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. 1484695]
[V. Provv. generale 17 gennaio 2008]

Prescrizioni sulla conservazione dei dati di traffico (Wind) - 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 27 giugno 2006 con la quale Wind telecomunicazioni S.p.A. (di seguito "Wind") 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 Wind (in *www.garanteprivacy.it*, doc. *web* nn. 1341009 e 1348670);

Vista la nota del 20 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 5 novembre 2007 con la quale, per conto della società, sono state rese ulteriori dichiarazioni e si è prodotta nuova documentazione 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 Chiaravalloti;

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 due accertamenti ispettivi sui sistemi utilizzati per la predetta finalità da Wind, in data 15 novembre 2006 e nel periodo dal 14 al 26 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, la società risulta utilizzare i seguenti sistemi informativi:

- *Cdct*, recante dati di traffico telefonico e telematico;
- *Dbag*, che comprende le anagrafiche;

Traffico storico Infostrada, contenente i dati di traffico relativi ai clienti di telefonia fissa Infostrada, raccolti antecedentemente alla fusione per incorporazione di Infostrada con Wind avvenuta nel 2001.

L'accesso a queste banche dati avviene tramite un "sistema portale magistratura" denominato *Magiportal*, che consente di effettuare tutte le operazioni di configurazione delle prestazioni obbligatorie da eseguire, utilizzando a valle una serie di sistemi *hardware* e *software* con specifiche funzionalità, fra i quali il sistema *Rational* per la protocollazione delle richieste provenienti dalle autorità competenti.

Il sistema *Cdct* è suddiviso al suo interno in più "istanze" dedicate allo svolgimento di diverse funzioni:

- l'istanza *Magiport* contiene i dati comuni a tutti gli ambiti funzionali (anagrafica, traffico, intercettazione) e i dati relativi a: decreto che dispone l'intercettazione, procedimento penale, utenza sottoposta a intercettazione, numero del centro di ascolto, numero registro intercettazioni telefoniche e tutti gli indirizzi *e-mail* dei destinatari cui sono inviati i tracciamenti *mms*;
- l'istanza *Maginter* riporta i dati relativi a: *e-mail*, *target*, procedimento penale, numero telefonico del punto di ascolto, numero telefonico intercettato, indirizzi *e-mail* dei destinatari, Rit (numero di protocollo del registro intercettazioni);
- l'istanza *Magiserv* reca esclusivamente le configurazioni inerenti al sistema (non dati di traffico);
- l'istanza *Anaprod* contiene le anagrafiche dei clienti Wind e Infostrada;
- l'istanza *Magiprod* è il *database online* del traffico.

Per quanto riguarda l'attivazione delle intercettazioni telefoniche (deviazione del traffico dalle utenze verso i punti di ascolto) per le utenze mobili, risultano essere utilizzati i seguenti sistemi:

- *Ims Formatter,* applicazione che permette l'attivazione delle intercettazioni;
- *Ccd,* deviatore di traffico, che effettua la duplicazione del traffico fonico verso un punto di ascolto;
- *Saidt*, applicazione che permette l'invio di dati di tracciamento.

Per quanto riguarda l'attivazione delle intercettazioni telefoniche per le utenze fisse risultano utilizzati i seguenti sistemi:

- *Dfd,* sistema attraverso il quale è possibile attivare manualmente sulle centrali di rete le intercettazioni;
- *Xvision,* applicazione che permette di collegarsi alla specifica centrale sulla quale è attestata l'utenza da intercettare.

Per quanto riguarda l'attivazione delle intercettazioni telematiche risultano utilizzati i seguenti sistemi:

- *Lidas,* sistema che permette l'estrazione dei dati di traffico telematico e contiene la parte propedeutica all'attivazione delle intercettazioni telematiche, a sua volta composto dai sottosistemi *Sdg* (applicazione che effettua la deviazione del traffico telematico) e *Sitrad* (sistema di *mediation*).

