QUESTIONI APERTE

Intercettazioni telefoniche – «Pin to pin» Blackberry

La decisione

Intercettazione telefoniche – «Pin to pin» Blackberry – Comunicazioni o corrispondenza – Modalità di apprensione - Violazione delle norme sulle rogatorie internazionali - Insussistenza - Necessità di sequestro probatorio (C.p.p., artt. 266-*bis*, 268, 271, 254, 254-*bis*).

Le captazioni telematiche riguardanti lo scambio di messaggi fra telefoni "Blackberry" con il sistema c.d. "pin to pin" trasmessi dalla società con sede in Italia direttamente sul server degli uffici della Procura non comporta la violazione delle norme sulle rogatorie internazionali, in forza dell'istituto dell'"instradamento".

Le chat, anche non contestuali, costituiscono sempre comunicazioni, acquisibili esclusivamente attraverso attività di intercettazione, ex *art. 266*-bis *c.p.p., e non mediante sequestro* ex *art. 254*-bis.

La trasmissione diretta dei dati tra società italiana e server della Procura garantisce la immodificabilità degli stessi.

TRIBUNALE REGGIO CALABRIA, (ord.) 16 giugno 2015 – BENNATO, *G.U.P.* – Brandimarte, *imputato.*

Ancora in tema di *chat* "pin to pin" su sistema telefonico BlackBerry

1. La questione, portata all'attenzione del GUP distrettuale presso il Tribunale di Reggio Calabria, riguardava la acquisizione, da parte della PG, di conversazioni *chat* intercorse in data precedente alla emissione del decreto di intercettazione urgente, da parte del PM, emesso ai sensi dell'art. 266-*bis* c.p.p.

La difesa aveva eccepito la inutilizzabilità, per vizio genetico, del materiale probatorio raccolto.

Infatti, i dati telematici relativi alle *chat "pin to pin"*[1], criptati e conservati presso un server ubicato in Canada, erano stati acquisiti all'estero, senza l'espletamento di attività rogatoriali e secondo procedure che non ne garantivano la genuinità e la immodificabilità.

2. Il GUP rigettava l'istanza difensiva, argomentando che le acquisizioni probatorie, essendo avvenute per il tramite della "consorella" italiana della socie-

[1] Per completezza si veda nota di FILIPPI, *Questioni nuove in tema di intercettazioni: quid iuris sul "pin to pin" dei blackberry?*, in *questa Rivista* online, 2016; FURFARO, *Le intercettazioni "pin to pin" del sistema blackberry, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche, ivi*; e ROMOLI, Chat BlackBerry: *una prima pronuncia in sede di riesame cautelare che forse ha sottovalutato alcuni profili di criticità del fenomeno, ivi,* 2015.

tà Research in Motion LTD, con sede in Canada, ovvero la RIM srl, sedente in Milano, non potevano dirsi come avvenute all'estero e, pertanto, non dovevano essere eseguite per rogatoria.
Riteneva, in particolare, il Giudice che la società estera avesse riversato, spontaneamente, sul server della omologa italiana il traffico dati richiesto dalla Procura.
Successivamente, e sempre spontaneamente, la RIM srl avrebbe inviato i dati, previa decrittazione, al server nella disponibilità della A.G.
La "spontaneità" della consegna avrebbe reso superfluo il ricorso alla rogatoria.
Quanto alla garanzia di immodificabilità, il GUP motivava che la trasmissione dei dati, dal Canada alla RIM srl e da questa al server della Procura Distrettuale, era avvenuta con modalità di trasmissione diretta che "impediscono ogni manipolazione".

