QUESTIONI APERTE

Intercettazioni telefoniche – «*Pin to pin*» *blackberry*

La decisione

Intercettazioni telefoniche – «*Pin to pin*» *blackberry* – Chat Blackberry – Rogatorie internazionali – Istradamento (C.p.p., artt. 266 ss. c.p.p.).

*In materia di acquisizione dei dati telematici relativi alla messaggistica fra telefoni "*Blackberry*" con il sistema "*pin to pin*", al pari delle tradizionali intercettazioni telefoniche, il ricorso alla procedura dell'istradamento - e cioè il convogliamento delle chiamate in partenza dall'estero in un nodo situato in Italia (nonché di quelle in partenza dall'Italia verso l'estero, confluite a mezzo del gestore sito nel territorio nazionale) – non comporta la violazione delle norme sulle rogatorie internazionali, poiché in tal modo tutta l'attività d'intercettazione, ricezione e registrazione delle telefonate viene interamente compiuta nel territorio italiano, mentre il ricorso alle forme dell'assistenza giudiziaria è necessario unicamente per gli interventi da compiersi all'estero, per l'intercettazione di conversazioni captate dal solo gestore straniero.*

CASSAZIONE PENALE, SEZIONE SESTA, 30 settembre 2015 (c.c. 22 settembre 2015) – AGRÒ, *Presidente* – DE AMICIS, *Relatore* – PINELLI, *P.M.* (diff.) – Petrusic, ricorrente.

Questioni nuove in tema di intercettazioni: *quid iuris* sul "*pin to pin*" dei *blackberry*?

1. La questione posta all'esame della Suprema Corte consisteva nella dedotta violazione di legge per aver utilizzato, nelle operazioni di intercettazione, impianti diversi da quelli in dotazione alla Procura e per l'omesso ricorso alla rogatoria alle autorità straniere (in particolare a quelle canadesi), poiché l'attività captativa era diretta a percepire contenuti di comunicazioni o conversazioni transitanti ed elaborati sul territorio straniero, attraverso *servers* ubicati tutti nel Canada, avendo le autorità italiane notificato i decreti autorizzativi ad una società esterna – con sede legale in Italia – fornitrice di servizi della società madre canadese, che aveva ideato e sviluppato un programma di messaggistica istantanea, utilizzata dagli indagati.

2. La Corte di cassazione risponde affermando, anzitutto, che «le operazioni di intercettazione sono avvenute in territorio italiano, tramite la registrazione dei dati nella memoria informatica centralizzata (*server*) installata nei locali della Procura di [...]». La Suprema Corte aggiunge che «i dati telematici delle

captazioni riguardanti lo scambio di messaggi fra telefoni "Blackberry" con il sistema c.d. "*pin to pin*" sono stati trasmessi in originale dalla società con sede in Italia direttamente sul *server* degli uffici della Procura, ove gli stessi si trovano attualmente custoditi, con possibilità di accesso e consultazione delle parti, a garanzia della genuinità della prova». Di conseguenza, richiamando il *dictum* delle Sezioni unite Carli del 2008, sarebbe stata «rispettata la condizione necessaria per l'utilizzabilità delle intercettazioni, ossia che l'attività di registrazione – consistente, sulla base delle tecnologie attualmente in uso, nella immissione dei dati captati in una memoria informatica centralizzata – avvenga nei locali della Procura della Repubblica mediante l'utilizzo di impianti ivi esistenti».
La pronuncia ribadisce un principio ormai consolidato in giurisprudenza in tema di intercettazioni telefoniche, secondo cui il ricorso alla procedura dell'istradamento, e cioè il convogliamento delle chiamate in partenza dall'estero in un nodo situato in Italia (e a maggior ragione di quelle in partenza dall'Italia verso l'estero, delle quali è certo che vengono convogliate a mezzo di gestore sito nel territorio nazionale) non comporta la violazione delle norme sulle rogatorie internazionali, poiché in tal modo tutta l'attività di intercettazione, ricezione e registrazione delle telefonate viene interamente compiuta nel territorio italiano, mentre il ricorso alle forme dell'assistenza giudiziaria all'estero è necessario unicamente per gli interventi da compiersi all'estero, per l'intercettazione di conversazioni captate solo da un gestore straniero.

3. Le argomentazioni e la soluzione offerta dalla sentenza annotata lasciano invero qualche perplessità.
È pacifico che trattandosi di *chat*, così come le *mail* ed i *social network*, si tratta di flusso di comunicazioni in corso relativo a sistemi telematici, per cui si tratta di intercettazione telematica alla quale deve applicarsi l'art. 266-*bis* c.p.p. e non di sequestro, mentre è l'art. 254-*bis* c.p.p., che non riguarda un flusso di comunicazioni, bensì i dati già detenuti da fornitori di servizi telematici su *hard disk* o altro supporto informatico, a disciplinare il sequestro.
È invece discutibile che le operazioni di intercettazione si possano considerare avvenute interamente in territorio italiano e che l'unica operazione compiuta sia stata la registrazione dei dati nella memoria informatica centralizzata (*server*) installata nei locali della Procura. Si perpetua, infatti, la giurisprudenza che ammette la procedura di intercettazione di flussi comunicativi su utenze mobili straniere, ricorrendo al cd. istradamento anziché procedere con la rogatoria, basandosi unicamente sul dato materiale del transito fisico, anche

