CAPTATORE INFORMATICO: È UTILIZZABILE LA REGISTRAZIONE AVVENUTA ALL'ESTERO

Corte di Cassazione, Sezione II Penale, sentenza n. 29362 del 22 luglio 2020 e pubblicato il 22 ottobre 2020

La difesa eccepisce che le conversazioni ambientali acquisite sarebbero inutilizzabili in quanto la relativa captazione è stata resa possibile tramite rete wi-fi estera (sita in Canada), rilevando che atteso che le conversazioni in questione (estero su estero) non transitavano attraverso nodi telefonici italiani ma si svolgevano esclusivamente tramite ponte telefonico canadese, la mancanza di rogatoria aveva determinato l'inutilizzabilità dei risultati dell'attività d'indagine per violazione dell'art. 729 cod. proc. pen. I giudici della Corte hanno invece rilevato che la registrazione della conversazioni tramite wi-fi sito in Canada abbia costituito una fase intermedia di una più ampia attività di captazione iniziata nella sua fase iniziale e conclusiva sul territorio italiano.

di Elena BASSOLI, avvocato di diritto e nuove tecnologie; è docente di "Diritto della comunicazione elettronica" presso l'Università di Genova, nonché del Master Universitario di II Livello in Cyber Security and Data Protection, presso il DIBRIS Unige, autore di oltre 250 pubblicazioni in materia dal 1995 ad oggi; è Formatore per il Ministero di Giustizia e già per il Ministero dell'Interno. È inoltre Presidente nazionale ANGIF (Associazione nazionale giuristi informatici e forensi) e CSIG-Genova (Centro studi informatica giuridica).

1. Premessa

L'annotata sentenza prende le mosse da un procedimento riguardante il riesame di una misura di custodia in carcere per l'accusa di associazione per delinquere di stampo camorristico, con l'aggravante della transnazionalità, confermata dal Tribunale del Riesame locale.
In ordine alla ammissibilità in giudizio di prove acquisite tramite captatori informatici la Cassazione italiana ricorda che: «i sistemi di captazione *de quibus* non sono costituiti solamente dal trojan, cioè dal semplice *software* (*rectius*, *malware*), che viene inoculato, ma anche dalle piattaforme necessarie per il loro funzionamento, che ne consentono il controllo e la gestione da remoto e che ricevono i dati inviati dal captatore in relazione alle funzioni investigative attivate.
I dati raccolti sono, infatti, trasmessi, per mezzo della rete internet, in tempo reale o ad intervalli prestabiliti ad altro sistema informatico in uso agli investigatori».
E ancora: «i dati provenienti dal captatore informatico devono essere cifrati e devono transitare su un canale protetto sino al server della Procura che è il primo ed unico luogo di memorizzazione del dato.
Ogni file è dunque cifrato e reca una password diversa rispetto a quella utilizzata per la memorizzazione sul server; ne consegue che ogni file per essere ascoltato deve essere decripato».

2. L'extraterritorialità delle conversazioni. La rogatoria internazionale è superflua

Sulla base di quanto sopra esposto deve, quindi, ritenersi che, nella specie, la registrazione della conversazioni tramite wifi sito in Canada abbia costituito una fase intermedia di una più ampia attività di captazione iniziata ed avente ad oggetto la registrazione, nella sua fase finale e conclusiva, sul territorio italiano. Infatti, al di là dei dettagli tecnici, ciò che rileva è che, in ultima analisi, l'ascolto delle conversazioni avvenga in Italia su apparecchi collegati ad un gestore italiano e la cui captazione abbia avuto origine sul territorio italiano.
L'atto investigativo risulta, dunque, compiuto sul territorio italiano.
In base a tale assunto la S.C. ha affermato che la procedura di cui agli artt. 727 e ss. cod. proc. pen. riguarda esclusivamente gli interventi da compiersi all'estero che, per tale motivo, richiedono l'esercizio della sovranità propria dello Stato estero.

Di conseguenza non risulta ipotizzabile alcuna necessità di rogatoria internazionale per un'attività di fatto svolta, autorizzata e realizzata in Italia, secondo le regole del codice di rito, e ciò perché quando il captatore informatico sia installato in Italia, e la captazione avvenga, di fatto, attraverso le centrali di ricezione ivi collocate, la sola circostanza che le conversazioni siano state eseguite, in parte, all'estero e ivi "temporaneamente" registrate tramite wi-fi locale a causa dello spostamento del cellulare sul quale è stato inoculato il trojan, ciò non può implicare l'inutilizzabilità della intercettazione per difetto di rogatoria.

