GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PROVVEDIMENTO 18 luglio 2013

Misure di sicurezza nelle attivita' di intercettazione da parte delle Procure della Repubblica. (Provvedimento n. 356). (13A06934)

(GU n.189 del 13-8-2013)

IL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Viste le disposizioni del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito «Codice») concernenti l'adozione delle misure di sicurezza (artt. 31 e 33 - 35, e Disciplinare tecnico di cui all'Allegato B) al Codice);

Viste le disposizioni del Codice riguardanti il trattamento dei dati personali in ambito giudiziario (artt. 46 e ss.);

Visti i provvedimenti del Garante recanti «Misure di sicurezza obbligatorie per le intercettazioni» del 15 dicembre 2005 e «Intercettazioni: misure di sicurezza presso i gestori» del 20 settembre 2006 (pubblicati sul sito istituzionale www.gpdp.it, doc. web n. 1203890 e n. 1341009), con cui sono stati prescritti ai gestori di servizi di comunicazione elettronica misure e accorgimenti specificamente volti ad adeguare i livelli di sicurezza nel trattamento e nella trasmissione dei dati relativi alle intercettazioni telefoniche e telematiche che gli stessi gestori sono tenuti ad attivare su richiesta dell'Autorita' giudiziaria;

Visto il provvedimento del Garante sulla «Sicurezza dei dati di traffico telefonico e telematico» del 17 gennaio 2008 (doc. web n. 1482111), con cui sono stati prescritti ai gestori di servizi di comunicazione elettronica misure e accorgimenti volti a incrementare i livelli di sicurezza nel trattamento e nella trasmissione dei dati di traffico telefonico e telematico svolto ai sensi dell'art. 132 del Codice per finalita' di accertamento e repressione dei reati da parte dell'Autorita' giudiziaria;

Visto il provvedimento del Garante riguardante l'«Attribuzione delle funzioni di amministratore di sistema» del 27 novembre 2008 (doc. web n. 1577499), con cui sono stati prescritti ai titolari di trattamento con strumenti elettronici misure e accorgimenti di carattere organizzativo e tecnico relativi alla designazione degli «amministratori di sistema» di sistemi informativi e impianti informatici;

Rilevato che ai trattamenti di dati personali effettuati anche per ragioni di giustizia (art. 47, comma 2, del Codice) presso gli Uffici giudiziari, di ogni ordine e grado, si applicano le disposizioni del Codice che prevedono specifiche garanzie in materia di protezione dei dati per quanto riguarda le misure di sicurezza da adottare, in particolare, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali e di accessi non autorizzati alle informazioni;

Ritenuto che, nel quadro dello svolgimento dei compiti previsti dal Codice, con provvedimento del 13 settembre 2012 il Garante ha deliberato di prendere in esame la problematica dell'applicazione delle misure di sicurezza ai trattamenti dei dati personali svolti presso le Procure della Repubblica, anche tramite la polizia giudiziaria o soggetti terzi, nell'ambito delle attivita' di intercettazione telefonica o ambientale di conversazioni o

comunicazioni, anche informatiche o telematiche, effettuate per ragioni di giustizia, nonche' di controllo preventivo (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.), tema gia' affrontato dal Garante con i richiamati provvedimenti rivolti ai soli gestori di servizi di comunicazione elettronica;

Rilevato che, a tal fine, l'Autorita' ha deliberato di inoltrare una richiesta di informazioni a cura dell'ufficio volta ad acquisire da alcune Procure elementi conoscitivi utili;

Dato atto che con detto provvedimento tali uffici sono stati individuati in alcune Procure della Repubblica di medie dimensioni, dislocate in diverse aree del territorio nazionale e che hanno sede presso capoluoghi di regione e, in particolare, nelle Procure della Repubblica presso i Tribunali di Bologna, Catanzaro, Perugia, Potenza e Venezia;

Vista la documentazione in atti e, in particolare, le richieste di informazioni inoltrate a dette Procure a cura dell'ufficio e i riscontri trasmessi dagli uffici giudiziari, che hanno fornito piena collaborazione;

Considerato che da detti riscontri e' emerso un quadro sufficientemente ampio ed esauriente delle modalita' e delle procedure attraverso cui detti uffici acquisiscono e gestiscono le informazioni raccolte attraverso le attivita' di intercettazione, e delle misure che ciascuna Procura adotta per la protezione dei dati personali e dei sistemi utilizzati per gestirli;

Rilevato, peraltro, che da detti riscontri e' emerso un quadro variegato e disomogeneo di misure, di natura fisica ed informatica, adottate dagli uffici a protezione delle informazioni personali e dei sistemi;

Udito il capo del Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi del Ministero della giustizia che ha illustrato le caratteristiche del progetto della gara unica per la fornitura di servizi di noleggio di apparati e di supporto informatico per le esigenze delle Procure della Repubblica connesse alla gestione delle intercettazioni;

