GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Nuove misure di sicurezza presso i gestori per le intercettazioni - 15 dicembre 2005

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;

VISTI gli accertamenti disposti dal Garante per verificare la liceità e la correttezza dei trattamenti di dati personali effettuati da fornitori di servizi di comunicazione elettronica per dare esecuzione a provvedimenti di intercettazione telefonica e telematica adottati dall'autorità giudiziaria;

VISTA la documentazione in atti;

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

RELATORE il prof. Francesco Pizzetti;

PREMESSO

Il 2 agosto 2005 il Garante ha avviato accertamenti nei confronti dei principali fornitori di servizi di comunicazione elettronica (di seguito, "fornitori") sulle modalità con le quali essi adempiono ai provvedimenti dell'autorità giudiziaria in materia di intercettazioni. Ciò, al fine di verificare la liceità e la correttezza dei trattamenti di dati in riferimento alla disciplina rilevante in materia di protezione dei dati personali, con particolare riguardo alle disposizioni a garanzia della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione.

Nell'ambito degli accertamenti, effettuati in conformità al predetto Codice con richiesta ai sensi del relativo art. 157, sono stati acquisiti presso i fornitori vari elementi necessari per il controllo sulle attività dagli stessi svolte a qualunque titolo per eseguire intercettazioni lecite (telefoniche, informatiche, telematiche o ambientali, anche di tipo preventivo: artt. 266 ss. e 226 disp. att. c.p.p.), o comunque correlate con le intercettazioni medesime.

Il 7 ottobre 2005 è stato disposto un supplemento di istruttoria, anche in riferimento alle operazioni svolte a supporto di attività investigative o di indagine in attuazione del recente d.l. n. 144/2005 sul contrasto al terrorismo. In questo quadro, sono stati esaminati anche i dati numerici delle richieste provenienti dall'autorità giudiziaria, inerenti al numero di intercettazioni che hanno avuto inizio e alla loro durata media, espressa in giorni, nonché al numero di tabulati forniti per la documentazione del traffico c.d. "storico".

OSSERVA

1. Intercettazioni telefoniche e telematiche

Il tema del trattamento dei dati connessi alle intercettazioni presso i fornitori riveste particolare delicatezza con riferimento alla sfera personale degli indagati (e delle altre persone estranee alle indagini, ma coinvolte nelle comunicazioni e conversazioni) e alla segretezza delle indagini.

L'esame dei vari profili, compreso quello della riservatezza dei dati e della sicurezza dei sistemi utilizzati per trattarli, è stato quindi condotto con particolare attenzione in considerazione dei diritti fondamentali delle persone interessate e degli interessi pubblici coinvolti.

Dagli elementi acquisiti e che i fornitori hanno prodotto sotto la propria responsabilità, anche penale, con riguardo alla genuinità di quanto attestato o documentato (art. 168 del *Codice-Falsità nelle dichiarazioni e notificazioni al Garante*), emerge che l'attività dei medesimi fornitori resta caratterizzata da una funzione strumentale rispetto a quanto disposto dall'autorità giudiziaria penale.

I fornitori hanno attestato di limitarsi a svolgere i soli adempimenti di carattere tecnico necessari a porre in essere le attività richieste dall'autorità giudiziaria (intercettazioni; fornitura di flussi di linee e circuiti; interruzione o sospensione di servizi; supporti tecnici per servizi di emergenza).

I medesimi fornitori hanno altresì attestato di non avere alcun accesso ai contenuti delle comunicazioni e delle conversazioni, anche temporaneo o mediante trascrizioni, a livello centrale o locale. Ciò, anche in quanto le medesime comunicazioni e conversazioni sono effettuate duplicando la linea di comunicazione dell'indagato e instradando la linea duplicata verso un c.d. *Cit* (Centro intercettazioni telefoniche), indicato dall'autorità giudiziaria richiedente e connesso ad una rete fissa. Le predette attività sono svolte senza intermediazione di terzi e -salvo che in alcuni casi di *roaming*- nei confronti solo degli utenti dei fornitori medesimi.

Pur non venendo a conoscenza dei predetti "contenuti", i fornitori raccolgono, selezionano, elaborano e trattano con altre operazioni una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali essi comunicano.

Si tratta di dati personali riservati e delicati che attengono, in particolare, all'identità dei soggetti sottoposti ad intercettazione, all'arco temporale di svolgimento dell'intercettazione e ai dati di traffico telefonico o telematico inerenti alle linee intercettate (data, ora, numero chiamato e durata della comunicazione o conversazione).

