GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Prescrizioni e divieto del Garante [art. 154, 1 c) e d) del Codice] - 10 gennaio 2008 Bollettino del n. 90/gennaio 2008, pag. 0

[doc. web n. 1484726]
[V. Provv. generale 17 gennaio 2008]

Prescrizioni sulla conservazione dei dati di traffico (H3G) - 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 recante nuove misure di sicurezza presso i gestori per le intercettazioni 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 28 giugno 2006 con la quale H3G S.p.A. (di seguito "H3G"), 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 di pertinenza di H3G (in *www.garanteprivacy.it*, doc. *web* nn. 1341009 e 1348670);

Vista la nota del 28 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 20 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;

Visti 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. Mauro Paissan;

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 di cui all'art. 132, comma 5 del Codice. Nell'ambito di tale iniziativa sono stati svolti due accertamenti ispettivi sui sistemi utilizzati per tali finalità da H3G, in data 16 novembre 2006 e nel periodo dal 28 febbraio al 19 marzo 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 mediante un'area operativa dedicata (c.d. "area Arpo") che si occupa di gestire le richieste dell'autorità giudiziaria volte all'acquisizione di dati anagrafici dei clienti, 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:

- *Hts*, contenente dati di traffico telefonico e le anagrafiche;
- *Crs*, recante dati di traffico telematico.

L'accesso a queste banche dati avviene tramite un sistema di autenticazione denominato *Acume*.

Per quanto riguarda l'attivazione delle intercettazioni (deviazione del traffico verso i punti di ascolto) risulta essere utilizzato il sistema *L.i.* che comprende i seguenti sottosistemi:

- *Li-Ims,* che permette l'attivazione delle intercettazioni, l'invio alle centrali di commutazione delle istruzioni per duplicazione del traffico fonico verso un punto di ascolto e la creazione dei c.d. "cartellini di traffico" Iri-*Intercept Related Information.* Tale sistema è costituito da due *server* denominati *Ims* e *Eims*;
- *Iri-Handler,* che permette l'invio dei "cartellini di traffico" *Iri* ai punti di ascolto.

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 per conto della società con nota del 20 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 20 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
Con riferimento al rispetto delle misure minime di sicurezza si sono potute rilevare:

1. l'adozione di alcune misure per garantire il ripristino dell'accesso ai dati e ai sistemi dell'"area *Arpo*"
Al fine di migliorare la c.d. "*continuità del business*", le due macchine del sistema *Hts*, le due macchine del sistema *Iri-Handler* e quelle del sistema *Crs* sono, rispettivamente fra loro, in configurazione di *cold-standby.* Pertanto, i processi di ogni macchina di ciascun sistema sono replicati nell'altra e possono essere attivati manualmente se necessario (come risulta dalle schede tecniche relative a tali sistemi, allegate al verbale delle operazioni compiute il 19 marzo 2007).

* * *

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

2. la mancanza di *log* di tracciamento delle operazioni sistemistiche per il sistema di intercettazione *Li-Ims*
Nel corso degli accertamenti, la società ha dichiarato che la versione evoluta del sistema *Li-Ims*, in fase di implementazione, prevederebbe adeguamenti in termini di sicurezza relativi, fra l'altro, all'attivazione di *log* di accesso sistemistico al *database* contenuto nel *server Ims*, allo stato non disponibili (come risulta dal verbale delle operazioni compiute il 12 marzo 2007);

3. l'assenza di procedure di cifratura dei dati giudiziari nel sistema *Li-Ims*
Dagli accertamenti è emersa, inoltre, l'assenza di procedure di cifratura dei dati giudiziari nel sistema *Li-Ims*. A tal riguardo, la società ha dichiarato che l'implementazione della versione evoluta di tale sistema, in corso di realizzazione, potrebbe comportare anche la cifratura del *database* contenuto nel *server Ims*, al momento non disponibile (come risulta dal verbale delle operazioni compiute il 12 marzo 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 è stato verificato il funzionamento del sistema che contiene dati di traffico telematico trattati per scopi di accertamento e repressione di reati, c.d. sistema *Crs* (come risulta dal verbale delle operazioni compiute il 14 marzo 2007).

Nel corso di tale accertamento è emerso, in particolare, che:

- il sistema *Crs* opera mediante utilizzo di sonde le quali, dalle centrali, intercettano tutto il traffico telematico effettuato da utenti H3G;
- i dati di traffico raccolti dalle sonde non sono utilizzati da altri sistemi e confluiscono direttamente e unicamente nel *server Crs*;
- viene raccolta e conservata l'indicazione dell'*Msisdn* (*Mobile Station Integrated Services Digital Network*), dell'*Imsi* (*International Mobile Subscriber Identity*), della data di inizio e fine sessione, del protocollo di comunicazione utilizzato, del numero Ip e della porta del mittente e del destinatario, nonché, in caso di protocollo di comunicazione *http*, dell'*Url* completa, ovvero con il dettaglio delle singole pagine aperte dall'utente interessato;

