QUESTIONI APERTE

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

La decisione

Intercettazione telefoniche – «*Pin to pin*» *Blackberry* – Violazione delle norme sulle rogatorie internazionali – Insussistenza (C.p.p., artt. 266-*bis*, 268, 271).

*Le captazioni telematiche riguardanti lo scambio di messaggi fra telefoni "*Blackberry*" con il sistema c.d. "*pin to pin*" trasmessi in originale dalla società con sede in Italia direttamente sul server degli uffici della Procura 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 e l'acquisizione dei dati avviene col ricorso alla procedura dell'istradamento e cioè con il convogliamento delle chiamate in partenza dall'estero in un nodo situato in Italia e di quelle in partenza dall'Italia verso l'estero, delle quali è certo che vengono convogliate a mezzo di gestore sito nel territorio nazionale.*

CASSAZIONE PENALE, SEZIONE SESTA, 5 ottobre 2015 (ud. 22 settembre 2015) – AGRÒ, *Presidente* – DE AMICIS, *Relatore* – PINELLI, *P.M.* (conf.) – Solimando, ricorrente.

Le intercettazioni "*pin to pin*" del sistema *blackberry*, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche

1. È un dato: il continuo sviluppo degli strumenti della comunicazione e la possibilità di apprensione di dati comunicativi non possono che andare di pari passo. Se con facilità sempre crescente si comunica, la violazione di spazi coperti dalla riservatezza utilizzando gli stessi sistemi della comunicazione o adattandone altri è consequenziale. L'esperienza giudiziaria degli ultimi decenni è significativa in proposito e consente di registrare, non soltanto la crescita esponenziale dell'utilizzazione di strumenti sempre più sofisticati per l'acquisizione di rilievi, tracce, notizie, comportamenti umani utili a fini di indagine e di prova, ma, attraverso l'interpretazione, il progressivo adattamento di istituti e precetti normativi a situazione che in comune tra loro hanno soltanto l'invasone degli spazi della vita privata e della comunicazione.

Si è assistito, così, per via di adattamenti interpretativi a volte evidentemente azzardati, all'estensione della disciplina delle intercettazioni ambientali alle videoriprese, nonostante la diversità dei diritti costituzionalmente protetti e la stessa assenza di una disciplina specifica per l'invasione del domicilio ai fini

dell'immissione delle microspie[1]; alla chiusura verso il compiuto riconoscimento di un diritto alla riservatezza diverso e distinto dai diritto all'inviolabilità del domicilio e delle comunicazioni, nonostante la riconosciuta esistenza di spazi di vita privata al di fuori del domicilio nei quali l'individuo normalmente vive ed esplica la sua personalità[2]; alla omologazione tra intercettazioni telefoniche e intercettazioni telematiche, nonostante la diversità dell'oggetto dell' intercettazione (lì, la comunicazione; qui, la corrispondenza)[3]; all'utilizzazione (per fortuna rientrata) della procedura segreta di acquisizione dei dati comunicativi della corrispondenza epistolare al fine di eludere in tal modo la disciplina positiva sul controllo della corrispondenza[4].

Insomma: *tout se tient* in questa materia che, evidentemente, più di altre è esposta alle influenze di un'impostazione culturale dura a morire: quella che privilegia l'utilità del risultato rispetto alle garanzie e, quindi, la salvaguardia del dato informativo acquisito rispetto alla tutela del diritto fondamentale eventualmente conculcato.

In tale inquieto (e inquietante) scenario, quasi a coronamento dell'imperante approssimazione che caratterizza la prova per intercettazioni, si inseriscono a pieno titolo i danni prodotti da quelle conclusioni interpretative che sono il frutto evidente della mancanza di conoscenze tecniche sulla produzione del fenomeno di cui pure si interessano. Qui, in verità, sarebbe qualunquistico attribuire responsabilità soltanto alla prassi giurisprudenziale e al privilegio del fine. Se l'ignoranza è di tutti e se il sistema, in talune fasi del procedere, non consente al giudice di colmare la propria ignoranza attraverso le conoscenze tecniche di un perito (si pensi alla procedura di riesame) il problema della conoscenza diventa problema di informazione del giudice attraverso l'attività dalle parti. Cosicché, per poter dire corretta o meno la scelta interpretativa a monte della decisione, la parte deve avere provveduto a fornire all'interprete tutto ciò che a livello di cognizioni tecniche gli era necessario al fini della

---

[1] Si veda la mai superata Corte cost., n. 135 del 2002, in *Cass. pen.*, 2002, 2285. Di recente, Cass., Sez. II, 13 febbraio 2013, Badagliacca e altri, in *Mass. Uff.*, n. 255541, ha dichiarato manifestamente infondata una questione di illegittimità costituzionale in tema di immissione delle microspie nella privata dimora.

[2] Non si registrano sviluppi degni di nota a seguito e in conseguenza di Cass., Sez. un., 28 marzo 2006, Prisco, in *Dir. pen. proc.*, 2006, 1331.