A seconda dei casi, tenendo conto delle specifiche richieste dell'autorità giudiziaria, i medesimi dati sono integrati da informazioni tecniche aggiuntive relative ai dettagli delle chiamate entranti, ai tentativi di chiamata in entrata o in uscita e ai i dati di localizzazione geografica dell'utenza intercettata. I fornitori di telefonia mobile tengono traccia anche dell'identificativo numerico della stazione base impegnata dall'utenza intercettata.

I servizi di messaggistica del tipo *sms/mms* sono compresi nelle attività di intercettazione; i fornitori hanno specificamente attestato di non avere alcuna possibilità di accedere, anche retroattivamente, al loro contenuto.

Tuttavia, una società (TIM Italia S.p.a.) ha espressamente specificato che, nei casi in cui il Cit non è dotato di risponditore idoneo a ricevere tali messaggi (risulta che ad oggi solo il 7% dei Cit ne disponga), alla documentazione di traffico viene abbinata la registrazione del testo del messaggio, per un tempo determinato. In tali casi, i messaggi vengono a volte archiviati dal fornitore, in forma cifrata, e successivamente trasmessi all'autorità giudiziaria richiedente. In questi stessi casi, il fornitore ha la materiale possibilità di entrare a contatto con il contenuto delle comunicazioni, la cui concreta riservatezza dipende dalle misure tecniche messe in atto e dal controllo esercitato sugli incaricati del trattamento.

Le intercettazioni telematiche sono quantitativamente meno rilevanti rispetto a quelle telefoniche e riguardano in prevalenza sia il traffico *Ip* sviluppato su linee telefoniche o collegamenti a larga banda (*Internet Protocol*), sia comunicazioni tramite posta elettronica. Queste ultime vengono realizzate predisponendo un inoltro automatico della corrispondenza ricevuta e spedita dall'intercettato mediante un'utenza di posta elettronica fornita dal fornitore.

2. Ulteriori servizi

Le operazioni svolte a supporto dell'attività investigativa possono riguardare aspetti diversi dalle intercettazioni. Si tratta di operazioni che coincidono con quelle elencate nel listino di cui al decreto interministeriale 26 aprile 2001 ("*Approvazione del listino relativo alle prestazioni obbligatorie per gli organismi di telecomunicazione*"), in attesa dell'approvazione in proposito del "Repertorio" previsto dal Codice delle comunicazioni (art. 96, comma 2).

Tra tali operazioni sono comprese le interrogazioni anagrafiche, la localizzazione dell'utenza, l'identificazione della linea chiamante o della linea connessa, il tracciamento, la sospensione o la limitazione dei servizi agli utenti, la documentazione del traffico pregresso contabilizzato e la documentazione integrale del traffico storico.

A differenza di quanto avviene in occasione delle conversazioni telefoniche intercettate, i fornitori hanno la possibilità di conoscere tali informazioni prodotte o raccolte nel compimento delle predette operazioni. Sono i fornitori, infatti, ad estrarre i dati, a selezionarli secondo i criteri richiesti dall'autorità giudiziaria, ad organizzarli in tabulati e a spedirli al richiedente. In tutte queste fasi, i dati restano nella disponibilità del fornitore e non può essere escluso che gli incaricati operanti in ambito aziendale debbano poterli conoscere, anche in parte, per svolgere alcune tra le operazioni medesime.

In alcuni casi, inoltre, i fornitori sono chiamati a prestare un supporto tecnico alla realizzazione di intercettazioni ambientali o di operazioni di videosorveglianza investigativa. Quest'ultima risulta svolta utilizzando la rete telefonica fissa per convogliare verso il centro indicato dall'autorità giudiziaria le immagini riprese da apposite telecamere.

3. Profili critici e prescrizioni del Garante
Dagli accertamenti svolti non emergono profili di illiceità nel trattamento dei dati personali.

In termini generali, le modalità esecutive previste dai diversi fornitori per le varie fasi di svolgimento dei servizi garantiscono un primo livello di sicurezza dei dati personali, con procedure sottoposte a un processo di certificazione di regola secondo *standard* internazionali di sicurezza.

In base agli elementi acquisiti va però constatata la necessità di incrementare sensibilmente tale livello di sicurezza, in particolare per quanto riguarda le diverse interazioni tra i fornitori e l'autorità giudiziaria.