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, dell'ulteriore documentazione prodotta, nonché delle dichiarazioni rese da ultimo per conto della società, con nota del 5 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 5 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 12 giugno 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. l'assenza di meccanismi di *strong authentication* per l'accesso ai sistemi
Nei sistemi di intercettazione telematica (*Sdg*) e di telefonia mobile (*Ims Formatter*) non risultano presenti meccanismi di autenticazione "forte". Inoltre, in relazione al sistema di estrazione di tabulati di traffico telefonico e telematico (sistema *Cdct*), solo alcune utenze sono già sottoposte a *strong authentication* (come risulta dai verbali delle operazioni compiute il 21 febbraio 2007 e il 26 febbraio 2007 con l'allegata *"Scheda Rilevamento Sistema-Magistratura Interc."*);
2. l'uso condiviso di *password* per l'apertura dei tabulati di traffico
La *password* di protezione dei *file* compressi, contenenti i tabulati inviati all'autorità giudiziaria, è comune per tutti i destinatari e viene modificata periodicamente (come risulta dal verbale delle operazioni compiute il 16 febbraio 2007);
3. la mancanza di tracciamento delle singole operazioni per il sistema *Cdct* e l'assenza di ogni tracciamento per il sistema di intercettazione di telefonia fissa *Dfd*
Per quanto riguarda il sistema *Cdct*, risultano presenti solo *log* di *auditing* di accesso a tale banca dati, contenenti la data e l'ora di "entrata" e di "uscita" (come risulta dal verbale di operazioni compiute il 19 febbraio 2007 e dalla *"Scheda rilevamento sistema-Magistratura Cdct"* allegata al verbale delle operazioni compiute il 26

febbraio 2007), mentre le operazioni svolte dagli incaricati non risultano tracciate. Per quanto riguarda il sistema di intercettazione di telefonia fissa (sistema *Dfd*), la società ha precisato che non è possibile estrarre i *file* di *log* in quanto il sistema non consente la memorizzazione di alcuna operazione (come risulta dal verbale delle operazioni compiute il 15 febbraio 2007);

4. l'assenza di strumenti di cifratura dei dati giudiziari

Con riferimento alle banche dati contenenti i tabulati di traffico telefonico e telematico (sistema *Cdct*) e le anagrafiche dei clienti (sistema *Dbag*), che i dati non sono cifrati, né altrimenti protetti con strumenti di cifratura (come risulta dal verbale delle operazioni compiute il 19 febbraio 2007). Inoltre, con riferimento alle banche dati contenenti le informazioni relative alle intercettazioni, è emerso che, per quanto riguarda il traffico telematico (sistema *Sdg*), i dati non sono cifrati; per quanto concerne, invece, il traffico telefonico fisso e mobile, i dati risultano visibili agli amministratori delle banche dati.

* * *

Dagli accertamenti ispettivi sono emerse, poi, ulteriori criticità. In particolare, si è rilevato:

5. la mancata previsione di un limite temporale di conservazione dei dati relativi alle richieste di intercettazione.

Il sistema *Magiportal* contiene tutte le operazioni effettuate su richiesta dell'autorità giudiziaria che sono conservate indistintamente. In tale sistema, l'istanza *Maginter* conteneva, specificamente, i dati relativi alle intercettazioni a partire dal 14 novembre 2002 (come risulta dal verbale delle operazioni compiute il 23 febbraio 2007). I dati relativi alle intercettazioni telematiche erano inseriti anche nel sistema *Rational* che aveva uno storico a partire dal 2001 (come risulta dal verbale delle operazioni compiute il 16 febbraio 2007);

6. l'assenza di meccanismi di verifica della corrispondenza fra i dati inseriti sui sistemi di protocollazione e quelli contenuti sui sistemi di attivazione delle intercettazioni

In relazione ai sistemi di protocollazione e attivazione delle richieste di intercettazione, la società ha dichiarato che non è allo stato, attiva una procedura per la "riconciliazione" ossia per l'allineamento dei dati presenti su *Magiportal* e quelli contenenti sui sistemi di protocollazione, con quelli rinvenibili sui sistemi di attivazione delle intercettazioni, ma che la stessa procedura sarebbe stata disponibile a breve (come risulta dai verbali delle operazioni compiute il 15 e il 16 febbraio 2007);

7. l'utilizzo di *e-mail* insicure per l'invio di comunicazioni con i fornitori in *outsourcing*, anche per i dati relativi alle intercettazioni

A seguito dell'attivazione dell'intercettazione gli incaricati del trattamento inviano una *e-mail* contenente i dati della richiesta (estratto del decreto, utenza da intercettare, punto di ascolto laddove predeterminato) a un terzo soggetto, Resi s.r.l. (come risulta dal verbale delle operazioni compiute il 21 febbraio 2007), designata responsabile del trattamento. Per questa comunicazione risulta essere utilizzato un servizio di posta elettronica non certificato;

8. l'inserimento manuale della selezione del punto di ascolto

Il numero del punto di ascolto indicato nella richiesta è inserito manualmente dagli incaricati nei sistemi di intercettazione (relativi alla telefonia sia fissa, sia mobile): non è infatti presente nell'applicazione *software* una lista completa delle numerazioni assegnate ai servizi giudiziari;