3. La soluzione adottata e le motivazioni ostese dal Giudice destano non poche perplessità.
La premessa dalla quale occorre muovere è che, nonostante le ripetute novelle legislative in tema di intercettazioni di conversazioni e comunicazioni, elementi indefettibili del meccanismo procedurale *ex* art. 266 c.p.p., chiamati a garantire nella sua massima espansione la prerogativa di tutela legata alla segretezza della corrispondenza, *ex* art. 15 Costituzione, restano la terzietà del soggetto captante e la contestualità dell'ascolto[2].
Nel caso di specie, in seguito ad un decreto d'urgenza del 27 giugno 2013 (convalidato dal GIP in data 29 giugno 2013), la P.G. ha acquisito una serie di *chat* "pin to pin", pregresse rispetto alla loro apprensione.
In esecuzione dell'ordine impartito, la RIM srl ha rimesso alla A.G., prima ricevendoli dalla consorella canadese e, successivamente, trasferendoli sul server messo a disposizione dalla Procura della Repubblica, i dati telematici.
Ora, la evidente mancanza di contestualità tra la conversazione, la sua captazione e la sua acquisizione fanno ritenere che non ci si trovi in presenza di una intercettazione di traffico telematico, disciplinata dagli artt. 266-*bis* e seguenti c.p.p., ma, piuttosto, di un sequestro di corrispondenza.
Infatti, la acquisizione di dati telematici già formati e già oggetto di operazioni di archiviazione di massa presso un server estero, è senz'altro maggiormente assimilabile ad una ablazione *ex* art. 254 c.p.p., che ad una intercettazione di conversazioni, *ex* artt. 266 e seguenti c.p.p.

[2] Cass., Sez. VI, 09 maggio 2014, X., in *Mass. Uff.,* n. 19237.

L'apprensione, infatti, cade, per usare l'espressione codicistica, su altri oggetti di corrispondenza, inoltrati per via telematica e detenuti da un soggetto che fornisce servizi telematici, ossia la SIM ltd, con sede in Canada.
L'adozione di un simile atto di indagine richiede l'esercizio dell'attività rogatoriale, apparendo inconferente il richiamo al c.d. "instradamento", grazie al quale i dati o i suoni, deviati su nodi di trasmissione nazionali, sono materialmente appresi mentre si trovano nei confini dello Stato.
Nella fattispecie considerata, infatti, i dati, partiti dal territorio nazionale e transitati all'estero, ove sono stati definitivamente immagazzinati, vengono *ivi* acquisiti, dopo essere stati memorizzati su supporti informatici.
Non convince, invece, il diverso divisamento espresso dal GUP, ed avallato dalla recentissima sentenza della Suprema Corte[3] a mente del quale le *chat*, anche non contestuali, sono da considerarsi un flusso di comunicazioni, la cui acquisizione è regolata dagli artt. 266-*bis* e seguenti del codice di rito penale.
Il Supremo Collegio, in particolare, giunge alla predetta conclusione dopo aver analizzato, in maniera peraltro davvero succinta, la diversità concettuale tra la nozione di "comunicazione" e quella di "dato telematico", termine, quest'ultimo, contenuto nell'art. 254-*bis* c.p.p.
La Corte, quindi, partendo dalla considerazione, in astratto condivisibile, che una *chat* costituisce una comunicazione e non un dato telematico, e ritenendo, di conseguenza, inapplicabile l'istituto del sequestro di dati informatici, elabora il principio di diritto in base al quale l'unica corretta modalità di apprensione delle conversazioni via *chat* sia l'intercettazione di comunicazioni informatiche e telematiche.
Tale principio è distonico rispetto al sistema normativo delineato dal codice di rito, perché, di fatto, presuppone la disapplicazione sistematica dell'art. 254 c.p.p., così come novellato dalla legge n. 48 del 2008.
Il testo della disposizione codicistica, a seguito dell'intervento del Legislatore, contempla oggi la possibilità di apprendere, con le modalità del sequestro, qualsiasi "oggetto di corrispondenza", anche se inoltrato per via telematica.
È chiaro allora che l'aspetto problematico delle conclusioni assunte dalla Suprema Corte sta nell'aver posto in termini di alternatività l'istituto delle intercettazioni di comunicazioni telematiche, con quello della acquisizione di dati telematici, senza considerare il sequestro di corrispondenza.
Premessa che ha condotto la Cassazione a concludere che una *chat* debba, di necessità, essere assimilata ad un flusso di comunicazioni e ad escludere, di converso, che possa essere considerata alla stregua di una corrispondenza pri-

[3] Cass., Sez. III, 23 dicembre 2015, in proc. Guarnera, in *Mass. Uff.* n. 50452.