Il Garante rileva quindi la necessità di prescrivere ai fornitori di adottare alcuni accorgimenti e misure, ulteriori rispetto a quelle minime di cui agli artt. 33 ss. del Codice in materia di protezione dei dati personali e al disciplinare tecnico allegato, atti a garantire maggiormente la protezione dei dati.

Tali prescrizioni riguardano la forma e l'autenticità dei decreti di inizio attività che pervengono ai fornitori, le modalità di invio e di ricezione della relativa documentazione, la gestione dei profili di autorizzazione e l'attribuzione dei diritti di accesso alle risorse informatiche, anche con riferimento a singoli incaricati.

Non sono oggetto di prescrizione i profili concernenti più direttamente la conservazione dei dati di traffico per finalità di accertamento e repressione dei reati, che saranno oggetto dell'apposito provvedimento del Garante da adottare ai sensi dell'art. 132, comma 5, del Codice.

3.1 Aspetti organizzativi della sicurezza

Profili esaminati
L'organizzazione delle funzioni aziendali dedicate ai servizi di supporto all'autorità giudiziaria, come attestata dai fornitori, risulta nel suo complesso sufficiente, rispondendo in termini generali a criteri di suddivisione delle competenze e di accentramento della responsabilità.

Devono essere tuttavia perseguiti, con idonei strumenti organizzativi, livelli di sicurezza più elevati, limitando in particolare la conoscibilità delle informazioni comunque attinenti all'attività svolta per scopi di giustizia.

Prescrizione
Le funzioni aziendali cui compete lo svolgimento di servizi per conto dell'autorità giudiziaria devono adottare un modello organizzativo che limiti al minimo la conoscibilità delle informazioni relative alle attività svolte per esigenze di giustizia, con una rigida partizione della visibilità dei dati su base organizzativa, funzionale e di area geografica di competenza.

Il personale che a qualsiasi titolo tratti questi dati deve essere designato in termini selettivi quale incaricato del trattamento.

Deve essere garantito ogni scrupolo nella gestione e nel mantenimento della qualità delle credenziali di autenticazione per l'accesso informatico ai dati trattati, conformando le procedure di gestione delle credenziali e i sistemi di autorizzazione a principi rigidi di coerenza delle abilitazioni nei sistemi informativi con i ruoli e le funzioni assegnate agli incaricati designati.

I mutamenti di ruolo o di funzione di un incaricato devono essere pertanto recepiti immediatamente, con le conseguenti opportune variazioni dei relativi profili di autorizzazione.

Deve essere realizzata, anche attraverso l'opportuna configurazione dei sistemi informatici utilizzati nel processo di gestione delle attività, una separazione marcata tra i dati di carattere amministrativo-contabile e i dati documentali prodotti nel corso delle attività svolte su richiesta dell'a.g., inibendo la possibilità per un operatore amministrativo-contabile di accedere ai dati documentali prodotti nell'ambito dell'attività svolta. L'accesso ai sistemi informatici di protocollazione ed archiviazione dei documenti scambiati con l'a.g. deve essere controllato tramite procedure di autenticazione robuste, con il ricorso anche a caratteristiche biometriche, in sintonia con le previsioni di cui alla regola n. 2 del predetto disciplinare tecnico in materia di misure minime di sicurezza.

3.2 Sicurezza dei flussi informativi con l'autorità giudiziaria

Profili esaminati
La gestione da parte del fornitore dei provvedimenti di intercettazione o che richiedono altri tipi di servizio sempre per conto dell'autorità giudiziaria è articolata in varie fasi, che comprendono:

- la ricezione in copia, con differenti modalità (posta ordinaria, messaggio telefax, posta elettronica o consegna diretta), del decreto di inizio attività;
- la verifica dell'autenticità e dell'esistenza dei requisiti formali della richiesta, nonché della loro completezza;
- gli accertamenti e le attività tecniche strumentali che portano a svolgere, anche attraverso flussi di informazioni interni al fornitore ed eventuali contatti con l'autorità giudiziaria, la vera e propria azione di intercettazione, per consentire la conoscenza delle conversazioni e delle comunicazioni da parte dei Cit;
- la trasmissione all'autorità giudiziaria dei dati accessori (dati di traffico, localizzazione, altre informazioni), utilizzando un mezzo di comunicazione concordato con la medesima autorità;
- la fatturazione e la cancellazione dei dati trattati (eccetto quelli necessari per scopi contabili e di documentazione delle attività svolte, che vengono custoditi con particolari modalità).

