

LE MISURE DI SICUREZZA A TUTELA DELLA PRIVACY NELLE INTERCETTAZIONI TELEFONICHE

di Pierangela Rodilloso

SOMMARIO: 1. PREMESSA. 2. IL PROVVEDIMENTO DEL 15 DICEMBRE 2005. 3. LE MISURE A GARANZIA DELLA SICUREZZA DEI FLUSSI INFORMATIVI CON L'AUTORITÀ GIUDIZIARIA. 4. LE NUOVE MISURE CONCERNENTI GLI ASPETTI ORGANIZZATIVI DELLA SICUREZZA. 5. LA PROTEZIONE DEI DATI CONOSCIBILI DA PARTE DEGLI INCARICATI AL TRATTAMENTO. 6. IL NUOVO PROVVEDIMENTO DEL 20 SETTEMBRE 2006. 7. IL RECENTE DECRETO LEGGE N. 259/2006 CONTRO LE INTERCETTAZIONI ILLEGALI.

1. PREMESSA

Con provvedimento in data 20 settembre 2006 il Garante per la protezione dei dati personali (di seguito, per brevità, il "Garante"), ha prescritto ai gestori telefonici di adottare, entro 90 giorni dalla ricezione dello stesso, le misure di sicurezza volte a tutelare sia i dati personali che i flussi di informazioni oggetto delle attività di intercettazione disposte dalla magistratura.

Il provvedimento dello scorso settembre, reso ai sensi dell'art. 154, comma 1, lett c) del Codice della Privacy¹, trova giustificazione nella mancata, parziale o ritardata attuazione delle misure già contenute nel precedente provvedimento del 15 dicembre 2005. Quest'ultimo richiedeva ai gestori telefonici di attuare le misure di sicurezza prescritte entro il termine di 180 giorni dalla notifica dello stesso.

In particolare, nel provvedimento del 15 dicembre 2005, il Garante aveva previsto una serie di misure di natura sia organizzativa che tecnologica, volte a garantire un più elevato livello di sicurezza nello scambio di dati tra gestori telefonici e uffici giudiziari durante le attività di intercettazione telefonica.

La concessione di un ulteriore termine di 90 giorni nasce, quindi, dalla duplice esigenza di non pregiudicare le attività di legale intercettazione in corso e di consentire ai gestori telefonici il completamento degli adeguamenti prescritti, alcuni dei quali di difficile o più lenta adozione se non accompagnati da un contestuale adeguamento delle medesime misure da parte degli uffici giudiziari coinvolti nello scambio di informazioni².

2. IL PROVVEDIMENTO DEL 15 DICEMBRE 2005

¹ Decreto Legislativo n. 196/2003, art. 154 (*Compiti*), comma 1, lett. c): "Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'art. 143".

² Cfr. Garante per la protezione dei dati personali, Comunicato stampa del 25 settembre 2006, "Intercettazioni legali: Garante privacy ai gestori, proteggete i dati o rischiate il blocco".

Il provvedimento del 15 dicembre 2005 rappresenta il risultato dell'attività di accertamento avviata dal Garante a partire dal 2 agosto 2005 nei confronti dei principali fornitori di servizi di comunicazione elettronica, relativamente alle modalità di attuazione dei provvedimenti dell'autorità giudiziaria in materia di intercettazioni.

Dagli accertamenti condotti, è emersa la necessità di rafforzare la protezione dei dati raccolti dai gestori durante le attività di intercettazione disposte dalla magistratura, e ciò in considerazione della delicatezza delle informazioni trattate, con riguardo sia alla tutela dei diritti fondamentali delle persone coinvolte, che alla garanzia di segretezza delle indagini.

Occorre, infatti, rilevare che i gestori telefonici raccolgono ed elaborano dati personali di particolare delicatezza, tra i quali rientrano, a titolo esemplificativo, le informazioni relative all'identità dei soggetti sottoposti ad intercettazione, i dati di traffico telefonico o telematico, i dati di localizzazione geografica dell'utenza intercettata e perfino i dati relativi all'utilizzo dei servizi di messaggistica sms ed mms.

Ebbene, le attività di trattamento dei dati personali a fini di legale intercettazione possono essere svolte da parte dei gestori telefonici solo nella misura in cui avvengano nel pieno rispetto dei presupposti di liceità, correttezza e proporzionalità del trattamento stesso.