Appare mutuabile alla fattispecie in esame il principio di diritto secondo cui l'intercettazione di comunicazioni tra presenti eseguita a bordo di una autovettura attraverso una microspia installata nel territorio nazionale, dove si svolge altresì l'attività di captazione, non richiede l'attivazione di una rogatoria per il solo fatto che il suddetto veicolo si sposti anche in territorio straniero ed ivi si svolgano alcune delle conversazioni intercettate (Cass. pen., sez. 2, n. 51034 del 04.11.2016).
Poiché, come detto, il captatore è stato installato in Italia e la captazione, nei suoi sviluppi finali e conclusivi è avvenuta in Italia, attraverso le centrali di ricezione facenti capo alla Procura locale, la sola circostanza che le conversazioni captate siano state in parte eseguite all'estero per lo spostamento dell'apparecchio e del suo utilizzatore risulta del tutto ininfluente per ritenere la necessità della rogatoria, non potendosi, nel caso di intercettazione ambientale su strumento mobile, conoscere tutti gli spostamenti, così vanificandosi le finalità del mezzo di ricerca della prova.

Occorre al proposito rammentare che lo strumento dell'intercettazione ambientale mediante "captatore informatico" è per sua stessa natura itinerante, in quanto l'attività di captazione segue tutti gli spostamenti nello spazio dell'utilizzatore.
A voler diversamente ragionare, i possibili reiterati spostamenti su territori esteri, resi possibili dalla facilità di frequenti collegamenti aerei con tutte le parti del pianeta, successivamente al momento dell'inizio delle operazioni, che, nella specie, è da individuarsi con certezza in Italia, comporterebbero una impossibilità tecnica di procedere alle intercettazioni, ben potendo l'Autorità Giudiziaria che le ha disposte ignorare il luogo dove si trova il soggetto

titolare dell'utenza su cui è stato inoculato il captatore, ed, essere, quindi impossibilitata a chiedere la rogatoria, neppure con l'urgenza e con i modi previsti dall'art. 727 comma 5 cod. proc. pen., venendo così frustrate le finalità di tale strumento investigativo.

Gli Ermellini condividono pertanto la motivazione della sentenza impugnata nella parte in cui ha ritenuto utilizzabili dette conversazioni, in quanto "iniziate" e "svolte" in Italia, risultando, quindi, rispettati i parametri di cui agli artt. 15 e 24 Cost. ed apparendo, anche, osservato il dettato di cui all'art. 8 della Convenzione Europea dei diritti dell'Uomo, così come interpretato nella giurisprudenza della Corte di Strasburgo, dovendosi escludere preclusioni riguardanti le intercettazioni effettuate mediante "captatore informatico" transitato all'estero.
In tal senso vanno richiamate le pronunzie della Corte Europea dei Diritti dell'Uomo Iordachi c. Moldavia, 10 febbraio 2009, Natoli c. Italia, 9 gennaio 2001; Mcleod c. Regno Unito, 23 settembre 1998, ove è stato affermato che le intercettazioni sono legittime se giustificate in base ai parametri indicati nell' articolo 8 § 2 CEDU, cioè la legalità, la legittimità dell'obiettivo perseguito, la necessità e la proporzionalità.
A tali pronunce si aggiunge, da ultimo, la sentenza Corte EDU, 23.2.2016, Capriotti c. Italia, che ha affermato la compatibilità delle intercettazioni disposte nei procedimenti per delitti di criminalità organizzata con il diritto al rispetto della vita privata e il diritto al "processo equo", sanciti rispettivamente dall'art. 8 e dall'art. 6 CEDU.

3. L'ammissibilità della prova

Il Tribunale del riesame ha, con motivazione ritenuta dalla S.C. congrua in fatto e corretta in diritto, precisato che poiché l'attività di intercettazione era stata posta in essere in relazione a un omicidio aggravato ex art. 7. L. 203/1991, inserito in un chiaro contesto di mafia, appariva corretta l'applicazione del regime normativo stabilito per le intercettazioni fra presenti, trattandosi di reati di **criminalità organizzata**.
Disattesa è stata quindi l'istanza della difesa secondo la quale la registrazione delle conversazioni non sarebbe avvenuta "direttamente nei locali della Procura" e che essa non avrebbe effettuato il necessario controllo "sulla catena di custodia della prova informatica", poiché per l'esecuzione di tale attività erano stati utilizzati "gli apparecchi siti presso la **Procura della Repubblica di Reggio Calabria** ed era stato facoltizzato l'ascolto da remoto presso gli uffici della P.G.".

Quanto all'ausilio di soggetti privati, in qualità di appaltatori della strumentazione necessaria ai fini delle operazioni, la pronuncia in esame ha rimarcato che in materia di intercettazioni, l'art. 268, comma terzo cod. proc. pen., richiede che le operazioni si svolgano sotto il diretto controllo degli inquirenti, ma **non vieta l'utilizzazione di impianti e mezzi appartenenti a privati**, né il ricorso all'eventuale ausilio tecnico ad opera di soggetti esterni che siano richiesti di intervenire per fronteggiare esigenze legate al corretto funzionamento delle apparecchiature noleggiate e che si trovino ad agire, in tale evenienza, come "*longa manus*" o ausiliari del Pubblico ministero o della polizia giudiziaria (cfr. Cass. pen., sez. 1, n. 3137 del 19.12.2014). Di conseguenza sembra che nessuna censura possa essere mossa in ordine al requisito della "genuinità della prova", ancorché ciò possa effettivamente di fatto privare il soggetto interessato delle proprie garanzie difensive, in violazione della L. 48/2008, in esecuzione della Convenzione di Budapest sul Cybercrime.