[3] Qui, è il legislatore, con l'art. 266-*bis* c.p.p. ad avere recepito il peggio della prassi. Si veda, in proposito, Cass., Sez. I, 14 febbraio 2005, Palamara, in *Mass. Uff.*, n. 231591.

[4] Cass., Sez. V, 18 ottobre 2007, N.N., in *Mass. Uff.*, n. 238902 e Id., Sez. I, 7 novembre 2007, Ditto, *ivi*, n. 238488, di diverso avviso rispetto a Id., Sez. VI, 13 ottobre 2009, Giacalone, *ivi*, n. 245183 e Id., Sez. V, 29 aprile 2010, Azoulay, *ivi*, n. 246870, hanno ritenuto applicabile alla corrispondenza la procedura utilizzata per le intercettazioni telefoniche. Il conflitto è stato risulto nel senso della inutilizzabilità da Id., Sez. un., 19 aprile 2012, Pasqua, *ivi*, n. 252893.

comprensione della particolarità di quel fenomeno rispetto ad altri fenomeni solo apparentemente simili o sovrapponibili a quello oggetto della questione.

2. Pare che la soluzione al problema dell'applicabilità o meno della prassi formatasi sulla tecnica dell'istradamento e, quindi, della necessità o meno della rogatoria internazionale nel caso di acquisizione dei messaggi "*pin to pin*" proposta dalla decisione in commento risenta proprio di una carenza di informazione sul funzionamento del sistema di messaggistica istantanea utilizzato dai telefoni *Blackberry* tra loro e con gli altri sistemi compatibili.
Al quesito se sia corretto non ricorrere alla rogatoria internazionale per intercettare le *chat* tra gli apparati or detti la decisione *de qua* ha risposto positivamente ritenendo, infatti, che i messaggi "*pin to pin*" sugli apparecchi *Blackberry* siano direttamente intercettabili mediante la tecnica dell' istradamento, in quanto la società italiana che rappresenta la società canadese *Blackberry*, se opportunamente richiesta consente di far trasmigrare direttamente i messaggi in originale al server della Procura della Repubblica, così determinando che tutta l'attività captativa delle *chat*, anche se proveniente dall'estero e comunque in ogni caso, come si vedrà, gestita, custodita e trattata all'estero, deve debba intendersi effettuata in Italia.
Alcuni passaggi del percorso argomentativo sfociato in tale conclusione rendono evidente il vizio di informazione alla base della conclusione proposta. Essi, infatti, non collimano col funzionamento del sistema di messaggistica istantanea in esame, caratteristica del quale è quella di essere: a) assolutamente autonomo rispetto al nodo del gestore telefonico di riferimento; b) esclusivamente gestito all'estero (in Canada, per l' esattezza) dove le *chat* criptate pervengono e sono trattate e custodite; c) insuscettibile di intercettazione per istradamento data l'assenza di server o nodi nel territorio dello Stato; d) totalmente inintelligibile senza decifratura nella trasmissione dei dati che transitano sui nodi del gestore telefonico.
Al fine di rendere chiaro il vizio, uno sguardo d'insieme è necessario.

3. Dalla letteratura specialistica sull'argomento si apprende che tra la fine degli anni Ottanta e l'inizio degli anni Novanta, a partire dagli Stati Uniti d' America, hanno avuto un notevole successo i c.d. *databanks* o "*personal digital assistants*" (PDAs). Si trattava di dispositivi tascabili capaci di immagazzinare rilevanti quantità di informazioni (rubrica telefonica, promemoria, archivio di documenti) consultabili in qualsiasi momento, ma incapaci di comunicare. Nello stesso periodo, però, hanno avuto molta popolarità anche i c.d. cercapersone ("*pagers*") che consentivano, invece, di ricevere in mobilità brevi

messaggi di testo e di rispondere, sempre in mobilità, a quelli ricevuti, ma che non consentivano di telefonare, né di immagazzinare dati in memoria come i *databanks*. La società canadese Research In Motion (RIM), proprio in quegli anni ha prodotto il cellulare *Blackberry* che ha colmato la lacuna di ciascuno dei due sistemi or detti, applicando la memoria dei *databanks* alla capacità di comunicare in maniera bidirezionale dei cercapersone e incorporando nel sistema un telefono.

Il successo del dispositivo *Blackberry* è costituito proprio da tale adattamento e dalla messa a punto della tecnologia c.d. "*Push*" che consiste, in sostanza, nella sincronizzazione continua della comunicazione e dell'aggiornamento dei dati attraversi apparecchi cellulari lontani mediante l'utilizzazione del server canadese che, dopo avere rilevato che un nuovo messaggio, una e-mail, un documento o quant'altro è pervenuto, comprime i dati in un pacchetto e reindirizza le informazioni al cellulare *Blackberry* o a quelli che utilizzano lo stesso sistema cui è diretto. Il processo di compressione e di trasmissione avviene necessariamente attraverso la formattazione e la cifratura dei dati e il confezionamento degli stessi in una sorta di "busta elettronica" che consente al destinatario di leggere solo il mittente o di scaricare, laddove lo voglia, pure il contenuto. I dati, così imbustati, viaggiano su nodi gestiti esclusivamente dalla RIM.