In particolare, infatti, l'art. 11 del Codice della Privacy prescrive a tutti i Titolari del trattamento di gestire i dati trattati in modo lecito e secondo correttezza³, e ciò al fine di evitare che l'elaborazione dei dati personali possa perseguire propositi dolosi o recare pregiudizio all'interessato⁴.

In relazione a quanto sopra esposto, i risultati degli accertamenti avviati dal Garante non hanno messo in luce profili di particolare illiceità nel trattamento dei dati personali da parte dei gestori: è emerso, infatti, che questi ultimi non vengono a conoscenza dei contenuti delle intercettazioni, poiché la linea di comunicazione dell'indagato viene duplicata e successivamente instradata verso il Centro Intercettazioni Telefoniche (CIT) indicato dall'autorità giudiziaria⁵.

Quindi, dalla documentazione acquisita nel corso degli accertamenti, è emerso che l'attività svolta dai fornitori di servizi di comunicazione elettronica riveste una funzione strumentale rispetto alle disposizioni dell'autorità giudiziaria penale.

Pur tuttavia, gli accertamenti condotti hanno evidenziato alcune criticità con riguardo, ad esempio, alle modalità di trasmissione all'autorità giudiziaria dei dati di traffico relativi ai servizi di messaggistica sms ed mms.

A tal proposito, infatti, uno dei fornitori coinvolti, TIM Italia S.p.A., ha posto in rilievo che, sebbene i gestori non abbiano alcuna possibilità di accedere al contenuto dei messaggi sms ed mms, nei casi in cui il Centro Intercettazioni Telefoniche indicato dall'autorità giudiziaria non sia dotato

³ Decreto Legislativo n. 196/2003, art. 11 (*Modalità del trattamento e requisiti dei dati*), comma 1, lett. a): "I dati personali oggetto di trattamento sono:

a) *trattati in modo lecito e secondo correttezza*".

⁴ Cr. sull'argomento P. Iamiceli, "Liceità, correttezza, finalità nel trattamento dei dati personali", in R. Pardolesi (a cura di), "Diritto alla riservatezza e circolazione dei dati personali", Vol. I, Milano, Giuffrè, 2003, pp. 419-435.

⁵ Cfr. Garante per la protezione dei dati personali, Comunicato stampa del 22 dicembre 2005, "Intercettazioni: il Garante ai gestori telefonici, maggiore sicurezza".

di risponditore idoneo a ricevere detti messaggi, alla documentazione di traffico viene abbinata la registrazione del testo del messaggio, per un tempo determinato.

Pertanto, in alcuni casi i messaggi vengono archiviati dal fornitore, in forma cifrata, per poi essere trasmessi all'autorità giudiziaria richiedente. In tali casi, quindi, il fornitore ha la possibilità di venire a conoscenza del contenuto delle comunicazioni⁶.

Un secondo aspetto critico, riscontrato nel corso degli accertamenti condotti dal Garante, attiene al contenuto delle informazioni raccolte dai gestori durante lo svolgimento di ulteriori operazioni, a supporto dell'attività investigativa. Tra queste rientrano, a titolo esemplificativo, le interrogazioni anagrafiche, la localizzazione dell'utenza, l'identificazione della linea chiamante o connessa, il tracciamento, la sospensione o limitazione dei servizi agli utenti, la documentazione del traffico pregresso contabilizzato e del traffico storico.

Ebbene, tali informazioni, selezionate secondo i criteri indicati dall'autorità giudiziaria e successivamente organizzate in tabulati, rimanendo nella disponibilità del fornitore, possono essere agevolmente conosciute dagli incaricati chiamati a svolgere le operazioni richieste⁷.

Dunque, alla luce delle criticità emerse, il Garante ha evidenziato la necessità di rafforzare il livello di sicurezza adottato dai fornitori nel trattamento dei dati personali per scopi di giustizia, prescrivendo l'adozione di accorgimenti e misure ulteriori rispetto a quelle già in uso, a garanzia della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione⁸.

