il Quotidiano Giuridico

Penale

INTERCETTAZIONI

La disciplina del captatore informatico. Nota breve al d.m. 20 aprile 2018

mercoledì 25 luglio 2018
di **Suraci Leonardo** Dottore di ricerca in diritto processuale penale presso l'Università La Sapienza di Roma

È stato pubblicato sul Bollettino Ufficiale del Ministero di Giustizia il d.m. 20 aprile 2018, recante "disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216".

Decreto Ministero della Giustizia, 20 aprile 2018 – Bollettino ufficiale del Ministero della Giustizia, 31 maggio 2018, n. 10

Una brevissima, ma necessaria, premessa introduttiva
Come è oltremodo noto, l'intercettazione di conversazioni mediate captatore informatico viene effettuata tramite il ricorso ad un *malware* il quale viene occultamente installato dall'inquirente in un dispositivo elettronico dotato di connessione *internet* attiva tramite l'invio con una *mail*, un *sms* o un'applicazione di aggiornamento.

Utilizzando il programma informatico appena descritto è possibile, tra le altre cose, attivare da remoto il microfono dell'apparecchio di destinazione e, quindi, apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo.

La **legge di delega** (l. 23 giugno 2017, n. 103) prospettava – rispetto ad un tema che, come già detto su questo quotidiano, coinvolge un mezzo di ricerca particolarmente insidioso – un intervento calibrato su tutti i punti, omogeneizzando i limiti di ammissibilità rispetto ai delitti diversi da quelli di criminalità organizzata: quelli, cioè, di cui si era occupata la nota **Cass. pen., Sez. unite, sentenza 1° luglio 2016, n. 26889**, la quale aveva affrontato proprio la questione relativa al perimetro di ammissibilità di un siffatto mezzo captativo.

Le Sezioni unite, nell'occasione, hanno approfondito gli spunti tratti dall'ordinanza di rimessione e, dopo avere innanzitutto ribadito la correttezza della qualificazione giuridica dell'attività investigativa svolta tramite agente intrusore come intercettazione di tipo "ambientale", hanno affermato i seguenti principi di diritto:

a. deve escludersi la possibilità di compiere intercettazioni nei luoghi indicati dall'art. 614 c.p., con il mezzo indicato, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'art. 13, d.l. 13 maggio 1991, n. 152, convertito in l. 12 luglio 1991, n. 203, non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'art. 266, co. 2 c.p.p., che in detto luogo "si stia svolgendo l'attività criminosa";**b.** è invece consentita la captazione nei luoghi di privata dimora *ex* art. 614 c.p., pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'art. 13 d.l. 13 maggio 1991, n. 152.
La Corte di cassazione ha, poi, colto l'occasione per ribadire l'adesione ad una interpretazione ampia della nozione di "criminalità organizzata", di talché ha chiarito che per procedimenti relativi a delitti riconducibili a siffatta nozione devono intendersi non soltanto quelli elencati

nell'art. 51, co. 3-*bis* e 3-*quater* c.p.p., ma anche quelli comunque facenti capo ad un'associazione per delinquere *ex* art. 416 c.p.p., con esclusione del mero concorso di persone nel reato.

Sul versante procedurale, invece, la legge di delega imponeva un peculiare dovere motivazionale del giudice in punto di necessità della metodologia captativa in discorso rispetto a specifiche esigenze investigative, modalità comunque da attuare mediante l'utilizzazione di programmi conformi ai requisiti predeterminati da un apposito decreto ministeriale.

L'esigenza di un controllo continuativo della dinamica esecutiva si poneva, invece, alla base sia della previsione secondo cui l'attivazione del microfono dell'apparecchio di destinazione dovesse avvenire previo invio di un apposito comando e non in conseguenza dell'installazione del captatore, sia della previsione di specifici obblighi documentativi correlati alla durata delle singole registrazioni.

Al fine di garantire integrità e originalità delle registrazioni, poi, era stata inserita la previsione secondo cui il trasferimento delle registrazioni dovesse essere effettuato esclusivamente verso il *server* della procura della Repubblica, senza, dunque, l'intermediazione di centri collocati presso gli uffici di polizia giudiziaria.