9. la vulnerabilità dei sistemi *server* e i flussi di trasmissione dati non sicuri

Su molti sistemi *server* utilizzati nell'area magistratura per particolari elaborazioni sono state riscontrate carenze di configurazione e prassi d'uso inidonee. In particolare è emerso:

- a livello di sistemi operativi, l'utilizzo di protocolli di comunicazione non cifrati per la connessione, anche interattiva, ai sistemi dell'area magistratura (come risulta dai verbali delle operazioni compiute il 19 e il 23 febbraio 2007 sul sistema *Cdct* e il 22 febbraio 2007 per il flusso dei dati di traffico dalle centrali di commutazione ai predetti sistemi), nonché la possibilità di interazione con i sistemi *web* su connessioni non cifrate (come risulta dai verbali delle operazioni compiute il 16 febbraio 2007 sul sistema di protocollazione intercettazioni *Rational* e il 21 febbraio 2007 per la gestione del sistema *Cem*);
- a livello di banche dati, l'utilizzo di protocolli di comunicazione non cifrati per la connessione ai *database Oracle* dell'area magistratura (come risulta dal verbale delle operazioni compiute il 19 febbraio 2007).

B) Dichiarazioni e documentazione prodotte successivamente agli accertamenti ispettivi

Con nota del 5 novembre 2007, la società ha reso da ultimo alcune dichiarazioni e prodotto documentazione 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:

- **adozione di meccanismi di *strong authentication* per l'accesso ai sistemi**
  La società ha dichiarato che nei sistemi operativi per l'accesso alle funzionalità di intercettazione su rete Alcatel e sugli impianti *Dfd-Urmet* è stata introdotta una procedura di *strong authentication* mediante *token Rsa*; inoltre, ha rappresentato che un'analoga procedura di *strong authentication* è stata implementata per i sistemi *Lidas*, per il sistema *Saidt* e per le applicazioni *Ims* (come risulta dalla comunicazione del 15 ottobre 2007, allegata alla nota del 5 novembre 2007);
- **uso di *password* per le comunicazioni con le autorità competenti**
  La società ha dichiarato di aver realizzato un sistema di posta elettronica certificata (*Pec*) per le comunicazioni con le autorità competenti, cifrando i contenuti trasmessi tramite una *password* che viene comunicata al destinatario su un canale di comunicazione differente, individuato nel servizio *sms* su rete cellulare. La *password* viene generata a ogni invio e trasmessa al numero cellulare del referente (come risulta dal documento di fattibilità "*Notifica ricezione mail e invio avvenuta attivazione PG/AG*" del 4 ottobre 2007, allegato alla nota

Wind del 5 novembre 2007);

- **sistemi di tracciamento delle operazioni effettuate su tutte le piattaforme e per il sistema di intercettazione telefonia fissa**
  La società ha dichiarato di aver realizzato sistemi di *audit log* per il tracciamento delle attività sulle piattaforme dell'area magistratura dedicate alle intercettazioni su rete fissa. I *log* prodotti vengono stampati in forma cartacea, datati e siglati dal responsabile del servizio, nonché conservati in locali protetti (come risulta dal documento "*Istruzioni operative di accesso ai sistemi Intercetto e Dfd/Tec Funzione Lawful Data Services Security*" del 20 agosto 2007, allegato alla nota del 5 novembre 2007).

La società ha inoltre dichiarato che "*su tutte le piattaforme*" sono state attivate procedure di *logging* che tengono traccia dell'identificativo dell'incaricato che ha svolto l'attività; "*il log delle attività accessibile agli operatori autorizzati al servizio contiene i dettagli necessari all'espletamento delle attività loro affidate*"; infine, che "*è stato istituito comunque un registro delle attività sul quale ciascun operatore registra le attività svolte sapendo che dette attività sono state comunque* loggate" (come risulta dalla comunicazione del 15 ottobre 2007, allegata alla nota del 5 novembre 2007);

- **adozione di strumenti di cifratura dei dati giudiziari.**
  La società ha dichiarato che "*dal 24 agosto u.s. su tutti i sottosistemi e sulle sonde in esercizio dislocate sul territorio (…) si è implementata la crittografia dei dati, la profilazione utenti e il* logging *delle attività" e che "dagli inizi di settembre sono state rilasciate in esercizio: la* strong authentication *applicativa, la crittografia dei dati, la profilazione utenti,* logging *delle attività*" (come risulta dalla comunicazione del 15 ottobre 2007, allegata alla nota del 5 novembre 2007).