In particolare, le misure prescritte dal Garante nel Provvedimento del 15 dicembre 2005 riguardano gli aspetti organizzativi della sicurezza, la sicurezza dei flussi informativi con l'autorità giudiziaria e la protezione dei dati trattati per scopi di giustizia.

3. LE NUOVE MISURE CONCERNENTI GLI ASPETTI ORGANIZZATIVI DELLA SICUREZZA

Sotto l'aspetto organizzativo, sebbene dagli accertamenti condotti non siano emersi particolari profili di illiceità nel trattamento dei dati, il Garante ha ritenuto opportuno incrementare il livello di sicurezza relativamente alle criticità riscontrate, prescrivendo ai gestori di conformarsi agli standard organizzativi di seguito descritti:

- l'adozione di un modello organizzativo tale da limitare al minimo la conoscibilità delle informazioni trattate per scopi di giustizia;
- l'individuazione più selettiva del numero di incaricati designati a trattare i dati;
- un maggiore scrupolo nelle verifiche delle credenziali di autenticazione per l'accesso informatico ai dati trattati;

⁶ Garante per la protezione dei dati personali, Provvedimento del 15 dicembre 2005, "Nuove misure di sicurezza presso i gestori per le intercettazioni", in Bollettino n. 67/dicembre 2005, par. 1.

⁷ Garante per la protezione dei dati personali, Provvedimento del 15 dicembre 2005, "Nuove misure di sicurezza presso i gestori per le intercettazioni", in Bollettino n. 67/dicembre 2005, par. 2.

⁸ Costituzione della Repubblica Italiana, art. 15: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.

La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

- la realizzazione di una marcata separazione tra i dati di carattere amministrativo-contabile e i dati di carattere documentale, elaborati durante le attività svolte su richiesta dell'autorità giudiziaria, inibendo l'accesso a queste ultime informazioni a tutti gli operatori amministrativo-contabili;
- l'adozione di procedure di autenticazione maggiormente rigorose per l'accesso ai sistemi informatici di protocollazione ed archiviazione dei documenti scambiati con l'autorità giudiziaria, anche ricorrendo a caratteristiche biometriche⁹.

4. LE MISURE A GARANZIA DELLA SICUREZZA DEI FLUSSI INFORMATIVI CON L'AUTORITÀ GIUDIZIARIA

Le attività di legale intercettazione si basano su un continuo interscambio di informazioni tra i gestori telefonici e l'autorità giudiziaria. Il Garante, pertanto, a garanzia della riservatezza delle comunicazioni, ha prescritto ai gestori di controllare con maggior rigore tali flussi informativi.

In particolare, fin dal momento di ricezione in copia del decreto di "inizio attività", i fornitori di servizi di telefonia dovranno verificare con maggiore accuratezza l'autenticità e la sussistenza dei requisiti formali della richiesta, nonché la loro completezza, al fine di evitare che possa essere dato seguito a richieste da parte di soggetti non legittimati.

Il Garante ha altresì prescritto ai gestori di veicolare le informazioni all'autorità giudiziaria attraverso sistemi di comunicazione basati su protocolli di rete sicuri ed utilizzando, inoltre, tecniche di firma digitale per la cifratura dei documenti.

Infine, nel caso in cui la trasmissione dei dati all'autorità giudiziaria avvenga attraverso lo strumento della posta elettronica, si prescrive ai gestori l'utilizzo in via esclusiva della posta elettronica certificata (PEC)¹⁰, limitando l'uso di mezzi di trasmissione meno sicuri, quali ad esempio il telefax analogico, ai soli casi di materiale impossibilità tecnica di utilizzare i canali sicuri appositamente predisposti. Il Garante precisa, inoltre, che l'eventuale consegna manuale della documentazione deve avvenire sempre tramite soggetti delegati dall'autorità giudiziaria, annotandone le operazioni in un apposito registro delle consegne¹¹.

5. LA PROTEZIONE DEI DATI CONOSCIBILI DA PARTE DEGLI INCARICATI AL TRATTAMENTO

Uno dei profili critici emersi all'esito degli accertamenti condotti dal Garante a partire dal 2 agosto 2005 concerne la conoscibilità, da parte degli incaricati al trattamento dei dati presso i gestori, di molteplici informazioni raccolte nel corso delle attività di legale intercettazione.