Ritenuto che la sicurezza dei dati personali e dei sistemi in questione, per la tipologia delle informazioni trattate e delle finalita' perseguite, riveste particolare importanza e delicatezza per gli effetti che tali informazioni possono esplicare sia riguardo alla dignita' e ai diritti delle persone sottoposte a intercettazione e di quelle che comunicano con esse, sia alla necessaria efficacia delle indagini giudiziarie nel cui ambito le intercettazioni vengono compiute;

Considerato quindi che, come gia' deliberato in relazione ai trattamenti di dati personali effettuati presso alcuni uffici giudiziari, la documentazione e le informazioni acquisite hanno evidenziato l'esigenza di realizzare alcuni interventi volti ad assicurare un rafforzamento del livello di protezione dei dati personali trattati e dei sistemi utilizzati, commisurato alla indicata tipologia delle informazioni detenute;

Ritenuto, altresi', che l'evoluzione tecnologica nel campo delle comunicazioni elettroniche e gli aggravati scenari di rischio connessi all'elaborazione informatica dei dati personali richiedono di armonizzare e specificare maggiormente le misure di sicurezza di quei trattamenti svolti presso gli uffici giudiziari e relativi all'acquisizione e alla successiva elaborazione di dati personali prodotti dai gestori di servizi di comunicazione elettronica;

Considerato, quindi, che appare necessario estendere l'adozione di tali interventi alla generalita' degli uffici inquirenti, anche al fine di assicurare una tendenziale omogeneita' delle misure e degli accorgimenti volti alla tutela dei dati personali e dei sistemi, ferme restando eventuali diverse misure, gia' adottate dagli uffici, che assicurino un livello di sicurezza di pari o maggiore efficacia;

Ritenuto che, tenuto conto della menzionata evoluzione tecnologica

nel campo delle comunicazioni elettroniche e dell'informatica, anche al fine di contenere i costi derivanti dalla realizzazione delle misure di sicurezza specie di natura fisica, nulla osta, nell'ottica della protezione dei dati personali e dei sistemi, all'eventuale accorpamento di piu' apparati tecnologici utilizzati da diversi Uffici di Procura per la gestione delle attivita' connesse alle intercettazioni;

Rilevato che il Garante ha il compito anche per gli uffici giudiziari di prescrivere al titolare del trattamento di dati personali le necessarie modificazioni e integrazioni, che il destinatario e' tenuto ad adottare; rilevato che il Garante deve, altresi', verificare l'attuazione delle misure indicate, anche attraverso le particolari forme e modalita' previste dall'art. 160 del Codice;

Rilevata, quindi, la necessita' di prescrivere misure e accorgimenti volti al rafforzamento della sicurezza nel trattamento dei dati personali e dei sistemi nell'attivita' di intercettazione di conversazioni o comunicazioni elettroniche, anche informatiche o telematiche, nonche' di controllo preventivo, svolta presso le Procure della Repubblica nei termini di seguito individuati.

1. Centri Intercettazioni Telecomunicazioni

Presso ogni Procura della Repubblica e' costituita una struttura, denominata Centro Intercettazioni Telecomunicazioni (C.I.T.), ove si svolgono le varie attivita' connesse all'effettuazione delle intercettazioni. La struttura e' costituita dai locali ove sono situate le postazioni di ascolto, unitamente agli apparati elettronici e informatici utilizzati per lo svolgimento dei servizi di intercettazione, tra cui: gli apparati su cui vengono indirizzate le telefonate e le altre forme di comunicazione intercettate per la loro registrazione e il loro successivo trattamento (oggi costituiti da server informatici su cui vengono registrati i flussi intercettati); i server tramite i quali vengono erogati i servizi per la gestione informatica e documentale delle intercettazioni (compilazione dei c.d. "brogliacci", trascrizione delle conversazioni, dati accessori); gli apparati per la generazione e conservazione di copie di sicurezza dei dati (backup).

Sono usualmente compresi nella struttura C.I.T. anche uffici tecnici e amministrativi ove vengono effettuate le operazioni di attivazione, proroga e chiusura delle attivita' di intercettazione e la c.d. «masterizzazione» o duplicazione dei dati acquisiti, nonche' gli archivi fisici per la custodia e la conservazione dei supporti ottici o magnetici contenenti i dati acquisiti.

In relazione all'insieme di tali strutture e ai trattamenti di dati personali che vi vengono svolti il Garante richiama i titolari dei trattamenti al rispetto degli obblighi di sicurezza di cui all'art. 31 del Codice, valutando l'idoneita' delle misure di sicurezza in essere e di quelle che potranno essere adottate alla luce di un'analisi dei rischi incombenti sui dati che funga da guida nello sviluppo di un sistema di gestione della sicurezza basato su metodologie standard.

Inoltre, il Garante ritiene necessario, per assicurare un piu' elevato livello di sicurezza dei dati e dei sistemi, anticipare eventuali azioni adeguative della sicurezza che potranno essere intraprese dai titolari sulla base della richiamata analisi dei rischi, prescrivendo le seguenti misure tecniche e organizzative da adottare presso le Procure della Repubblica.

1.a Misure di sicurezza fisica

I locali in cui viene effettuata la registrazione delle conversazioni telefoniche o ambientali intercettate, o di dati digitali anche a carattere audiovisivo derivanti da forme piu' avanzate di intercettazione ambientale o telematica, nonche' i locali in cui sono installati gli apparati terminali connessi alla rete pubblica di comunicazione per la ricezione dei flussi telefonici o

telematici intercettati, devono essere protetti con misure di sicurezza di carattere fisico e organizzativo quantomeno contro i rischi di accesso abusivo e contro quelli derivanti da altri fattori suscettibili di incidere sulla integrita' e disponibilita' dei dati personali.

A tali scopi, devono essere previsti:

impianti per il rilevamento e l'estinzione di incendi, comprensivi di porte antincendio di accesso ai locali dotate di idonee serrature di sicurezza;

misure di protezione e idonee serrature di sicurezza alle finestre dei locali che ne siano eventualmente dotati;

strumenti per il monitoraggio dei locali adibiti ad attivita' di intercettazione e delle aree di ingresso, attraverso l'adozione di impianti di videosorveglianza a circuito chiuso, ivi incluse le sale di ascolto, con registrazione delle immagini, nel rispetto delle prescrizioni dettate dal Garante nel «Provvedimento in materia di videosorveglianza» dell'8 aprile 2010 (pubblicato nella Gazzetta Ufficiale n. 99 del 29 aprile 2010, doc. web n. 1712680);

accesso fisico alle sale di ascolto consentito, in alternativa, tramite l'utilizzo di badge individuali e nominalmente assegnati, cui va associato un codice numerico individuale posto nell'esclusiva conoscenza dell'interessato, oppure attraverso strumenti elettronici che prevedano procedure di identificazione mediante l'utilizzo di dispositivi biometrici;

accesso fisico ai locali ove sono collocati i server e gli archivi tramite l'utilizzo di dispositivi biometrici;

registrazione automatica degli accessi ai locali effettuati tramite badge o dispositivi biometrici;

custodia in armadi ignifughi muniti di serratura di sicurezza dei supporti di memorizzazione removibili, qualora utilizzati per la registrazione dei contenuti delle intercettazioni e delle informazioni accessorie, della documentazione cartacea e dei registri concernenti le attivita' svolte nell'ambito delle intercettazioni, dall'inizio alla cessazione del trattamento;

accesso ai locali per operazioni di manutenzione e interventi tecnici sulle apparecchiature, anche da parte di ditte esterne fornitrici degli apparati o erogatrici di servizi manutentivi, consentito solo a personale previamente autorizzato dalla Procura, identificato e registrato al momento dell'accesso e operante sotto il controllo di personale in servizio presso il C.I.T.; al personale tecnico in questione deve essere inibito l'accesso a dati, informazioni e documenti prodotti, se non nei limiti strettamente necessari al compimento degli interventi di manutenzione.

1.b Misure di sicurezza informatica

I titolari dei trattamenti devono evitare che l'interscambio di informazioni tra l'Autorita' giudiziaria e i gestori di servizi di comunicazione elettronica avvenga tramite il ricorso a canali di comunicazione non sufficientemente affidabili dal punto di vista delle prestazioni e da quello della sicurezza, adottando a tal fine sistemi basati su aggiornati strumenti telematici sviluppati con protocolli di rete sicuri.

Pertanto, devono essere adottati i seguenti accorgimenti:

comunicazioni elettroniche tra l'Autorita' giudiziaria e i gestori effettuate esclusivamente in modo cifrato con strumenti, anche di tipo online o web, che assicurino comunque l'identificazione delle parti comunicanti, l'integrita' e la protezione dei dati, nonche' la completezza e la correttezza delle informazioni temporali relative alle informazioni trasmesse (date ed orari di formazione dei documenti o della loro trasmissione e consegna);

protezione dei documenti informatici trasferiti su supporti rimovibili con idonee tecniche crittografiche, ricorrendo preferibilmente ad algoritmi a chiave pubblica (come nel caso dell'uso di strumenti di firma digitale in funzione di cifratura),

evitando comunque la trasmissione di chiavi simmetriche di cifratura in modo informale su canali insicuri;

utilizzo nelle comunicazioni tra Autorita' giudiziaria e gestori della posta elettronica Internet esclusivamente nella forma di posta elettronica certificata (Pec) di cui all'art. 48 del d.lg. 7 marzo 2005, n. 82, e del telefax esclusivamente nella forma di fax digitale «gruppo 4» (ISDN) oppure di Fax over IP;

trasmissione cifrata delle comunicazioni telematiche intercettate (flussi IP, posta elettronica) dal punto di loro estrazione dalla rete del gestore fino agli apparati riceventi presso i C.I.T..

Sia la trasmissione delle disposizioni ai gestori, sia la comunicazione dei risultati elaborati dai gestori, possono avvenire anche mediante consegna manuale della documentazione, da effettuarsi tramite soggetti delegati dall'Autorita' giudiziaria, opportunamente designati quali incaricati o responsabili del trattamento, ove abbiano accesso ai dati.

2. Remotizzazione

2.a Attivita' di solo ascolto

Risulta generalizzato il ricorso alla c.d. «remotizzazione» degli ascolti, ovvero il reindirizzamento dei flussi delle comunicazioni oggetto di intercettazione dai C.I.T. verso gli uffici di polizia giudiziaria delegata, nel caso, frequente, in cui le strutture presso le Procure risultino insufficienti o inadeguate. Premessa la necessita', in tale contesto, della designazione, con le modalita' di cui all'art. 29 del Codice, di detti uffici quali responsabili del trattamento dei dati loro affidato, e ferma restando l'esigenza che le operazioni di intercettazione siano compiute per mezzo degli impianti installati presso le Procure della Repubblica, e che la remotizzazione venga disposta, in via residuale, nei soli casi eccezionali previsti dalle norme codicistiche (art. 268 c.p.p.), in relazione alle strutture in cui sono collocate le sale di ascolto esterne agli uffici giudiziari si ritiene necessaria l'adozione delle seguenti misure di sicurezza fisica:

porte di accesso ai locali dotate di idonee serrature di sicurezza;

misure di protezione e idonee serrature di sicurezza alle finestre dei locali che ne sono eventualmente dotati;

monitoraggio dei locali e delle aree di ingresso, attraverso l'adozione di impianti di videosorveglianza a circuito chiuso con registrazione delle immagini, nel rispetto del citato provvedimento del Garante in materia di videosorveglianza;

accesso fisico alle sale di ascolto consentito, in alternativa, tramite l'utilizzo di badge individuali e nominalmente assegnati, cui va associato un codice numerico individuale posto nell'esclusiva conoscenza dell'interessato, oppure attraverso strumenti elettronici che prevedano procedure di identificazione mediante l'utilizzo di dispositivi biometrici;

registrazione automatica degli accessi ai locali effettuati tramite badge o dispositivi biometrici;

custodia in armadi ignifughi blindati della documentazione cartacea e dei registri concernenti le attivita' svolte nell'ambito delle intercettazioni;

accesso ai locali per operazioni di manutenzione delle apparecchiature di ascolto consentito solo a personale previamente autorizzato, identificato e registrato al momento dell'accesso e affiancato da personale di polizia giudiziaria; al personale in questione deve essere inibito l'accesso a dati, informazioni e documenti prodotti, se non nei limiti strettamente necessari al compimento degli interventi di manutenzione.

2.b Attivita' di ascolto e registrazione

In relazione alle strutture ubicate presso gli uffici di polizia giudiziaria in cui vengano svolte, oltre all'ascolto o al riascolto di comunicazioni intercettate, anche attivita' di registrazione e/o di custodia delle informazioni acquisite, si ritiene necessaria

l'adozione, oltre agli accorgimenti di cui al punto 2.a, delle seguenti ulteriori misure:

installazione di porte antincendio di accesso ai locali;

installazione di impianti automatici di rilevamento dei fumi, estinzione e allarme antincendio;

accesso ai locali consentito attraverso strumenti elettronici che prevedano procedure di identificazione mediante l'utilizzo di dispositivi biometrici;

registrazione degli accessi ai locali effettuato attraverso l'utilizzo dei dispositivi biometrici;

custodia in armadi ignifughi muniti di serratura di sicurezza dei supporti removibili contenenti i contenuti delle intercettazioni e i dati connessi, ove temporaneamente detenuti presso tali strutture.

3. Misure di sicurezza informatica

3.a Sistemi di autenticazione e autorizzazione

Riguardo sia all'accesso da parte di ciascun operatore abilitato, compresi gli utenti con profilo di amministratore di sistema, ai sistemi e ai server utilizzati nelle attivita' di intercettazione -fermo restando, in via prioritaria, il necessario rispetto delle disposizioni in materia di misure minime di sicurezza, specie con riferimento alla designazione di detti operatori quali incaricati del trattamento loro consentito, e al sistema di autenticazione informatica e autorizzazione (artt. 30 e 34, regole da 1 a 15 e da 27 a 29 del Disciplinare tecnico di cui all'Allegato B) del Codice)- si rende necessaria, in considerazione del peculiare ambito di trattamento dei dati personali, l'adozione delle seguenti misure:

accessi ai sistemi solo da postazioni preventivamente abilitate e censite, connesse a reti protette dotate di sistemi di protezione perimetrale (firewall);

accessi ai sistemi, sia per scopi di configurazione delle intercettazioni, che per ascolto o riascolto, ad operatori abilitati e autenticati tramite procedure di strong authentication, qualunque sia la modalita', locale o remota, con cui venga realizzato l'accesso al sistema di elaborazione utilizzato per il trattamento;

applicazione della strong authentication anche agli addetti tecnici (amministratori di sistema, di rete, di data base) che possano materialmente accedere ai dati delle intercettazioni in ragione delle mansioni loro attribuite;

attribuzione di utenze di amministratore di sistema a soggetti preventivamente individuati e designati secondo i criteri stabiliti dal Garante con il citato provvedimento del 27 novembre 2008 e con il provvedimento del 25 giugno 2009 (doc. web n. 1626595);

immediato recepimento dei mutamenti di funzione e ruolo degli incaricati con conseguenti opportune variazioni dei relativi profili di autorizzazione.

3.b Ulteriori misure di sicurezza informatica

Si rende, infine, necessario adottare le seguenti ulteriori misure:

collegamenti telematici tra Procure della Repubblica e Uffici di polizia giudiziaria realizzati ricorrendo a connessioni «punto-punto» di tipo dedicato oppure a collegamenti virtuali in rete di tipo VPN (Virtual Private Network), in modalita' «LAN to LAN», tra sedi previamente individuate e censite;

effettuazione delle operazioni di «masterizzazione» ed eventuale duplicazione dei contenuti delle intercettazioni solo quando strettamente indispensabili, da parte di personale specificamente abilitato;

fermo restando il dettato dell'art. 89 disp. att. c.p.p. in ordine alla etichettatura dei supporti di memorizzazione delle intercettazioni, e in attesa dell'eventuale adeguamento delle disposizioni in materia di intercettazioni all'evoluzione degli strumenti tecnologici utilizzati in tale ambito, adozione di idonei accorgimenti al fine di impedire che i contenitori o i plichi utilizzati per il trasporto dei supporti stessi rechino indicazioni

esteriori che possano consentire a soggetti non abilitati alla relativa conoscenza di individuare direttamente l'oggetto dell'intercettazione ed i soggetti intercettati (ricorrendo, ad esempio a codici identificativi conoscibili solo dai soggetti legittimati ovvero inserendo il predetto materiale in un secondo involucro privo di riferimenti);

annotazione in registri informatici, con tecniche che ne assicurino la inalterabilita', con indicazione dei riferimenti temporali relativi alle attivita' svolte e al personale operante, dell'esecuzione delle operazioni (quali l'ascolto, la consultazione, registrazione, masterizzazione, archiviazione e duplicazione delle informazioni, la trascrizione delle intercettazioni, la manutenzione e la gestione dei sistemi, la distruzione dei supporti, dei verbali, delle registrazioni e di ogni altra documentazione attinente alle intercettazioni) svolte nell'ambito delle attivita' di intercettazione sia presso i C.I.T., sia presso gli Uffici di polizia giudiziaria delegati (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.; d.m. 30 settembre 1989; d.m. 17 dicembre 1999);

conservazione in forma cifrata, indipendentemente dal formato di registrazione, delle tracce foniche e delle altre informazioni, in modo da impedirne l'ascolto (nel caso delle tracce foniche) o la intelligibilita' a soggetti non legittimati anche in caso di acquisizione fortuita o a seguito di guasti o interventi manutentivi sulle apparecchiature informatiche;

conservazione in forma cifrata delle eventuali copie di sicurezza (backup) dei dati allo stesso modo di quanto previsto per i dati on line; ogni altra estrazione di dati, anche parziale, su qualsiasi tipo di supporto removibile deve essere assistita da procedure crittografiche per la protezione dei contenuti;

trasmissione dei supporti e della documentazione cartacea (quali le trascrizioni del contenuto delle intercettazioni) all'Autorita' giudiziaria esclusivamente mediante personale di polizia giudiziaria;

designazione dei soggetti esterni all'Ufficio giudiziario e, in particolare, delle ditte operanti per conto delle Procure nell'ambito di appalti di fornitura di beni e di servizi informatici strumentali alla realizzazione delle intercettazioni o alla elaborazione delle informazioni intercettate, quali responsabili del trattamento ai sensi dell'art. 29 del Codice, ponendo particolare attenzione all'individuazione da parte del titolare dei profili di autorizzazione degli incaricati e delle misure di sicurezza, nonche' al controllo periodico sull'operato del responsabile esterno;

cancellazione sicura, alla cessazione del rapporto contrattuale, dei contenuti registrati nei server e negli altri apparati delle societa' noleggiatrici esterne che forniscono la strumentazione hardware.

Ritenuta la necessita' che le modificazioni e integrazioni alle misure di sicurezza indicate nel presente provvedimento, attesa la delicatezza delle informazioni e dei dati connessi trattati attraverso le attivita' di intercettazione, avuto riguardo alla riservatezza delle persone e all'efficacia delle indagini, siano apportate dalle Procure della Repubblica nel termine che l'Autorita' ritiene congruo fissare in diciotto mesi, decorrente dalla pubblicazione del presente provvedimento nella Gazzetta Ufficiale della Repubblica italiana;

Rilevata la necessita' che le Procure, al fine dell'espletamento del compito di verifica dell'attuazione delle misure da parte del Garante, forniscano riscontro all'Autorita' circa la loro completa adozione entro il predetto termine;

Ritenuto, altresi', necessario che le Procure riferiscano all'Autorita', entro la data del 30 giugno 2014, sullo stato di avanzamento dell'attuazione di dette misure;

Ritenuto, peraltro, che le misure indicate dipendono significativamente dalla collaborazione delle competenti strutture

del Ministero della giustizia, con riferimento alle pertinenti attribuzioni in tema di organizzazione e funzionamento dei servizi relativi alla giustizia;

Ritenuta, quindi, l'opportunita' di segnalare al Ministero della giustizia la necessita' di fornire alle Procure della Repubblica le risorse idonee a consentire a detti uffici di apportare le modificazioni e integrazioni indicate nel presente provvedimento volte a rafforzare la sicurezza nel trattamento dei dati personali e dei sistemi nell'ambito delle attivita' di intercettazione;

Ritenuta, altresi', l'opportunita' che copia del presente provvedimento venga inviata al Consiglio superiore della magistratura, per ogni opportuna conoscenza in relazione alle relative attribuzioni, nonche' per l'adozione di ogni iniziativa ritenuta idonea a favorire la massima diffusione presso gli uffici giudiziari interessati;

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

Relatore il dott. Antonello Soro;

Tutto cio' premesso il garante

a) Ai sensi dell'art. 154, comma 1, lett. c), del Codice, prescrive alle Procure della Repubblica di apportare le seguenti modificazioni e integrazioni alle misure di sicurezza adottate in relazione ai trattamenti di dati personali svolti, anche tramite la polizia giudiziaria o soggetti terzi, nell'ambito delle attivita' di intercettazione di conversazioni o comunicazioni, anche informatiche o telematiche, effettuate per ragioni di giustizia, ai sensi dell'art. 47, comma 2, del Codice, nonche' di controllo preventivo (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.), ferme restando eventuali diverse misure, gia' adottate dagli uffici, che assicurino un livello di sicurezza di pari o maggiore efficacia:

1. Centri Intercettazioni Telecomunicazioni

In relazione alle strutture site presso le Procure della Repubblica ove si svolgono le varie attivita' connesse all'effettuazione delle intercettazioni (C.I.T.) prevedere:

1.a Misure di sicurezza fisica

impianti per il rilevamento e l'estinzione di incendi, comprensivi di porte antincendio di accesso ai locali dotate di idonee serrature di sicurezza;

misure di protezione e idonee serrature di sicurezza alle finestre dei locali che ne siano eventualmente dotati;

strumenti per il monitoraggio dei locali adibiti ad attivita' di intercettazione e delle aree di ingresso, attraverso l'adozione di impianti di videosorveglianza a circuito chiuso con registrazione delle immagini, nel rispetto delle prescrizioni dettate dal Garante nel «Provvedimento in materia di videosorveglianza» dell'8 aprile 2010 (pubblicato in G.U. n. 99 del 29 aprile 2010, doc. web n. 1712680);

accesso fisico alle sale di ascolto consentito, in alternativa, tramite l'utilizzo di badge individuali e nominalmente assegnati, cui va associato un codice numerico individuale posto nell'esclusiva conoscenza dell'interessato, oppure attraverso strumenti elettronici che prevedano procedure di identificazione mediante l'utilizzo di dispositivi biometrici;

accesso fisico ai locali ove sono collocati i server e gli archivi tramite l'utilizzo di dispositivi biometrici;

registrazione automatica degli accessi ai locali effettuati tramite badge o dispositivi biometrici;

custodia in armadi ignifughi muniti di serratura di sicurezza dei supporti di memorizzazione removibili, qualora utilizzati per la registrazione dei contenuti delle intercettazioni e delle informazioni accessorie, della documentazione cartacea e dei registri

concernenti le attivita' svolte nell'ambito delle intercettazioni, dall'inizio alla cessazione del trattamento;

accesso ai locali per operazioni di manutenzione e interventi tecnici sulle apparecchiature, anche da parte di ditte esterne fornitrici degli apparati o erogatrici di servizi manutentivi, consentito solo a personale previamente autorizzato dalla Procura, identificato e registrato al momento dell'accesso e operante sotto il controllo di personale in servizio presso il C.I.T.; al personale tecnico in questione deve essere inibito l'accesso a dati, informazioni e documenti prodotti, se non nei limiti strettamente necessari al compimento degli interventi di manutenzione;

1.b Misure di sicurezza informatica

comunicazioni elettroniche tra l'Autorita' giudiziaria e i gestori effettuate esclusivamente in modo cifrato con strumenti, anche di tipo on line o web, che assicurino comunque l'identificazione delle parti comunicanti, l'integrita' e la protezione dei dati, nonche' la completezza e la correttezza delle informazioni temporali relative alle informazioni trasmesse (date ed orari di formazione dei documenti o della loro trasmissione e consegna);

protezione dei documenti informatici trasferiti su supporti rimovibili con idonee tecniche crittografiche, ricorrendo preferibilmente ad algoritmi a chiave pubblica (come nel caso dell'uso di strumenti di firma digitale in funzione di cifratura), evitando comunque la trasmissione di chiavi simmetriche di cifratura in modo informale su canali insicuri;

utilizzo nelle comunicazioni tra Autorita' giudiziaria e gestori della posta elettronica Internet esclusivamente nella forma di posta elettronica certificata (Pec) di cui all'art. 48 del d.lg. 7 marzo 2005, n. 82, e del telefax esclusivamente nella forma di fax digitale «gruppo 4» (ISDN) oppure di Fax over IP;

trasmissione cifrata delle comunicazioni telematiche intercettate (flussi IP, posta elettronica) dal punto di loro estrazione dalla rete del gestore fino agli apparati riceventi presso i C.I.T..

Sia la trasmissione delle disposizioni ai gestori, sia la comunicazione dei risultati elaborati dai gestori, possono avvenire anche mediante consegna manuale della documentazione, da effettuarsi tramite soggetti delegati dall'Autorita' giudiziaria, opportunamente designati quali incaricati o responsabili del trattamento, ove abbiano accesso ai dati.

2. Remotizzazione

2.a Attivita' di solo ascolto

In relazione alle strutture site presso gli Uffici di polizia giudiziaria, ove sono collocate solo le sale di ascolto, da designarsi quali responsabili del trattamento dei dati loro affidato, ai sensi dell'art. 29 del Codice prevedere:

porte di accesso ai locali dotate di idonee serrature di sicurezza;

misure di protezione e idonee serrature di sicurezza alle finestre dei locali che ne sono eventualmente dotati;

monitoraggio dei locali e delle aree di ingresso, attraverso l'adozione di impianti di videosorveglianza a circuito chiuso con registrazione delle immagini, nel rispetto del citato provvedimento del Garante in materia di videosorveglianza;

accesso fisico alle sale di ascolto consentito, in alternativa, tramite l'utilizzo di badge individuali e nominalmente assegnati, cui va associato un codice numerico individuale posto nell'esclusiva conoscenza dell'interessato, oppure attraverso strumenti elettronici che prevedano procedure di identificazione mediante l'utilizzo di dispositivi biometrici;

registrazione automatica degli accessi ai locali effettuati tramite badge o dispositivi biometrici;

custodia in armadi ignifughi blindati della documentazione cartacea e dei registri concernenti le attivita' svolte nell'ambito delle intercettazioni;

accesso ai locali per operazioni di manutenzione delle apparecchiature di ascolto consentito solo a personale previamente autorizzato, identificato e registrato al momento dell'accesso e affiancato da personale di polizia giudiziaria; al personale in questione deve essere inibito l'accesso a dati, informazioni e documenti prodotti, se non nei limiti strettamente necessari al compimento degli interventi di manutenzione.

2.b Attivita' di ascolto e registrazione

In relazione alle strutture site presso gli Uffici di polizia giudiziaria, ove si svolgono anche attivita' di registrazione e/o custodia delle informazioni acquisite, da designarsi quali responsabili del trattamento dei dati loro affidato, ai sensi dell'art. 29 del Codice, oltre agli accorgimenti di cui al punto 2.a, prevedere:

installazione di porte antincendio di accesso ai locali;

installazione di impianti automatici di rilevamento dei fumi, estinzione e allarme antincendio;

accesso ai locali consentito attraverso strumenti elettronici che prevedano procedure di identificazione mediante l'utilizzo di dispositivi biometrici;

registrazione degli accessi ai locali effettuato attraverso l'utilizzo dei dispositivi biometrici;

custodia in armadi ignifughi muniti di serratura di sicurezza dei supporti removibili contenenti i contenuti delle intercettazioni e i dati connessi, ove temporaneamente detenuti presso tali strutture.

3. Misure di sicurezza informatica

3.a Sistemi di autenticazione e autorizzazione

Ferme restando la designazione degli operatori abilitati quali incaricati del trattamento loro consentito, nonche' l'adozione di sistemi di autenticazione informatica e di autorizzazione, prevedere:

accessi ai sistemi consentiti solo da postazioni preventivamente abilitate e censite, connesse a reti protette dotate di sistemi di protezione perimetrale (firewall);

accessi ai sistemi consentiti, sia per scopi di configurazione delle intercettazioni, che per ascolto o riascolto, ad operatori abilitati e autenticati tramite procedure di strong authentication, qualunque sia la modalita', locale o remota, con cui venga realizzato l'accesso al sistema di elaborazione utilizzato per il trattamento;

applicazione della strong authentication anche agli addetti tecnici (amministratori di sistema, di rete, di data base) che possano materialmente accedere ai dati delle intercettazioni in ragione delle mansioni loro attribuite;

attribuzione di utenze di amministratore di sistema a soggetti preventivamente individuati e designati secondo i criteri stabiliti dal Garante con i provvedimenti del 27 novembre 2008 e del 25 giugno 2009;

immediato recepimento dei mutamenti di funzione e ruolo degli incaricati con conseguenti opportune variazioni dei relativi profili di autorizzazione.

3.b Ulteriori misure di sicurezza informatica

collegamenti telematici tra Procure della Repubblica e Uffici di polizia giudiziaria realizzati ricorrendo a connessioni «punto-punto» di tipo dedicato oppure a collegamenti virtuali in rete di tipo VPN (Virtual Private Network), in modalita' «LAN to LAN», tra sedi previamente individuate e censite;

effettuazione delle operazioni di «masterizzazione» ed eventuale duplicazione dei contenuti delle intercettazioni solo quando strettamente indispensabili, da parte di personale specificamente abilitato;

fermo restando il dettato dell'art. 89 disp. att. c.p.p. in ordine alla etichettatura dei supporti di memorizzazione delle intercettazioni, e in attesa dell'eventuale adeguamento delle disposizioni in materia di intercettazioni all'evoluzione degli

strumenti tecnologici utilizzati in tale ambito, adozione di idonei accorgimenti al fine di impedire che i contenitori o i plichi utilizzati per il trasporto dei supporti stessi rechino indicazioni esteriori che possano consentire a soggetti non abilitati alla relativa conoscenza di individuare direttamente l'oggetto dell'intercettazione ed i soggetti intercettati (ricorrendo, ad esempio a codici identificativi conoscibili solo dai soggetti legittimati ovvero inserendo il predetto materiale in un secondo involucro privo di riferimenti);

annotazione in registri informatici, con tecniche che ne assicurino la inalterabilita', con indicazione dei riferimenti temporali relativi alle attivita' svolte e al personale operante, dell'esecuzione delle operazioni (quali l'ascolto, la consultazione, registrazione, masterizzazione, archiviazione e duplicazione delle informazioni, la trascrizione delle intercettazioni, la manutenzione e la gestione dei sistemi, la distruzione dei supporti, dei verbali, delle registrazioni e di ogni altra documentazione attinente alle intercettazioni) svolte nell'ambito delle attivita' di intercettazione sia presso i C.I.T., sia presso gli Uffici di polizia giudiziaria delegati (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.; d.m. 30 settembre 1989; d.m. 17 dicembre 1999);

conservazione in forma cifrata, indipendentemente dal formato di registrazione, delle tracce foniche e delle altre informazioni, in modo da impedirne l'ascolto (nel caso delle tracce foniche) o la intelligibilita' a soggetti non legittimati anche in caso di acquisizione fortuita o a seguito di guasti o interventi manutentivi sulle apparecchiature informatiche;

conservazione in forma cifrata delle eventuali copie di sicurezza (backup) dei dati allo stesso modo di quanto previsto per i dati on line; ogni altra estrazione di dati, anche parziale, su qualsiasi tipo di supporto removibile deve essere assistita da procedure crittografiche per la protezione dei contenuti;

trasmissione dei supporti e della documentazione cartacea (quali le trascrizioni del contenuto delle intercettazioni) all'Autorita' giudiziaria esclusivamente mediante personale di polizia giudiziaria;

designazione dei soggetti esterni all'Ufficio giudiziario e, in particolare, delle ditte operanti per conto delle Procure nell'ambito di appalti di fornitura di beni e di servizi informatici strumentali alla realizzazione delle intercettazioni o alla elaborazione delle informazioni intercettate, quali responsabili del trattamento ai sensi dell'art. 29 del Codice, ponendo particolare attenzione all'individuazione da parte del titolare dei profili di autorizzazione degli incaricati e delle misure di sicurezza, nonche' al controllo periodico sull'operato del responsabile esterno;

cancellazione sicura, alla cessazione del rapporto contrattuale, dei contenuti registrati nei server e negli altri apparati delle societa' noleggiatrici esterne che forniscono la strumentazione hardware.

b) Ai sensi dell'art. 154, comma 1, lett. c), del Codice, prescrive alle Procure della Repubblica di adottare le predette misure entro il termine di diciotto mesi, decorrente dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana, fornendo riscontro all'Autorita' circa la loro completa adozione entro il predetto termine.

c) Ai sensi del medesimo articolo, prescrive alle Procure della Repubblica di riferire all'Autorita', entro la data del 30 giugno 2014, sullo stato di avanzamento dell'attuazione di dette misure.

d) Dispone che copia del presente provvedimento venga inviata al Ministero della giustizia, segnalando la necessita' di fornire alle Procure della Repubblica le risorse idonee a consentire a detti Uffici di apportare le modificazioni e integrazioni indicate nel presente provvedimento volte a rafforzare la sicurezza nel trattamento dei dati personali e dei sistemi nell'ambito delle

attivita' di intercettazione.

e) Dispone che copia del presente provvedimento venga inviata al Consiglio superiore della magistratura, per ogni opportuna conoscenza in relazione alle relative attribuzioni, nonche' per l'adozione di ogni iniziativa ritenuta idonea a favorire la massima diffusione presso gli Uffici giudiziari interessati.

f) Dispone di trasmettere al Ministero della giustizia - Ufficio pubblicazione leggi e decreti copia del presente provvedimento per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 18 luglio 2013

Il presidente e relatore: Soro

Il segretario generale: Busia