parziale (magari solo a fini di fatturazione), della comunicazione in territorio italiano, anziché sull'aspetto sostanziale della lesione della segretezza delle comunicazioni viaggianti su linee anche di Paesi stranieri, ove si trovano i *server* che hanno gestito la comunicazione. La Corte di cassazione motiva al riguardo che i dati telematici delle captazioni riguardanti lo scambio di messaggi fra telefoni "*Blackberry*" con il sistema c.d. "*pin to pin*" sarebbero stati trasmessi in originale dalla società con sede in Italia direttamente sul *server* degli uffici della Procura. Ma in realtà vi è da dubitare che la succursale locale sia legittimata ad autorizzare l'acquisizione dei dati da essa detenuti, senza una formale decisione da parte della casa madre canadese, che non risulta nemmeno interpellata, nonostante sia l'unica abilitata e responsabile della detenzione e della gestione dei dati trattati.

In ogni caso è certo che gli impianti utilizzati per le intercettazioni non sono stati quelli installati presso la Procura della Repubblica, nel cui *server* – come riconosce la sentenza – è avvenuta soltanto la «registrazione dei dati nella memoria informatica centralizzata (*server*) installata nei locali della Procura». Infatti, l'art. 268, co. 3, c.p.p., coniato pensando soltanto alle intercettazioni telefoniche, impone l'impiego di «impianti installati nella procura della Repubblica», ma è ovvio che tutti gli impianti utilizzati per le operazioni di intercettazione (e quindi sia gli apparecchi di captazione, sia quelli di registrazione) devono essere installati presso la procura o almeno autorizzati e quindi sotto il controllo dalla stessa procura (compresi i terminali di captazione ambientale, informatica e telematica), dato che la *ratio* della disposizione è che solo in questo modo è garantito il controllo dell'autorità giudiziaria sulla regolarità delle operazioni di intercettazione. Non si comprende, infatti, per quale ragione le "microspie" o i dispositivi di acquisizione delle intercettazioni informatiche o telematiche dovrebbero essere sottratti al controllo dell'autorità giudiziaria. Invece, nella fattispecie concreta gli impianti utilizzati per la captazione delle comunicazioni telematiche furono dei privati (la società con sede in Italia e facente capo alla *Blackberry*), senza alcuna autorizzazione del pubblico ministero, come invece richiede il successivo co. 3-*bis*.

Inoltre, una siffatta acquisizione, con consegna diretta dei dati dalla succursale italiana all'autorità giudiziaria urta con diversi principi fondamentali del processo.

Anzitutto, non consente al difensore di chiedere al gestore la consegna dei dati detenuti, essendo per ogni tipo di intercettazione il potere di acquisizione riservato al monopolio del pubblico ministero, in spregio al principio del "contraddittorio tra le parti, in condizioni di parità davanti a giudice terzo e imparziale". Inoltre, tale procedura non offre alcuna trasparenza e quindi al-

cuna certezza sull'autenticità del contenuto dei messaggi inviati per *chat*, perché nessun controllo è possibile né sull'autenticità dei dati trasmessi da un privato senza alcun controllo, né sull'integrità della "catena di custodia" dei dati, né sull'identità e sull'attività svolta dal tecnico decifratore. Ancora, in nessuno di questi, fondamentali, segmenti procedurali (controllo sull'autenticità dei dati forniti da un privato, integrità della catena di custodia dei dati, identità e attività svolta dal tecnico decifratore) è ammesso alcun diritto di difesa, che pure sarebbe possibile senza compromettere le esigenze di indagine. Infine, la procedura di instradamento comporta il convogliamento di fasci di comunicazioni estranee alle indagini in un nodo posto in Italia, tra l'altro con rischio di possibile violazione della loro segretezza.
Il problema della protezione dei dati personali trasferiti è delicato e la sua importanza è stata avvertita di recente anche dalla Corte di Giustizia UE, che ha dichiarato invalida la decisione della Commissione europea che attesta che gli Stati Uniti garantiscono un adeguato livello di protezione dei dati personali trasferiti. In particolare, si afferma il principio per cui solo la Corte è competente a dichiarare invalido un atto dell'Unione, ma le autorità nazionali di controllo, investite di una domanda, possono, anche se esiste una decisione della Commissione che dichiara che un paese terzo offre un adeguato livello di protezione dei dati personali, esaminare se il trasferimento dei dati di una persona verso quel paese rispetta i requisiti della normativa dell'Unione sulla protezione di tali dati, nonché adire i giudici nazionali, allo stesso titolo della persona interessata, affinché procedano ad un rinvio pregiudiziale per l'esame della validità della decisione (Corte Giust. UE, 6 ottobre 2015, Schrems).

4. In conclusione, la giurisprudenza ricorre alla *fictio iuris* dell'istradamento soltanto al fine di evitare la più lunga procedura della rogatoria internazionale o quella prevista dalla direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014, relativa all'Ordine Europeo di Indagine penale, nonché le relative regole sull'attendibilità della prova e sulle garanzie della difesa.

LEONARDO FILIPPI