⁹ Garante per la protezione dei dati personali, Provvedimento del 15 dicembre 2005, "Nuove misure di sicurezza presso i gestori per le intercettazioni", in Bollettino n. 67/dicembre 2005, par. 3.1.

¹⁰ Si segnala in proposito che la posta elettronica certificata (PEC) è stata istituita con il D.P.R. 11 febbraio 2005, n. 68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3 (G.U. n. 97 del 28 aprile 2005). In particolare, il sopra citato D.P.R. all'art. 2, lett. g) definisce la posta elettronica certificata come "ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici".

¹¹ Garante per la protezione dei dati personali, Provvedimento del 15 dicembre 2005, "Nuove misure di sicurezza presso i gestori per le intercettazioni", in Bollettino n. 67/dicembre 2005, par. 3.2.

Ebbene, nel chiaro intento di evitare ogni possibile violazione della riservatezza di tali informazioni, il Garante ha prescritto ai gestori di telefonia di incrementare, attraverso l'utilizzo di appropriati strumenti informatici, il controllo delle attività svolte dagli incaricati al trattamento sui dati personali raccolti ed elaborati per scopi di giustizia.

In particolare, con il provvedimento del 15 dicembre 2005 il Garante ha richiesto ai gestori di adottare tecniche di cifratura tali da precludere la conoscenza dei dati trattati per scopi di giustizia a tutti quei soggetti non legittimati ad accedervi.

Infine, il Garante ha evidenziato l'esigenza di limitare la presenza dei dati personali nel sistema informativo del fornitore per il periodo strettamente necessario all'attuazione delle finalità di giustizia, con conseguente obbligo di cancellazione immediata una volta comunicati all'autorità giudiziaria richiedente¹². E ciò anche alla luce del più generale principio di necessità del trattamento, consacrato dall'art. 3 del Codice della Privacy con espresso riferimento ai trattamenti effettuati mediante l'impiego di sistemi informativi e programmi informatici¹³.

6. IL NUOVO PROVVEDIMENTO DEL 20 SETTEMBRE 2006

Il provvedimento del 15 dicembre 2005 prescriveva ai gestori telefonici di adeguarsi alle norme di sicurezza in esso contenute entro il termine di 180 giorni dalla ricezione dello stesso.

Tuttavia, in alcuni casi non è risultato semplice per i gestori attuare le misure, tanto organizzative quanto tecnologiche, prescritte nel suddetto provvedimento. Ad esempio, come evidenziato da alcune compagnie telefoniche, alcune misure risultano di più difficile o lenta attuazione se non accompagnate da un contestuale adeguamento da parte degli uffici giudiziari coinvolti nello scambio di dati trattati nel corso delle attività di intercettazione.

Pertanto, con il nuovo provvedimento del 20 settembre 2006, il Garante, preso atto della mancata, parziale o ritardata attuazione del provvedimento del 15 dicembre 2005 e tenuto conto sia della delicatezza dei dati trattati, che della necessità di non pregiudicare le attività di intercettazione in corso, ha ritenuto opportuno concedere ai gestori un breve ed ultimo termine di 90 giorni per ultimare le procedure di adeguamento¹⁴.

Scaduto il suddetto termine - che decorre dalla ricezione del nuovo provvedimento da parte dei singoli destinatari - l'Autorità potrà vietare, ai gestori telefonici che non risulteranno in regola, le

¹² Garante per la protezione dei dati personali, Provvedimento del 15 dicembre 2005, "Nuove misure di sicurezza presso i gestori per le intercettazioni", in Bollettino n. 67/dicembre 2005, par. 3.3.

¹³ Decreto Legislativo n. 196/2003, art. 3 (*Principio di necessità nel trattamento dei dati*): "I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità". Cfr. sull'argomento R. Acciai e S. Melchionna, in R. Acciai (a cura di), *Il diritto alla protezione dei dati personali*, Maggioli Editore, 2003, p. 71.

¹⁴ Garante per la protezione dei dati personali, Provvedimento del 20 settembre 2006, "Intercettazioni telefoniche: monito del Garante", in Bollettino n. 75/settembre 2006.

operazioni di trattamento dei dati riferite alle attività di intercettazione, ai sensi dell'art. 154, comma 1, lett. d) del Codice della Privacy¹⁵.