5. l'assenza di verifica della corrispondenza fra attivazioni delle intercettazioni e decreti provenienti dall'autorità giudiziaria
Da alcune verifiche effettuate sui sistemi di intercettazione, è emersa la mancata adozione di una verifica della corrispondenza tra le effettive attivazioni delle intercettazioni e le correlative richieste riportate nel decreto dell'autorità giudiziaria (c.d. "riconciliazione automatica") (come risulta dal verbale delle operazioni compiute il 2 marzo 2007);

6. la presenza di un sistema di distribuzione nel trattamento non in linea con le disposizioni di cui agli artt. 28 e ss. del Codice
Dagli accertamenti e dalla documentazione prodotta è emerso che le designazioni effettuate ai sensi degli artt. 28 e ss. del Codice da H3G, in qualità di titolare del trattamento, non investono la totalità dei soggetti che operano nell'ambito dell'area Arpo per la gestione delle c.d. "prestazioni obbligatorie".

In particolare, risulta che H3G e un'altra società (Kelyan Smc S.p.A.) sono titolari autonomi del trattamento e che H3G ha designato quali "responsabili esterni" del trattamento Comdata S.p.A. e Ericsson telecomunicazioni S.p.A. (di seguito "Ericsson").

Per quanto riguarda tale seconda designazione, si è rilevato dal contratto di appalto di servizi stipulato tra le due società che H3G ha concordato con Ericsson che quest'ultima deve effettuare il trattamento *"scegliendo le modalità adeguate all'erogazione dei servizi"*. In tale contesto è emerso inoltre che Ericsson ha effettuato, in qualità di titolare, diverse altre designazioni nei confronti di soggetti individuati quali responsabili e incaricati del trattamento;

7. la vulnerabilità dei sistemi *server* e i flussi di trasmissione di dati non sicuri
Su alcuni sistemi *server*, utilizzati nell'area Arpo per particolari elaborazioni, sono state riscontrate carenze di configurazione e prassi d'uso inidonee. In particolare è emerso:

1. l'utilizzo di protocolli di comunicazione non cifrati per la connessione, anche interattiva, ad alcuni sistemi

dell'area Arpo (come risulta dai verbali delle operazioni compiute il 12 marzo 2007 sul sistema *Li-Ims* per le intercettazioni e dagli allegati denominati "Hts *Flussi in ingresso e uscita*" e "*Flussi Fisici*", forniti da H3G nel *cd rom* in data 3 aprile 2007). Nella stessa sede, la società ha tuttavia dichiarato che l'implementazione della versione evoluta del sistema *Li-Ims* avrebbe previsto adeguamenti in termini di sicurezza anche con riferimento ai protocolli di comunicazione e scambio dati sicuri (Ssh);

2. la possibilità di interazione con i sistemi *web* su connessioni non cifrate (come risulta dal predetto allegato denominato "*Flussi Fisici*" relativamente alle connessioni dei sistemi con l'applicazione *Acume*, nonché dal verbale delle operazioni compiute il 2 marzo 2007 per l'accesso *web* al sistema di traffico storico telematico *Crs*);
3. la possibilità di interazione con i sistemi *database* Oracle su connessioni non cifrate (come risulta dall'allegato denominato "Hts *Flussi in ingresso e uscita*", fornito da H3G nel citato *cd rom*).

B) Dichiarazioni rese successivamente agli accertamenti ispettivi
Con nota del 20 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 Arpo.

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 Arpo.

In questa sede va quindi preso 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:

- **aggiornamento del sistema Li-Ims**
  La società ha dichiarato che il sistema *Ims* è in fase di aggiornamento e avrebbe avuto una configurazione ridondante in "*hot stand-by*" entro la fine del 2007; ha dichiarato inoltre che lo stesso sistema è stato aggiornato dal punto di vista del *software* nel mese di maggio 2007, con l'introduzione di una *release* che "*ha superato la criticità rilevata*" nel corso degli accertamenti ispettivi in relazione alla visibilità, da parte dei sistemisti, dell'utenza *target* intercettata;
- **conservazione dei dati nel sistema *Iri-H***
  La società ha confermato che la conservazione dei dati inviati non supera le quarantotto ore;
- **re-ingegnerizzazione del sistema *Crs***
  La società ha attestato che il sistema *Crs* è in fase di re-ingegnerizzazione allo scopo di accrescere ulteriormente i livelli di sicurezza; il completamento del progetto è previsto entro la fine del primo semestre del 2008, anche in ragione della necessità di recepire eventuali indicazioni in ordine alla consistenza dei dati per prestazioni obbligatorie.

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 20 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 sistemistiche per il sistema di intercettazione *Li-Ims.* Resta ferma la necessità di acquisire ulteriori elementi conoscitivi in merito alla dichiarata adozione di strumenti di cifratura dei dati trattati nell'area Arpo. Tali elementi dovranno pervenire a questa Autorità entro e non oltre il termine di sessanta giorni dalla ricezione del presente provvedimento.

L'Autorità si riserva altresì di acquisire ulteriori elementi conoscitivi all'esito dei dichiarati aggiornamenti del sistema informatico *Crs,* che non risulta ancora completato.