Il **d.lgs. 29 dicembre 2017, n. 216** ha, in primo luogo, modificato l'art. 266 c.p.p. il quale ribadisce la collocazione delle intercettazioni mediante captatore informatico nell'ambito delle intercettazioni tra persone presenti.

Inoltre, come prospettato dal legislatore delegante, la captazione "domiciliare" mediante agente intrusore, in generale consentita rispetto a qualsiasi tipologia di reato prevista dall'art. 266, co. 1 c.p.p., viene circoscritta rispetto ai delitti diversi da quelli indicati all'art. 51, co. 3-*bis* e 3-*quater* ai casi in cui vi siano elementi idonei a fare ritenere che nell'ambiente domiciliare sia in corso di svolgimento attività criminosa.

L'intervento sul versante motivazionale viene attuato mediante una duplice previsione che, nel complesso, delinea un obbligo di motivazione rafforzata diversamente calibrato a seconda dell'oggetto del procedimento ma che, per struttura e scopo, consente di intravedere l'intenzione del legislatore di individuare nel ricorso alla metodica investigativa che ci occupa una sorta di *extrema ratio*.

Invero, sul piano generale il giudice per le indagini preliminari deve esporre nel decreto autorizzativo, accanto alle ragioni di indispensabilità del mezzo di ricerca della prova ai fini della prosecuzione delle indagini, i motivi per i quali appare necessario il ricorso al captatore informatico.

In relazione, invece, ai delitti diversi da quelli di criminalità organizzata – quelli, per intendersi, indicati nell'art. 51, co. 3-*bis* e 3-*quater* c.p.p. – è richiesta l'indicazione dei luoghi e dei tempi in relazione ai quali è consentita l'attivazione del microfono: indicazione di difficile attuazione ma necessaria perché coinvolgente un mezzo di captazione installato su un dispositivo itinerante, rispetto alla quale è utilizzabile anche una forma di determinazione che il nuovo art. 267, co. 1 c.p.p. definisce "indiretta" e che, nelle possibili quanto prevedibili disquisizioni circa la ricorrenza di un requisito prescritto a pena di inutilizzabilità *ex* art. 271 c.p.p., rischia di schiudere le porte verso modalità descrittive poco o per nulla dotate di efficacia delimitativa.

Anche perché, specifica l'art. 271, co. 1-*bis* c.p.p., i dati acquisiti al di fuori dei limiti spaziali e temporali stabiliti nel decreto sono inutilizzabili.

I delitti di cui all'art. 51, co. 3-*bis* e 3-*quater* c.p.p. sono gli unici a poter fruire del mezzo di captazione in discorso secondo la procedura speciale prevista dall'art. 267, co. 2 c.p.p., previa specifica indicazione delle ragioni di urgenza: prescrizione, quest'ultima, che sembra costituire una inutile ripetizione di quanto già previsto dalla norma generale – le ragioni d'urgenza non potendo consistere in altro se non nella prospettazione del pericolo che il ritardo produca un grave pregiudizio alle indagini.

In linea – ma soltanto apparentemente – con le previsioni della legge di delega ed in termini derogatori rispetto ad un consolidato orientamento giurisprudenziale secondo cui i risultati delle intercettazioni telefoniche disposte per un reato rientrante tra quelli indicati nell'art. 266 c.p.p. sono utilizzabili anche relativamente ai restanti reati per i quali si procede nel medesimo procedimento, pur se per essi le intercettazioni non siano consentite, (Cass. pen., Sez. V, 29 aprile 2014, n. 17939. L'impostazione è stata autorevolmente ribadita pochi mesi più tardi, da Cass. pen., Sez. VI, 9 agosto 2016, n. 34765), il legislatore ha previsto che, in generale, le risultanze dell'intercettazione eseguita mediante captatore informatico possano essere utilizzate

esclusivamente al fine di provare i reati oggetto del provvedimento autorizzativo.

La successiva disposizione derogatoria, però, autorizza l'utilizzo delle risultanze medesime anche per delitti diversi, allorché si tratti di delitti per i quali è obbligatorio l'arresto in flagranza e rispetto all'accertamento dei quali le stesse risultino indispensabili.