Occorre, infine, segnalare che, entro il predetto termine di 90 giorni, i singoli gestori dovranno dare documentata conferma dell'integrale adempimento delle misure e degli accorgimenti prescritti con il nuovo provvedimento, con comunicazione da inoltrarsi al Garante, anche ai sensi e per gli effetti di cui all'art. 157 del Codice della Privacy¹⁶.

7. IL RECENTE DECRETO LEGGE N. 259/2006 CONTRO LE INTERCETTAZIONI ILLEGALI

Nell'intento di inibire l'illecita diffusione dei dati personali acquisiti attraverso la raccolta illegale di informazioni, il legislatore, con la recente Legge n. 281 del 20 novembre 2006 (pubblicata nella Gazzetta Ufficiale n. 271 del 21 novembre 2006), ha convertito con modificazioni il D.L. n. 259/2006, recante disposizioni urgenti per il riordino della normativa in tema di intercettazioni telefoniche¹⁷.

In particolare, il Decreto Legge sopra citato stabilisce, all'art. 1 (sostitutivo dell'art. 240 del codice di procedura penale) che *"il Pubblico Ministero dovrà disporre l'immediata secretazione e la custodia in luogo protetto dei documenti, dei supporti e degli atti concernenti dati e contenuti di conversazioni o comunicazioni relativi a traffico telefonico e telematico, illegalmente formati o acquisiti"*. Ed inoltre che *"allo stesso modo provvede per i documenti formati attraverso la raccolta illegale di informazioni"* (art. 1, comma 2).

L'art. 1 del provvedimento suddetto prescrive, altresì, il divieto sia di effettuare copia, in qualunque forma e in qualunque fase del procedimento, dei documenti illegalmente formati, che di utilizzarne il contenuto (art. 1, comma 2).

Occorre, inoltre, evidenziare che il nuovo Decreto Legge stabilisce, tra l'altro, che sia il giudice per le indagini preliminari, su richiesta del Pubblico Ministero, a disporre in tempi rapidi e certi la distruzione delle intercettazioni illegalmente raccolte (art. 1, comma 5), e che delle operazioni di distruzione sia redatto apposito verbale (art. 1, comma 6).

Sotto l'aspetto sanzionatorio, il provvedimento prevede la reclusione da sei mesi a quattro anni per *"chiunque detiene consapevolmente gli atti, i supporti o i documenti di cui sia stata disposta la distruzione"* (art. 3, comma 1), mentre se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio *"si applica la pena della reclusione da uno a cinque anni"* (art. 3, comma 2).

¹⁵ Decreto Legislativo n. 196/2003, art. 154 (Compiti), comma 1, lett. d): *"Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporre il blocco ai sensi dell'art. 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali"*.

¹⁶ Decreto Legislativo n. 196/2003, art. 157 (Richiesta di informazioni e di esibizione di documenti): *"Per l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti"*.

¹⁷ Cfr. sull'argomento gli articoli: *"Approvato il decreto contro le intercettazioni illegali: fino a 5 anni di carcere"*, Il Sole 24 Ore - Norme & Tributi, 20 novembre 2006; *"Intercettazioni, approvato il decreto così i "verbali" verranno distrutti"*, La Repubblica - Cronaca, 19 novembre 2006.

Inoltre, nel caso in cui il contenuto di intercettazioni illecite venga pubblicato, a titolo di riparazione potrà essere richiesta all'autore della pubblicazione, al direttore responsabile e all'editore, in solido tra loro, *“una somma di denaro determinata in ragione di cinquanta centesimi per ogni copia stampata, ovvero da 50.000 a 1.000.000 di euro secondo l'entità del bacino di utenza ove la diffusione sia avvenuta con mezzo radiofonico, televisivo o telematico”*, e che *“in ogni caso, l'entità della riparazione non può essere inferiore a 10.000 euro”* (art. 4, comma 1).

Occorre, infine, rilevare che, ai sensi dell'art. 4, comma 3, del Decreto Legge, l'azione penale *“è esercitata senza pregiudizio di quanto il Garante per la protezione dei dati personali possa disporre ove accerti o inibisca l'illecita diffusione di dati o documenti, anche a seguito dell'esercizio di diritti da parte dell'interessato”*.