Dall'analisi dei vari flussi informativi si evidenzia la necessità di un rigoroso controllo, per evitare che venga dato seguito ad ipotetiche richieste da parte di soggetti non legittimati. Sono altresì necessarie modalità di comunicazione tra i fornitori e l'autorità giudiziaria che garantiscano maggiormente la riservatezza delle informazioni scambiate.

Va in proposito constatata favorevolmente la messa a disposizione per questi scopi, da parte di alcuni fornitori, di servizi *e-mail* con interfaccia *web* di tipo *Ssl* (*Secure Socket Layer*–connessione cifrata), o anche di più articolati strumenti software basati sullo stesso tipo di interfaccia, che evitano la circolazione in rete di messaggi, con relativi allegati, ancorché protetti da forme di cifratura, che potrebbero andare incontro a tutti gli ordinari inconvenienti che possono interessare i sistemi di posta *Smtp*: ritardate consegne, mancate consegne a causa di errori di indirizzo o di condizioni di traffico sulla rete, fino al caso più preoccupante di possibile erronea consegna a un destinatario diverso da quello legittimo.

Prescrizione
I fornitori devono provvedere affinché l'interscambio di informazioni con l'autorità giudiziaria avvenga evitando il ricorso a canali non affidabili, o affidabili solo parzialmente, sia dal punto di vista delle prestazioni, sia da quello della sicurezza, adottando a tal fine sistemi di comunicazione basati su aggiornati strumenti telematici sviluppati con protocolli di rete sicuri.

In questo ambito devono essere adottate tecniche di firma digitale evitando la cifratura dei documenti con strumenti tecnicamente deboli a livello applicativo, ed altre prassi inidonee, come la negoziazione di chiavi crittografiche simmetriche in modo informale su canali insicuri.

La comunicazione all'autorità giudiziaria dei risultati dell'attività strumentale svolta (tramite tabulati elettronici o in altro formato informatico), deve quindi avvenire esclusivamente in modo cifrato con strumenti di firma digitale che assicurino l'identificazione delle parti comunicanti, l'integrità e la

protezione dei dati, nonché la completezza e la correttezza delle informazioni temporali (date ed orari di formazione dei documenti o della loro trasmissione e consegna).

Queste forme più sicure di comunicazione possono essere realizzate con tecnologie di rete disponibili anche in forma di applicazioni *web oriented* dedicate, accessibili ai soli utenti legittimati e che consentano anche l'interscambio di messaggi tra i fornitori e l'autorità giudiziaria.

La posta elettronica Internet può essere utilizzata esclusivamente nella forma della posta elettronica certificata (Pec) di cui al d.P.R. 11 febbraio 2005, n. 68 e relative regole tecniche di attuazione.
Sia il ricevimento delle richieste, sia la comunicazione dei risultati, possono avvenire anche mediante consegna manuale della documentazione, da effettuarsi tramite soggetti delegati dall'autorità giudiziaria. I fornitori, al momento della consegna, dovranno acquisire i dati identificativi del latore della comunicazione e annotare in un apposito registro gli estremi della comunicazione (data, ora, identità del messo, ecc.).
Durante il decorso del termine di seguito stabilito per adempiere al presente provvedimento, i mezzi di comunicazione meno sicuri, come ad esempio il telefax analogico, vanno utilizzati soltanto in caso di impossibilità tecnica di utilizzare i canali sicuri eventualmente già disponibili.

3.3 Protezione dei dati trattati per scopi di giustizia

Profili esaminati
Come già rilevato, nel prestare altri servizi a supporto di indagini giudiziarie oltre alle intercettazioni, i fornitori vengono a conoscenza di una notevole mole di informazioni personali collegate alle modalità di comunicazione della persona sottoposta ad intercettazione con i propri interlocutori. Queste informazioni vengono elaborate e raccolte dal fornitore, per essere successivamente consegnate all'autorità giudiziaria che le ha richieste. Almeno per il lasso di tempo intercorrente tra la loro raccolta e la comunicazione all'autorità giudiziaria, queste stesse informazioni possono essere trattate lecitamente tramite i sistemi tecnologici e le funzioni aziendali preposte dal fornitore, il quale rimane però investito della responsabilità di proteggerle in modo idoneo a prevenire, per quanto tecnicamente possibile, ogni forma di abuso.