Lo scostamento dalla previsione di cui all'art. 1, co. 84 lett. e) n. 7 della legge di delega è, tuttavia, immediatamente percepibile: mentre, da un lato, essa riferiva l'ipotesi derogatoria all'utilizzazione delle risultanze in procedimenti diversi – la norma attuativa, al contrario, non opera alcuna distinzione sul punto – dall'altro, la stessa limitava il perimetro di impiego degli esiti investigativi all'accertamento di delitti di cui all'art. 380 c.p.p., norma che individua ma non esaurisce i casi in cui è obbligatorio l'arresto in flagranza di reato.

Il decreto delegato si è fatto carico dell'esigenza di assicurare il costante controllo della procedura captativa, innanzitutto (purtroppo, viene da dire, semplicemente) lasciando intravedere alla luce del riferimento contenuto nel nuovo art. 267, co. 1 c.p.p. la necessità di sganciare la procedura di installazione del captatore dall'effettiva ed autonoma attivazione del microfono dell'apparecchio di destinazione.

Norma insoddisfacente soprattutto perché, precisa l'art. 271, co. 1-*bis* c.p.p., non sono utilizzabili i dati acquisiti non già in casi precedenti l'attivazione, bensì nel corso delle operazioni preliminari all'inserimento del captatore informatico, e dunque in frangenti che precedono – non già seguono – l'installazione (ma non l'attivazione).

L'esigenza posta dal legislatore delegante di rispettare *standards* tecnici predefiniti sul versante della garanzia di affidabilità, sicurezza ed efficacia è stata delineata dall'art. 89, co. 2-*bis* disp. att. c.p.p., il quale ha modo di ribadire che ai fini dell'installazione e dell'intercettazione mediante il ricorso al captatore informatico possono essere impiegati soltanto programmi – la cui tipologia, puntualizza il comma precedente, deve essere indicata nel verbale di cui all'art. 268, co. 1 c.p.p. – conformi ai requisiti tecnici stabiliti con decreto del Ministro di giustizia da emanare, precisa l'art. 7 del decreto legislativo, entro trenta giorni dalla data di entrata in vigore di questo.

Il decreto ministeriale 20 aprile 2018
Il d.m. 20 aprile 2018 si occupa delle **caratteristiche dei programmi informatici funzionali all'esecuzione delle intercettazioni mediate captatore informatico su dispositivo portatile** all'art. 4, disposizione tanto laconica quanto poco descrittiva e, quindi, scarsamente persuasiva anche rispetto all'opportunità che la predisposizione di essa fosse preceduta da un maggiormente approfondito confronto tra versante squisitamente giuridico e profilo di rilievo tecnico-scientifico.

Confronto che, evidentemente, è mancato sebbene l'inserimento di una clausola di salvaguardia del tipo di quella contenuta nel co. 5 della disposizione avrebbe certamente evitato che ad una maggiore normativizzazione dei profili tecnici fosse associabile il rischio di una eccessiva cristallizzazione delle soluzioni tecnologiche.

La norma, infatti, prescrive un obbligo di periodico adeguamento dei programmi a standard di funzionalità ed operatività "in linea con l'evoluzione tecnologica" e se, da un lato, sembra ribadire (ed in effetti fa questo) un'ovvia esigenza di costante aggiornamento tecnico dei sistemi di captazione, dall'altro sembra dare impulso (ed in effetti fa anche questo) ad una scelta all'insegna della deregolamentazione: dunque, una soluzione nel complesso ispirata alla logica del dire e non dire, trattandosi (si pensa) di questioni tanto tecniche e poco giuridiche.

Poche regole (se così le si vuol chiamare, trattandosi per lo più di principi generalissimi), dunque, per cui pochi spazi per verifiche di carattere giuridico e, infine, scarsissimi ambiti di effettività sul versante delle sanzioni processuali.

Ed allora, si dice che gli esperti di informatica devono elaborare i programmi funzionali all'esecuzione delle intercettazioni mediante ricorso al *trojan horse* in modo da assicurare "integrità, sicurezza e autenticità" dei dati captati su ogni canale di trasmissione riferibile al captatore.