4. La valutazione delle fonti di prova

La sentenza della Cassazione afferma che la scelta e la valutazione delle fonti di prova rientrano tra i compiti istituzionali del giudice di merito e sfuggono al controllo del giudice di legittimità se adeguatamente motivate e immuni da errori logico-giuridici. In tema di intercettazioni di conversazioni o comunicazioni, l'interpretazione del linguaggio adoperato dai soggetti intercettati, anche quando sia criptico o cifrato, costituisce questione di fatto, rimessa alla valutazione del giudice di merito, la quale, se risulta logica in relazione alle massime di esperienza utilizzate, si sottrae al sindacato di legittimità. (Cass. SS.UU., n. 22471 del 26.02.2015).
Il fatto quindi che l'identificazione dei soggetti intercettati sia avvenuta sulla base di pseudonimi o soprannomi utilizzati nelle conversazioni, che non avrebbero potuto identificare univocamente i soggetti coinvolti, lungi dall'essere frutto di un "ragionamento apodittico e congetturale" operato dal giudice di merito,

è stato invece il risultato di una lettura logico-sistematica delle intercettazioni dalla quale è emerso in maniera univoca che il soggetto indicato nelle captazioni fosse certamente l'indagato.
Il tribunale ha correttamente evidenziato il contenuto inequivoco delle conversazioni intercettate da cui emergeva il fattivo coinvolgimento dell'indagato all'interno della consorteria mafiosa di cui al capo provvisorio di incolpazione, che in tale veste è risultato soggetto chiamato a fare da messaggero di ambasciate fra le **consorterie di 'ndrangheta operanti in Italia ed in Canada**, come emerso non solo da numerose intercettazioni, ma anche sulla scorta di accertamenti di Polizia Giudiziaria.

5. Le tecniche investigative invasive

La sentenza in esame offre lo spunto per approfondire il tema delle tecniche investigative invasive, da ultimo affrontato dal d. lgs. 216 del 29 dicembre 2017, rubricato "Disposizioni in materia di intercettazione di conversazioni o comunicazioni, in attuazione della delega di cui all'art. 1, commi 82, 83 e 84, lettere a), b), c), d), ed e), della legge 23 giugno 2017, n. 103", avente il fine di disciplinare l'utilizzo, nell'ambito delle indagini penali, di nuovi strumenti tecnologici in grado di stare al passo con l'evoluzione delle nuove forme di comunicazione e, conseguenzialmente, di sfruttare al meglio le possibilità investigative offerte dalla rete, salvaguardando al contempo interessi costituzionalmente garantiti e meritevoli di tutela.
Sul punto, ancor prima del legislatore, erano intervenute le Sezioni Unite con la sentenza n. 26889/2016 le quali avevano affermato che "è legittimo nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei virus informatici, suscettibili di ledere riservatezza, dignità e libertà delle persone", anche se "è del pari legittimo ricordare che solo siffatti strumenti sono oggi in grado di penetrare canali criminali di comunicazione o di scambio di informazioni utilizzati per la commissione di gravissimi reati contro le persone".

Fine primario della disciplina normativa è regolamentare l'utilizzo dei captatori informatici, adeguando il modello alle esigenze processuali, dotare le indagini di strumenti al passo con i tempi e dotare gli stessi di un opportuno riconoscimento in ambito legislativo.
Ciò al fine di consentirne un uso giuridicamente corretto, nonché di tutelare i diritti fondamentali del singolo, secondo un adeguato bilanciamento degli interessi in gioco, nell'intento di rendere maggiormente equilibrata la salvaguardia fra interessi parimenti meritevoli di tutela a livello costituzionale.
Ed in effetti l'uso di questi sistemi, nell'ambito delle indagini penali, pone delicatissimi problemi proprio per il valore degli interessi coinvolti: da un lato la tutela dei diritti fondamentali dell'individuo, dall'altro le esigenze di verità e giustizia.
Nel dettaglio si parla di libertà e segretezza della corrispondenza e delle forme di comunicazione, nonché di inviolabilità del domicilio, diritti che sono destinati a subire delle limitazioni nella misura in cui lo Stato, tra i suoi doveri primari, pone l'accertamento delle responsabilità penali, il perseguimento e la repressione dei reati.

La normativa del 2017 tenta di ridefinire i limiti fino a cui spingersi a fronte dell'utilizzo di tecniche investigative che, da un lato, rischiano di essere maggiormente invasive, ma che, dall'altro, costituiscono un necessario adeguamento del sistema processuale alle nuove tecniche comunicative, che implicano necessariamente l'ammodernamento delle modalità di indagine, nel caso in cui si agisca per l'accertamento di determinati reati, considerati dall'ordinamento giuridico particolarmente gravi. Senza tale aggiornamento, il sistema non sarebbe più in grado di ottenere validi risultati dalle indagini tradizionali, stante la sempre più frequente criptazione delle comunicazioni. ©