vata.
Conclusione che stride, peraltro, con la pacifica giurisprudenza di legittimità in tema, ad esempio, di diffamazione o di tutela della segretezza delle comunicazioni, che, invece, considera le *chat* (ad eccezione di quelle "pubbliche") come corrispondenza privata, al pari delle mail[4].
La distinzione tra "dato informatico" e "comunicazione informatica", pur corretta, non può in definitiva condurre alla apprensione dei flussi di *chat* con il solo strumento della intercettazione, dal momento che il codice di rito prevede, espressamente, la possibilità di sottoporre gli stessi a sequestro *ex* art. 254 c.p.p.
Il discrimine tra i due istituti, dunque, rimane sempre quello della contestualità, dovendosi applicare il sequestro di corrispondenza telematica, nel caso di comunicazioni non contestuali, e l'intercettazione telematica, in caso di captazione in tempo reale del flusso di dati comprendente oggetti di corrispondenza.

4. Sotto altro profilo, a prescindere dallo strumento procedurale adottato per la apprensione delle comunicazioni, non convince la motivazione adottata dal GUP, in ordine all'eccepita mancata formazione di una copia dei dati acquisiti, con modalità tali da garantirne la conformità all'originale.
Pur essendo evidente che la duplicazione, estrazione e trasmissione dei dati è avvenuta senza alcun controllo (o senza che tale controllo sia stato reso ostensibile e, quindi, verificabile per le Difese) che garantisse la intangibilità del dato telematico, in aperta violazione della normativa comunitaria, recepita in Italia con legge n. 48 del 2008, modificativa del codice di rito penale, il Giudice si limita ad affermare, in modo meramente assertivo, che tale modalità di acquisizione garantisce la immodificabilità dei dati.
In realtà, senza positivo accertamento delle concrete modalità di estrazione, duplicazione e conservazione dei dati, deve dirsi, interrotta o, comunque, non garantita la "catena di custodia", che presuppone la conservazione dell'originale, la ripetibilità del procedimento di estrazione delle copie, la conformità delle copie all'originale mediante la cosiddetta "validazione giuridica", ovvero attraverso l'attribuzione alla copia della medesima firma digitale (codice fisso contraddistinto dall'*algoritmo di hash*) generata dall'originale.
Non è ultroneo osservare che la *ratio legis*, che ha ispirato la riforma del 2008, è quella di rendere verificabile e sempre ripetibile il procedimento di copia dei dati acquisiti.

[4] Cass., Sez. V, 11 dicembre 2007, P.G. in proc. Tramalloni, in *Mass. Uff.,* n. 238284.

È evidente, invece, che la mancata conservazione dei dati originali e la mancata certificazione di conformità delle copie rendono, da un lato, incerta e non verificabile la regolarità del procedimento di estrazione, che, dall'altro, diviene atto irripetibile.
Ciò tanto più se si pone mente alla circostanza che tali flussi telematici sono criptati e risultano intellegibili solo se sottoposti al programma di decrittazione detenuto (in esclusiva) dalla RIM srl.
Di talché qualsiasi, anche minima, modificazione del dato originale può comportare sensibili alterazioni del contenuto dello stesso.

5. A diversa conclusione non si perverrebbe, peraltro, neanche qualificando la attività di indagine preliminare quale intercettazione di comunicazioni telematiche, *ex* art. 266-*bis* c.p.p.
Anche in questo caso, infatti, mancherebbe qualsiasi attività, condotta personalmente dal PM o da un ufficiale di P.G., finalizzata ad attestare la tracciabilità scientifica della prova, ovvero che la acquisizione dei dati è avvenuta con modalità tali da assicurarne la genuinità e la immodificabilità, così da consentirne la verifica e la ripetibilità.
Attività che l'art. 267, co. 4, c.p.p. riserva al Pubblico Ministero o ad un Ufficiale di PG, nell'esercizio di una funzione di garanzia per l'indagato, che non ammette modalità equipollenti.

6. È necessario, in definitiva, che si proceda ad una corretta ermeneusi delle norme del codice di rito relative alla apprensione di corrispondenza telematica, per discernere (e motivare correttamente tale discernimento) i casi nei quali si debba procedere ad intercettazione di comunicazioni, da quelli nei quali, invece, si debba adottare un sequestro di corrispondenza.

GIANCARLO PITTELLI
FABRIZIO COSTARELLA