Se l'espressione "funzionali all'esecuzione" sembra idonea a coprire sia la fase dell'installazione dell'agente intrusore che quella dell'intercettazione vera e propria – in linea, quindi, con la prescrizione di cui all'art. 89, co. 2-*bis* disp. att. c.p.p. – i requisiti caratteristici dei dati captati impongono la predisposizione di sistemi idonei a garantire la completezza, la non dispersione e la riservatezza di essi, oltre che la perfetta corrispondenza con quanto costituisce oggetto di percezione.

In ordine al requisito della completezza dell'informazione acquisita, il co. 4 della norma che si esamina consente di intravedere la scelta normativa di recepire una nozione ampia di informazione, certamente più estesa di quella di "dato captato" che figura al co. 2 siccome inclusiva, altresì, di riferimenti al c.d. contesto dell'acquisizione.

Nell'ambito della relazione che si instaura tra un (definiamolo così) contesto delle operazioni – descritto dal verbale di cui all'art. 268 c.p.p. e collocato presso la sede dell'apparecchio remoto – e quello dell'acquisizione non v'è dubbio che quest'ultimo afferisca al sistema di informazioni rilevanti che, spingendosi oltre il dato costituito dalla conversazione, si colloca nell'ambiente in cui quest'ultima si costruisce e, così come matura e viene in esistenza, costituisce oggetto di captazione.

La norma, dunque, impone il ricorso a sistemi capaci di assicurare una potenzialità acquisitiva piena, estesa ad ogni informazione idonea ad assicurare il rispetto delle prescrizioni legislative poste a tutela dei diritti fondamentali della persona – si pensi, ad esempio, ai dati spazio-temporali richiamati dall'art. 267, co. 1 c.p.p. – oltreché a garantire la genuinità del dato propriamente comunicativo.

La sicurezza, oltre che sul terreno della non dispersione, deve essere garantita anche sul versante della riservatezza e dell'integrità dei dati captati, per cui il sistema informatico deve essere predisposto in modo da prevenire indebite intrusioni durante ogni fase dell'attività acquisitiva e, dunque, deve garantire innanzitutto che gli strumenti di comando e di funzionamento del captatore siano accessibili esclusivamente da parte degli operatori autorizzati.

Ciò impone, ovviamente, che le strutture le quali ospitano gli apparati di captazione siano fisicamente inaccessibili da parte di figure diverse o, comunque, che sia impraticabile l'apparato captativo che contiene le apparecchiature gestionali del sistema intrusivo.

I sistemi di sicurezza devono prevedere, poi, accorgimenti – questi, evidentemente, di natura informatica – idonei a prevenire forme di intrusione provenienti da fonti esterne rispetto ai protagonisti della relazione captativa – forme che possono esplicarsi sia mediante condotte umane direttamente incidenti sul sistema intercettativo, sia attraverso il ricorso a specifici software di bonifica – ed afferenti all'identificazione sia del captatore che dei dati captati.

La norma impone, dunque, che la relazione intercettativa sia unica e inaccessibile sia dall'interno che dall'esterno, di modo che non vengano turbati i requisiti caratteristici costituiti dalla genuinità, efficacia, integrità, completezza e riservatezza dei dati.

Per realizzare i risultati investigativi prefissati e, quindi, conseguire l'efficienza nelle attività d'indagine, i programmi informatici devono configurare accorgimenti idonei ad assicurare la permanenza e la funzionalità del captatore nell'ambito del dispositivo infiltrato per tutta la durata delle operazioni, secondo quanto stabilito nel provvedimento autorizzativo e fino alla definitiva disattivazione di esso, ai sensi dell'art. 89, co. 2-*quinquies* disp. att. c.p.p.

Invero, la rimozione accidentale del programma oppure la sua erronea ed anticipata disattivazione o, ancora, un qualsiasi difetto di funzionamento rischierebbero di compromettere il conseguimento di significativi risultati investigativi, in ipotesi rispetto a gravissime fattispecie delittuose.

Nel complesso, può dirsi che il **principio cardine** che deve ispirare l'attività di predisposizione dei programmi finalizzati alla captazione mediante il ricorso al *trojan* è quello della **sicurezza**, non senza notare che il decreto delegato, così come il decreto ministeriale, non prevedono una fase di controllo ed approvazione dei dispositivi da parte degli organi competenti del Ministero di giustizia.