 1, lett. *c*) del Codice, prescrive a Vodafone Omnitel N.V. di adottare le misure e gli accorgimenti di cui alla lettera B) entro il termine di sessanta giorni dalla data di ricezione del presente provvedimento, dando riscontro entro lo stesso termine a questa Autorità dell'avvenuto adempimento.

Roma, 10 gennaio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

stampa **chiudi**