Sotto diverso profilo si dà atto che la società, sebbene dagli accertamenti ispettivi non risultava aver implementato delle procedure di *business continuity* per l'area Arpo, ha dichiarato di avere in fase di aggiornamento il sistema *Li-Ims* che sarebbe stato configurato in "*hot stand-by*" entro la fine del 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 7) e riguardano specificamente: la conservazione di dati di traffico telematico in violazione dell'art. 132 del Codice, l'assenza di verifica della corrispondenza fra attivazioni delle intercettazioni e decreti provenienti dall'autorità giudiziaria, la presenza di un sistema di distribuzione delle responsabilità nell'ambito del trattamento non in linea con le disposizioni di cui agli artt. 28 e ss. del Codice, la vulnerabilità dei sistemi *server* e i 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 invece all'accertata conservazione di dati di traffico telematico in violazione dell'art. 132 del Codice, l'Autorità dispone il divieto dell'ulteriore conservazione 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 emerse dai predetti accertamenti relativi al sistema *Crs*, nonché dall'analisi della documentazione in atti, risulta che H3G, 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. 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 inoltre capillare, interessando tutti gli utenti H3G.

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 dati personali sui siti visitati dagli utenti, anche quando esse siano specificate con notazione *Url* o con mero indirizzo Ip di destinazione. I dati già trattati illecitamente dovranno essere cancellati al più presto dando riscontro a questa Autorità dell'avvenuta cancellazione entro, e non oltre, il termine che appare congruo stabilire in sessanta giorni dalla ricezione del presente provvedimento.

* * *

Un ulteriore aspetto riguarda il rispetto delle disposizioni del Codice relative ai soggetti che effettuano il trattamento nelle figure del titolare, responsabile e incaricato (disposizioni del titolo IV del Codice, artt. 28-30).

Dalle risultanze istruttorie emerge un quadro alquanto complesso di designazioni da parte non solo dell'effettivo titolare del trattamento (H3G), ma anche da parte di altri soggetti designati formalmente responsabili. Questi ultimi, in alcuni casi, svolgono trattamenti di dati personali in maniera del tutto autonoma e con il relativo potere decisionale divenendo, pertanto, di fatto titolari del trattamento, con conseguente facoltà di designazione di responsabili e incaricati. Il quadro così delineato risulta aggravato dall'affidamento in *outsourcing* alla Ensi S.p.A. (Ericsson Network Service Italia S.p.A.) della gestione e della manutenzione dei sistemi informativi e di rete di H3G, regolata da apposito contratto di cessione di ramo d'azienda del 1° aprile 2005 (come risulta dal verbale delle operazioni compiute il 16 novembre 2006).

In relazione a quanto detto, va prescritto alla società di porre rimedio alle designazioni impropriamente effettuate e di comunicare, entro il termine di sessanta giorni dalla ricezione del presente provvedimento, tutte le designazioni compiute, indicando le qualifiche di ciascun soggetto operante nell'ambito di applicazione del Codice e specificando chi riveste appropriatamente la qualifica di titolare, responsabile e incaricato del trattamento, fornendo la relativa documentazione.

* * *

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 H3G S.p.A., con sede legale in Trezzano sul Naviglio (MI), via Leonardo da Vinci n. 1, il divieto della conservazione, in qualsiasi forma e grado di dettaglio, di informazioni sui siti visitati dagli utenti, anche qualora esse siano specificate con notazione *Url* o 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 H3G S.p.A:

1. in relazione al rispetto delle misure minime di sicurezza indicate nell'allegato B al Codice:

   - di chiarire se le misure e gli accorgimenti adottati siano atti a garantire il ripristino dell'accesso ai dati e ai sistemi dell'area magistratura (c.d. area Arpo) in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e in tempi certi non superiori a sette giorni, così come prescritto dalla regola 23;

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

   - di adottare, con riferimento alla mancanza di *log* di tracciamento delle operazioni sistemistiche per il sistema di intercettazione *Li-Ims*, misure e accorgimenti compatibili con quanto previsto dal provvedimento in relazione 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), 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;

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

- di adottare, con riferimento all'assenza di verifica della corrispondenza fra attivazioni delle intercettazioni e decreti provenienti dall'autorità giudiziaria, misure organizzative o tecniche che consentano di verificare la corrispondenza fra il numero delle intercettazioni effettivamente attivate e quelle richieste con i decreti provenienti dall'autorità giudiziaria;
- di porre rimedio, con riferimento al rispetto delle prescrizioni di cui agli artt. 29 e 30 del Codice, alle designazioni impropriamente effettuate, indicando dettagliatamente chi rivesta la qualifica di titolare, responsabile o incaricato del trattamento, trasmettendo a questa Autorità la relativa documentazione;
- di adottare, con riferimento alle carenze di configurazione e alle prassi d'uso inidonee riscontrate su molti sistemi *server* utilizzati nell'area magistratura (c.d. "area Arpo"), 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 H3G S.p.A. 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
Paissan

IL SEGRETARIO GENERALE
Buttarelli

stampa **chiudi**