Per ciò che riguarda lo scambio di messaggi, i cellulari *Blackberry* possono operare in due modi: utilizzando il numero identificativo assegnato a ciascun apparecchio (il "PIN") oppure tramite l'applicazione *Blackberry* Messenger (BBM), che consente di scambiare messaggi anche con telefoni che utilizzano sistemi diversi le cui società abbiano acquisito il prodotto o con le quali la RIM abbia accordi. Nell'un modo e nell'altro, i messaggi in partenza o in arrivo utilizzano il PIN, sono cifrati alla partenza e, così come per le e-mail, viaggiano sui nodi RIM e sono impermeabili al gestore dell'utenza telefonica abbinata al cellulare.

Diversamente da ciò che avviene per le comunicazioni vocali, dunque, le comunicazioni dei messaggi "*pin to pin*", pur essendo intercettabili attraverso la IMEI del cellulare sui nodi dell'operatore mobile del telefono cellulare intercettato, non sono intelligibili, in quanto la cifratura degli impulsi della comunicazione dalla partenza all'arrivo (la c.d. criptazione "*end-to-end*": "da un capo all'altro") impedisce a chiunque non abbia la chiave di lettura di avere cognizione del messaggio lungo tutto il canale di trasmissione. In caso di intercettazione, quindi, è possibile ottenere la comunicazione "in chiaro" esclusivamente soltanto laddove si utilizzi la chiave di decifratura e ciò può avvenire in un unico modo, sottoponendo ad intercettazione i nodi di servizio RIM

che, allo stato delle cose, sono ubicati in Canada e, in Europa, soltanto nel Regno Unito.

4. Ora, allorquando si afferma che per ottenere la comunicazione "in chiaro" è sufficiente richiedere l'intervento della RIM Italia – che è una società che non ha potere gestorio del traffico telefonico ed ha come unico scopo quello della distribuzione dei telefoni cellulari *Blackberry* in Italia – si dice cosa assolutamente inesatta per ciò che concerne l'intercettazione dei flussi informativi. La società RIM Italia, infatti, nel territorio dello Stato non ha server per il passaggio dei flussi di comunicazioni telematiche "*pin to pin*", né – e il punto non è di poco momento – ha alcun centro di raccolta dati destinato comunque a captare o a conservare i dati delle comunicazioni che, come s'è detto, transitano esclusivamente attraverso server canadesi e in Europa su un nodo situato nel Regno Unito.
Tanto vero ciò, che, laddove sia destinataria di un decreto *ex* art. 266-*bis* c.p.p. (come si presume sia accaduto nel caso oggetto della decisione in commento), la società italiana meramente collabora all'estrazione dei dati, facendo confluire sul server della Procura della Repubblica indagante i messaggi decifrati che comunque provengono dal server ubicato in Canada dopo averli opportunamente resi in chiaro con le proprie chiavi di decriptazione. Avviene, in sostanza, che, nonostante l'assenza di server o di nodi sul territorio dello Stato, la società italiana proceda ad un convogliamento delle comunicazioni attingendo dal server canadese, secondo un agire che appare *ictu oculi* incompatibile, non soltanto rispetto all'apprensione della prova che è formata, raccolta e custodita (oltre che resa intelligibile) all'estero, ma – è la cosa non è di poco momento – con le norme a garanzia della genuinità della stessa prova.
In relazione al primo aspetto, va sottolineato che l'inesistenza di un server o di un nodo RIM sul territorio dello Stato comporta *de facto* l'impossibilità di far ricorso alla prassi sull'istradamento, per l'insussistenza appunto della fonte situata nel territorio nazionale cui attingere, non potendo, nel caso, essere quella del gestore telefonico di riferimento che, come s'è visto, nel sistema "*pin to pin*" smista esclusivamente flussi di comunicazioni cifrate. Né, per superare ciò, può dirsi che comunque il flusso di comunicazioni giunge nel territorio dello Stato sul cellulare che utilizza il sistema che riceve le *chat*. La localizzazione nello Stato del terminale della comunicazione, infatti, per tutto ciò che proviene dall'estero è assolutamente irrilevante, tanto vero ciò che proprio per tale ragione è utilizzata la tecnica dell'istradamento.
In relazione al secondo aspetto – quello concernente la genuinità della prova

– è evidente che l'intervento di un soggetto (la società **RIM** Italia) che non ha poteri di conservazione e di controllo dei dati e di controllo (la c.d. "*chain of custody*": "catena di controllo") non può provvedere alla certificazione (per così dire) della genuinità del dato; cosa che, nel caso, può essere concessa esclusivamente dalla società canadese che, ove richiesta, potrebbe negare l' accesso ai dati in ossequio alla locale legislazione.

L'assenza di server e di nodi nel territorio dello Stato determina, insomma, che ai fini dell'intercettazione delle chat "pin to pin" sia necessaria la cooperazione internazionale, risultando ogni altro strumento un vero e proprio escamotage per intercettare ciò che non può essere legittimamente intercettato.

SANDRO FÙRFARO