Prescrizione
Il Garante ritiene necessario che i fornitori sviluppino o integrino nei propri sistemi informativi rivolti al trattamento dei dati personali acquisiti o formati per scopi di giustizia strumenti informatici idonei ad assicurare il controllo sulle attività svolte da ciascun incaricato sui singoli elementi di informazione presenti nei *database* utilizzati. Ogni accesso a dati personali relativi a persone sottoposte ad intercettazione o a persone che comunicano con esse deve essere tracciato tramite una registrazione in un apposito *audit log* che consenta di verificare a posteriori il corretto utilizzo delle informazioni.

Tutti i dati personali acquisiti o formati per scopi di giustizia devono essere protetti con moderni strumenti di cifratura precludendo la loro conoscibilità da parte di soggetti non legittimati -dipendenti del fornitore, addetti alla manutenzione, ecc.- nel periodo di loro presenza nel sistema informativo del fornitore.

La persistenza di dati personali nei sistemi informativi dei fornitori, se imposta da ragioni tecniche, deve essere comunque strettamente limitata a quanto necessario per attuare i provvedimenti dell'autorità giudiziaria, prevedendone la cancellazione immediatamente dopo la loro corretta comunicazione all'a.g. richiedente.

Le prescrizioni di cui al presente punto 3 sono impartite prevedendo un termine di adeguamento di 180 giorni decorrenti dalla data di ricezione del presente provvedimento, termine che tiene in debito conto anche la necessità che l'evoluzione e l'aggiornamento tecnologico in corso negli uffici giudiziari avvengano secondo modalità coerenti con le prescrizioni suindicate.

Entro tale termine, i singoli fornitori oggetto degli accertamenti dovranno fornire al Garante un dettagliato riscontro sulle misure e sugli accorgimenti adottati in attuazione del presente provvedimento, anche in relazione alle attività pianificate e al loro stato di avanzamento.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'articolo 154, comma 1, lett. c), del Codice prescrive ai fornitori di servizi di comunicazione elettronica che svolgono le attività su richiesta dell'autorità giudiziaria di adottare, nei termini di cui in motivazione, le misure e gli accorgimenti indicati al punto 3, in particolare per quanto riguarda:

a) aspetti organizzativi della sicurezza

1. adozione di un modello organizzativo che limiti al minimo la conoscibilità delle informazioni trattate, con una rigida partizione della visibilità dei dati su base organizzativa, funzionale e di area geografica di competenza;
2. designazione selettiva degli incaricati, a qualsiasi titolo, del trattamento di dati personali;
3. rigoroso controllo della qualità e della coerenza delle credenziali di autenticazione per l'accesso informatico ai dati trattati;
4. separazione tra i dati di carattere amministrativo-contabile e i dati documentali prodotti;
5. procedure di autenticazione robuste, con il ricorso anche a caratteristiche biometriche;

b) sicurezza dei flussi informativi con l'autorità giudiziaria

1. adozione di sistemi di comunicazione basati su aggiornati strumenti telematici sviluppati con protocolli di rete sicuri;
2. adozione di tecniche di firma digitale per la cifratura dei documenti;
3. utilizzo di strumenti di cifratura basati su firma digitale per la comunicazione all'autorità giudiziaria dei risultati dell'attività strumentale svolta;
4. utilizzo della posta elettronica Internet esclusivamente nella forma della posta elettronica certificata (Pec);
5. ricorso alla consegna manuale di documenti esclusivamente tramite soggetti delegati dall'autorità giudiziaria, provvedendo alla tenuta di un apposito registro delle consegne;
6. limitazione dell'uso dei mezzi di comunicazione meno sicuri ai soli casi di impossibilità tecnica di utilizzare i canali sicuri eventualmente già disponibili;

c) protezione dei dati trattati per scopi di giustizia

1. sviluppo 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;
2. adozione di moderni strumenti di cifratura per la protezione dei dati nel periodo di loro presenza nel sistema informativo del fornitore;
3. 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;

d) integrale adeguamento entro 180 giorni decorrenti dalla data di ricezione del presente provvedimento e riscontro al Garante sulle misure e sugli accorgimenti adottati, termine che tiene in debito conto anche la necessità che l'evoluzione e l'aggiornamento tecnologico in corso negli uffici giudiziari avvengano secondo modalità coerenti con le prescrizioni suindicate.

Roma, 15 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli