Garante della privacy - Deliberazione del 25 giugno 2015 [4120817]

Ulteriore differimento dei termini di adempimento delle prescrizioni di cui al provvedimento del 18 luglio 2013, in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica.

di Giovanni Nazzaro

ULTERIORE DIFFERIMENTO IN MATERIA DI MISURE DI SICUREZZA NELLE ATTIVITÀ DI INTERCETTAZIONI

***Giovanni NAZZARO**, ing. delle telecomunicazioni, opera nell'information technology e nelle reti di telecomunicazioni ed è esperto in security e compliance in tali ambiti, con particolare riferimento alle c.d. "Prestazioni obbligatorie per l'Autorità Giudiziaria". È stato tra i fondatori dell'associazione Experts of Lawful Interception and Security Standards (ELISS), di cui è Presidente. È Direttore responsabile delle riviste tecnico-giuridiche "Sicurezza e Giustizia" e "Il Documento Digitale". È Direttore della "Lawful Interception Academy". Docente a contratto, autore di monografie e numerosi articoli, è ospite di seminari e convegni in qualità di relatore o moderatore.*

1. *Introduzione*

Il pervadere delle nuove tecnologie nella nostra sfera privata ha sempre più aumentato il bisogno di protezione nel quale si cerca di creare un collegamento che soddisfi reciprocamente le ragioni della sicurezza, della giustizia, ma anche dell'informazione e della tutela della riservatezza. In tale contesto, negli anni passati dobbiamo rilevare il lavoro svolto dal nostro Garante della protezione dei dati personali che è intervenuto in tali settori con specifici provvedimenti, a volte in periodi storici nei quali i poteri a lui attribuiti probabilmente sono apparsi non del tutto adeguati considerando la complessità del fenomeno ed il quadro normativo vigente. Sul fronte della sicurezza, con particolare riferimento alla raccolta dei dati per finalità di polizia, è indubbia l'attenzione che il Garante ha posto nei confronti delle banche dati, anche appoggiata dai vari atti normativi e di altra natura formalizzati in materia di scambi di dati e di cooperazione internazionale. Sul versante della giustizia, l'attività è stata parimenti intensa poiché ispirata dall'esigenza di un rafforzamento del livello di protezione dei dati personali in un cotesto di una giustizia che lentamente si avvia ad essere sempre più "tecnologica".

2. *Il provvedimento del 18 luglio 2013*

Uno degli ultimi interventi in materia riguarda la prescrizione del 18 luglio 2013 alle Procure della Repubblica, in merito a misure e accorgimenti per incrementare la sicurezza dei dati personali raccolti e usati nello svolgimento delle intercettazioni. L'intervento seguiva l'indagine conoscitiva svolta nel 2012 presso un campione di Procure della Repubblica di medie dimensioni (Bologna, Catanzaro, Perugia, Potenza e Venezia) allo scopo di valutare le misure tecnologiche e organizzative adottate negli Uffici giudiziari nell'attività di intercettazione telefoniche e telematiche.
È utile ricordare che l'intervento si pone cronologicamente dopo il provvedimento verso i principali gestori di telefonia fissa e mobile, risalente al 15 dicembre 2005, riguardo alle modalità con cui essi adempiono alle richieste dell'Autorità Giudiziaria (AG) in materia di intercettazione. In modo del tutto logico, quindi, l'attenzione del Garante si è soffermata prima sulla sfera in cui l'intercettazione viene eseguita tecnicamente ed ha inizio in modo strumentale rispetto a quanto disposto dalla stessa AG, ed un secondo momento all'ambito in cui l'intercettazione è ricevuta, archiviata e analizzata. Tra il 2005 ed il 2013 l'attenzione del Garante sul tema è rimasta immutata, come lo dimostra il provvedimento di carattere generale del 17 gennaio 2008 - poi modificato il 24 luglio 2008 - per la messa in sicurezza dei dati di traffico telefonico e Internet che vengono conservati dai gestori per finalità di accertamento e repressione dei reati, che seguiva i provvedimenti verso i singoli gestori (10 gennaio 2008).

Con il provvedimento del 18 luglio 2013 Il Garante ha dunque prescritto alle Procure una serie di stringenti misure da adottare entro 18 mesi dalla pubblicazione in GU. Le misure riguardano sia i Centri Intercettazioni Telecomunicazioni (CIT) situati presso ogni Procura sia gli Uffici di polizia giudiziaria delegata all'attività di intercettazione, e possono così essere raggruppati:

1. Misure di sicurezza fisica

Il Garante ha richiamato i titolari del trattamento dei dati svolto all'interno della struttura denominata Centro Intercettazioni Telecomunicazioni (CIT) al rispetto degli obblighi di sicurezza di cui all'art. 31 del Codice, valutando l'idoneità delle misure in essere e di quelle che potranno essere adottate alla luce di un'analisi dei rischi incombenti sui dati. Nel CIT infatti si svolgono le attività connesse all'effettuazione delle intercettazioni. La struttura è costituita dai locali ove sono situate le postazioni di ascolto, gli apparati su cui vengono ricevute le comunicazioni intercettate e che gestiscono le informazioni documentali relative, gli apparati per la l'archiviazione e per la conservazione delle copie di sicurezza (backup). Fisicamente nei CIT vengono usualmente compresi anche uffici tecnici e amministrativi dove vengono effettuate le operazioni di attivazione, proroga e chiusura delle attività di intercettazione.

In questi locali devono essere previsti principalmente: impianti per il rilevamento e l'estinzione di incendi; misure di protezione e idonee serrature di sicurezza alle finestre dei locali; strumenti per il monitoraggio dei locali attraverso l'adozione di impianti di videosorveglianza a circuito chiuso, ivi incluse le sale di ascolto, con registrazione delle immagini; accesso fisico alle sale di ascolto consentito, in alternativa, attraverso procedure di identificazione con dispositivi biometrici oppure tramite l'utilizzo di *badge* individuali e nominalmente assegnati; accesso fisico ai locali ove sono collocati i *server* e gli archivi tramite l'utilizzo di dispositivi biometrici; registrazione automatica degli accessi ai locali.
Oltre alle misure di sicurezza di carattere fisico devono essere previste anche quelle di natura organizzativa quantomeno contro i rischi di accesso abusivo e contro quelli derivanti da altri fattori suscettibili di incidere sulla integrità e disponibilità dei dati personali.

2. Misure di sicurezza informatica

Le misure di sicurezza classificate di tipo informatico e prescritte dal Garante possono essere suddivise concettualmente in tre macrocategorie:
a) Accesso ai sistemi e autenticazione: accessi ai sistemi consentiti solo da postazioni preventivamente abilitate e censite; autenticazione tramite procedure di *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.

b) Trasmissione delle informazioni: comunicazioni elettroniche tra l'AG e i gestori effettuate esclusivamente in modo cifrato e che assicurino l'identificazione delle parti comunicanti, l'integrità e la protezione dei dati; collegamenti telematici tra Procure della Repubblica e Uffici di polizia giudiziaria di tipo "punto-punto" dedicato o di tipo VPN (*Virtual Private Network*); trasmissione cifrata delle comunicazioni telematiche intercettate; trasmissione dei supporti e della documentazione cartacea all'AG esclusivamente mediante personale di polizia giudiziaria.

c) Conservazione delle informazioni: protezione dei documenti informatici trasferiti su supporti rimovibili con idonee tecniche crittografiche; effettuazione delle operazioni di "masterizzazione" solo quando strettamente indispensabili; annotazione in registri informatici con tecniche che ne assicurino la inalterabilità dell'esecuzione delle operazioni svolte nell'ambito delle attività di intercettazione sia presso i CIT sia presso gli Uffici di polizia giudiziaria; conservazione in forma cifrata delle intercettazioni e delle eventuali copie di sicurezza (backup); cancellazione sicura dei contenuti registrati nei *server* e negli altri apparati delle società noleggiatrici esterne alla cessazione del rapporto contrattuale.

3. *La nomina a "Responsabile del trattamento"*

Nel suo provvedimento il Garante affronta il rapporto con i soggetti esterni all'Ufficio giudiziario nel quadro dei ruoli previsti dal Codice, con particolare riferimento alle 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.
Il Garante ha prescritto che soggetti esterni vengano designati dal titolare 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, nonché al controllo periodico sull'operato del responsabile (esterno).
Questo aspetto merita un approfondimento a parte, considerando che a parità di Ufficio giudiziario c'è più di una società esterna operante per conto della Procura. Questo tuttavia non costituisce una criticità poiché il titolare può liberamente decidere che "*Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.*" (art. 29.3 – D.Lgs 196/03). L'aspetto rilevante è che "*I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare*" e che "*Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*" (artt. 29.4 e 29.5 – D.Lgs 196/03). Un buon modello di applicazione concreta al caso, già applicato in alcune PA, potrebbe essere quello di prevedere un responsabile interno e tanti responsabili esterni coincidenti con il rappresentante legale della rispettiva società. Nel rapporto tra titolare e responsabile esterno andrebbero elencate in modo dettagliato tutte le attività previste dal servizio, tra cui l'individuazione degli "incaricati al trattamento". A tal proposito Giova ricordare che il Garante nelle misure di sicurezza fisica nel provv. del 18 luglio prevedeva che in caso di operazioni di manutenzione e interventi tecnici da parte di ditte esterne, **al personale di quest'ultime deve essere inibito l'accesso a dati, informazioni e documenti prodotti, se non nei limiti strettamente necessari al compimento degli interventi di manutenzione**.

4. *Provvedimento del 26 giugno 2014*

Con il successivo provvedimento del 26 giugno 2014 il Garante ci ha reso noto di aver segnalato al Ministero di Giustizia la necessità di fornire alle Procure della Repubblica le risorse idonee a consentire le modificazioni e integrazioni indicate nel provvedimento e che lo stesso Ministero ha istituito un gruppo di lavoro per l'attuazione del provvedimento, del quale il Garante è stato chiamato a far parte. È stata quindi intrapresa una ricognizione riguardo alle condizioni di adeguatezza strutturale e organizzativa degli Uffici giudiziari requirenti di primo grado e agli interventi di adeguamento resi necessari dal provvedimento dell'Autorità, in modo coerente con le finalità di razionalizzazione organizzativa e contenimento dei costi correlate al progetto della cd. "gara unica nazionale delle intercettazioni". Il Ministro ha sottoposto al Garante l'opportunità di disporre un congruo differimento dei termini indicati nel provvedimento del 18 luglio 2013 che prevedeva l'adeguamento entro diciotto mesi dalla pubblicazione in G.U., cioè entro febbraio 2015. Il Garante ha differito al 30 giugno 2015 il termine assegnato.

5. *Deliberazione del 25 giugno 2015*

Veniamo quindi a giorni più recenti, quando con la deliberazione del 25 giugno 2015 il Garante ci informava che il 29 ottobre 2014 il Dipartimento dell'Organizzazione Giudiziaria del Personale e dei Servizi del Ministero di Giustizia ha trasmesso allo stesso la documentazione pervenuta relativa al monitoraggio dello stato di attuazione delle misure, stimando altresì i relativi costi. Tra le note riferite nella deliberazione, c'è quella del 10 giugno 2015 della Direzione Generale per i Sistemi Informativi Automatizzati, che "*indica i tempi di possibile attuazione delle misure di sicurezza informatiche prescritte nel provvedimento del 2013, da un lato evidenziando l'esigenza di adeguare entro il 31 dicembre 2015 i contratti in essere con le società fornitrici dei beni e servizi necessari per le intercettazioni, nonché di utilizzare risorse, anche umane, non attualmente disponibili, e dall'altro rappresentando in quale misura le prescrizioni in parola sono state sin qui attuate*". Ritenendo di dover riconoscere priorità alle misure di tipo logico-informatico, caratterizzate da minor costo e massima resa, il Garante ha sospeso il termine per l'attuazione delle misure prescritte ad eccezione di:

- 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 CIT;
- annotazione in registri informatici, con tecniche che ne assicurino la inalterabilità, con indicazione dei riferimenti temporali relativi alle attività svolte e al personale operante, dell'esecuzione delle operazioni svolte nell'ambito delle attività di intercettazione sia presso i CIT;

per le quali il termine è fissato al 31 luglio 2016. Entro tale termine il Garante si è riservato comunque di rivalutare la rilevanza delle misure sospese alla luce delle iniziative che saranno state nel frattempo intraprese dal Ministero.

6. *Il programma ELCAP dell'ELISS*

Nel contesto appena descritto, un'importante iniziativa a sostegno della regolamentazione del settore è arrivata dall'Associazione ELISS (*Experts of Lawful Interception and Security Standards*) nata nel 2005 con lo scopo di "*promuovere e di diffondere la conoscenza delle raccomandazioni e delle specifiche tecniche in ambito di intercettazione delle telecomunicazioni richieste dall'Autorità Giudiziaria, ivi compreso l'ambito della data retention, della sicurezza dei sistemi informativi e delle reti di telecomunicazioni, fornendo un ausilio alla loro corretta analisi e interpretazione*" (rif. art. 4 Statuto http://www.eliss.org/index.php/statuto/). Fondata nella forma di associazione *no profit*, libera e non di categoria, aperta a soggetti giuridici pubblici e privati, ELISS ha dato vita negli ultimi anni ad una serie di iniziative volte sia a far conoscere le raccomandazioni tecniche del settore sia a declinarle opportunamente sotto il profilo pratico indicando, laddove possibile, un modello di lavoro di riferimento ispirato ai principi della standardizzazione e delle *best practices*.

MARKUP 2° LIV.	MARKUP 3° LIV.	TIPO	DESCRIZIONE
VersionLog		Obblig.	Versione del log utilizzata
TimeStampLog		Obblig.	Data Ora nel formato UTC (es. `2001-10-26T21:32:52+02:00` oppure `2002-01-18T11:00:00-01:00`) in cui è stato prodotto il Log
VendorLemf		Obblig.	Costruttore del LEMF
VersionLemf		Obblig.	Versione del LEMF
Country		Opzion.	Paese in cui opera il LEMF
User	IpLemfClient	Obblig.	IP della postazione Client su cui è avvenuta l'autenticazione dell'Operatore
	IPLemfServer	Obblig.	IP del Server dell'archiettura del LEMF che ha concesso l'autenticazione dell'Operatore
	IPEsternal	Obblig.	IP della postazione esterna all'architettura della Procura che ha avuto accesso ai dati del LEMF
	TypeUser	Obblig.	Tipologia di utenza per la quale è stato prodotto il Log: 1. **Operator** per l'Operatore di PG, 2. **M2M** per collegamenti tra Client e Server, 3. **Admin** per lAmministraore di sistema
	UserIdentity	Obblig.	Tutti i dati identificativi dell'utente (matricola, user-id, nome, cognome, ecc..)
	TimeStampUserStart	Obblig.	Data Ora nel formato UTC (es. `2001-10-26T21:32:52+02:00` oppure `2002-01-18T11:00:00-01:00`) in cui è iniziata l'attività dell'utente (LogIn)
	TimeStampUserEnd	Obblig.	Data Ora nel formato UTC (es. `2001-10-26T21:32:52+02:00` oppure `2002-01-18T11:00:00-01:00`) in cui è terminata l'attività dell'utente (LogOut)
UserActivity	TypeOfActivity	Obblig.	Macro descrizione dell'attività svolta. 1. Per **Operator**: Activation of monitoring, Termination of monitoring, Modify Warrant Data, Audit (ascolto, visualizzazione dati intercettazione), Update Monitoring Data (brogliaccio) Export Data, Monitoring Status List, Delete Data, LEMF Administration 2. Per **M2M**: Transmitting client-server data, Generic interworking 3. Per **Admin**: Database administration, Application administration, Stop/Restart Collecting data, Stop/Restart Lemf, View Status Lemf, View Warrant Data, View Monitoring Data, Update SW.
	ContentOfActivity	Obblig.	Descrizione estesa dell'attività con l'indicazione del target e dell'autorizzazione (Registro generale e Registro Intercettazioni).
	TimeStampActivity	Obblig.	Data Ora nel formato UTC (es. `2001-10-26T21:32:52+02:00` oppure `2002-01-18T11:00:00-01:00`) dell'attività svolta.
Error		Obblig.	Da valorizzare in caso di errore con la descrizione del problema.

Tabella 1 - Formato XML del log delle attività dell'apparato per le intercettazioni (rif. http://www.eliss.org/)

Una delle ultime attività condotte dall'ELISS è l'ELCAP, acronimo di ***Eliss Lemf Conformity Assessment Program*** (http://www.eliss.org/index.php/certificazione-apparati-per-la-lawful-interception/), ovvero un programma di attestazione di possesso da parte dell'apparato deputato alla raccolta dei risultati delle intercettazioni (LEMF) di determinati requisiti funzionali e di sicurezza, ispirati dalle *best practices*, dagli standard internazionali in materia, dalle norme e dalle leggi nazionali ed europee e dai provvedimenti del nostro Garante della privacy. Benché al momento la conformità può essere autodichiarata dal costruttore dell'apparato, è indubbio che per la prima volta in Italia sono stati definiti i requisiti tecnici che devono possedere tali apparati, considerando che essi costituiscono l'unico strumento a disposizione della Polizia Giudiziaria che possa conservare i dati intercettati, elaborarli e presentarli in una forma intellegibile ed utile alle indagini. È chiaro, pertanto, che il loro mancato funzionamento, o il funzionamento non corretto, mette in serio rischio le indagine stesse, oltre a far venir meno le necessarie garanzie per le parti coinvolte.
I requisiti sono stati suddivisi in quattro livelli:

1. liceità del software di base;
2. aderenza agli standards tecnici internazionali ETSI;
3. aderenza alle linee guida di ELISS sulla visualizzazione dei contenuti;
4. aderenza alle linee guida di ELISS sulla sicurezza delle operazioni di mantenimento ed esportazione dei dati, di tracciamento delle operazioni sugli apparati.

Il lavoro di definizione dell'ELCAP è durato due anni e, anche se altri aspetti dovranno essere meglio definiti come il collegamento protetto tra i gestori e gli apparati, ha prodotto a maggio di quest'anno il documento relativo al quarto livello relativo agli aspetti di sicurezza che ha tratto ispirazione proprio dal provvedimento del Garante in commento. In particolare il livello 4 dell'ELCAP riporta con sufficiente dettaglio implementativo (formato XML e schema XSD) l'elenco delle informazioni che dovranno essere tracciate relativamente alle attività svolte e al personale operante, dell'esecuzione delle operazioni (quali l'ascolto, la consultazione, la registrazione, la masterizzazione, l'archiviazione e la 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). Considerando che i requisiti sono stati definiti e condivisi tra le principali società italiane costruttrici di tali apparati, inevitabilmente gli uffici giudiziari potranno trarre massimo vantaggio, nonché anche un certo risparmio economico, nel dover trattare informazioni con modalità omogenee. ©