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 5 novembre 2007, emerge attualmente un quadro di sostanziale adeguamento alle prescrizioni impartite con il provvedimento 15 dicembre 2005, ferma restando la necessità 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 sessanta giorni dalla ricezione del presente provvedimento.

Sotto diverso profilo si dà atto che la società, pur se dagli accertamenti ispettivi non risultava aver implementato procedure di *business continuity* per l'area magistratura, ha dichiarato di aver adottato procedure di ripristino dei dati e dei sistemi compatibili con quanto stabilito dalla regola 23 dell'allegato B al Codice. Ciò, a fronte dell'analisi del rischio svolta con riferimento all'area magistratura, in base al disposto della regola 19.5 dello stesso allegato B (come risulta dal documento programmatico di sicurezza, aggiornato il 30 giugno 2007, allegato alla nota del 5 novembre 2007).

* * *

Tuttavia, dagli accertamenti ispettivi sono emerse ulteriori criticità con riferimento ad altri aspetti della normativa in materia di protezione dei dati personali (indicate nei punti da 5 a 9) e riguardanti specificamente: la mancata previsione di un limite temporale di conservazione dei dati relativi alle richieste di intercettazione; l'assenza di meccanismi per la verifica della corrispondenza tra i dati presenti nei sistemi di protocollazione e quelli inseriti nei sistemi di attivazione delle intercettazioni (c.d. "riconciliazione automatica"); l'utilizzo di *e-mail* insicure per lo scambio con Resi s.r.l.; l'inserimento manuale della selezione del punto di ascolto; la vulnerabilità dei sistemi *server* e i flussi di trasmissione 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.

* * *

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. *c*) del Codice, prescrive a Wind telecomunicazioni S.p.A., con sede legale in Roma, via Cesare Giulio Viola n. 48:

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

   - di chiarire se, e in quali termini, la dichiarata implementazione di strumenti di cifratura sia compatibile con quanto prescritto nel medesimo provvedimento del 15 dicembre 2005 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 da rendere;

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

   - di adottare, con riferimento alla mancata previsione di un limite temporale di conservazione dei dati relativi alle richieste di intercettazione, una disciplina interna che contenga l'indicazione di un limite massimo di conservazione dei medesimi dati, nel rispetto dei princìpi 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 comunicare, con riferimento all'assenza di meccanismi per la verifica della corrispondenza tra i dati presenti nei sistemi di protocollazione e quelli contenuti nei sistemi di attivazione delle intercettazioni (c.d. "riconciliazione automatica"), le modalità con le quali è stata adottata la dichiarata prevista procedura di "riconciliazione";
- di adottare, per l'interscambio di dati giudiziari con Resi s.r.l., con riferimento all'utilizzo di *e-mail* insicure, misure di sicurezza corrispondenti a quelle che il provvedimento 15 dicembre 2005 prevede per l'interscambio di "flussi informativi con l'autorità giudiziaria" (come risulta dalla lett. b) del citato provvedimento). Ciò, in particolare, mediante:
  - l'adozione di sistemi di comunicazione basati su aggiornati strumenti telematici sviluppati con protocolli di rete sicuri;
  - l'adozione di tecniche di firma digitale per la cifratura dei documenti;
  - l'utilizzo di strumenti di cifratura basati su firma digitale per la comunicazione dei risultati dell'attività strumentale svolta;
  - l'utilizzo della posta elettronica Internet esclusivamente nella forma della posta elettronica certificata (*Pec*);
  - il ricorso alla consegna manuale di documenti esclusivamente tramite soggetti delegati dal titolare, provvedendo alla tenuta di un apposito registro delle consegne;
  - la limitazione dell'uso dei mezzi di comunicazione meno sicuri ai soli casi di impossibilità tecnica di utilizzare i canali sicuri eventualmente già disponibili;

- di adottare, con riferimento all'inserimento manuale della selezione del punto d'ascolto dell'intercettazione, misure organizzative o tecniche che consentano di verificare la corrispondenza fra il numero telefonico inserito e quello indicato dall'autorità giudiziaria quale punto di ascolto;
- di adottare, con riferimento alle carenze di configurazione e alle prassi d'uso inidonee riscontrate su molti sistemi *server* utilizzati nell'area magistratura, 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;

B) ai sensi dell'art. 154, comma 1, lett. *c*) del Codice, prescrive a Wind telecomunicazioni S.p.A. di adottare le misure e gli accorgimenti di cui alla lettera A) 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
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

stampa **chiudi**