Corte di Cassazione, Sezioni Unite Penali, sentenza n. 26889 del 28 aprile 2016 e depositata il 1° luglio 2016

Con la sentenza n. 27100 del 26 maggio 2015 era stata rimessa alle Sezioni Unite la questione di diritto in tema di intercettazioni tramite virus informatico ovvero se anche nei luoghi di privata dimora sia consentita l'intercettazione mediante tale strumento. All'udienza del 28 aprile 2016, la Cassazione ha confermato la sua utilizzazione limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica (a norma dell'art. 13 d.l. n. 152 del 1991), intendendosi per tali quelli elencati nell'art. 51, commi 3-bis e 3-quater, cod. proc. pen., nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.

di Milto Stefano De Nozza

INTERCETTAZIONE MEDIANTE *TROJAN*: LA DECISIONE DELLE SEZIONI UNITE

Milto Stefano DE NOZZA, Magistrato in servizio presso la Procura della Repubblica di Brindisi, applicato alla D.D.A. di Lecce, Magistrato responsabile della sala intercettazioni della Procura di Brindisi, Componente della commissione per il noleggio dei servizi di supporto alle attività di intercettazione, Magistrato di riferimento per l'informatica della Procura di Brindisi su incarico del Consiglio Superiore della Magistratura, Magistrato referente per i rapporti con la associazione antiracket Salento.

La Corte di Cassazione a Sezioni Unite[1], chiamata a pronunciarsi sulla legittimità dell'uso delle intercettazioni mediante virus autoinstallante, a seguito di ordinanza di remissione[2] che aveva rilevato un contrasto di giurisprudenza[3], con la decisione in commento ha dettato una prima, ma certamente non ultima, linea di orientamento sul tema. La questione oggetto di remissione riveste una importanza strategica nelle azioni investigative di contrasto al crimine di qualunque natura e confine (comune, organizzato, nazionale e/o internazionale), ed è terreno di frizione di interessi tutelati a livello costituzionale e comunitario, tenuto conto di quanto a breve verrà evidenziato. Sullo sfondo si staglia, in modo dirompente, la imponente espansione del perimetro, tradizionalmente circoscritto, delle intercettazioni di comunicazioni tra presenti, ottenute per il tramite dell'uso del c.d. *virus* informatico, oggi rese necessarie dalla diffusione di modalità di comunicazione a carattere cifrato (*whatsapp, facebook, instagram*).

Al fine di meglio comprendere la questione oggetto di analisi dalla Suprema Corte, appare necessario illustrare, a brevi tratti, la natura della intercettazione telematica attiva, meglio conosciuta con il nome di "intercettazione con *trojan*".
L'evoluzione nella gestione delle strategie di diffusione delle telecomunicazioni, unita alla necessità di contenimento dei costi ad opera degli operatori telefonici, ed altresì, alla crescente esponenziale richiesta di accesso alla rete, hanno, di fatto, comportato la deviazione della stragrande maggioranza del traffico voce (si stima un volume pari a quasi il 90% del totale) su canali di trasmissione basati su protocolli *over IP*[4], gestiti da licenziatari di *APP* che, allocando i propri *server* al di fuori del territorio italiano – e, quindi, non agendo quali concessionari di pubblico servizio – sfuggono alle prestazioni obbligatorie[5] previste dalla normativa italiana, ivi compresa la cessione del "protocollo di decodifica" del segnale digitale, nel quale viene convertito il flusso voce in transito sulla rete di trasporto.

Gli organi di investigazione, infatti, chiamati a dare esecuzione alle operazioni di intercettazione a seguito di autorizzazione della A.G., provvedono a comunicare la numerazione della utenza *target* al gestore titolare, così da permettere all'operatore di rete l'aggiornamento degli elenchi sui propri sistemi informativi.[6] Le conversazioni così catturate vengono, successivamente, trasmesse, con linea dedicata sicura (V.P.N.), al *server* installato presso la Procura della Repubblica. Snodo essenziale della menzionata modalità di captazione[7] è la disponibilità dei protocolli di decodifica, unico strumento che consente di leggere in chiaro il flusso delle

1 Cass. Pen. SS.UU, 28 aprile 2016, Scurato, n.13;

2 Cass. pen., sez. VI, ord. 10 marzo 2016 (dep. 6 aprile 2016), Scurato, n.359

3 Cass. pen., sez. VI, 26 maggio 2015, Musumeci , n. 27100;

4 Voice over IP (Voce tramite protocollo Internet), acronimo VoIP, è la tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o una qualsiasi altra rete dedicata a commutazione di pacchetto che utilizzi il protocollo IP senza connessione per il trasporto dati.

5 Al Codice delle Comunicazioni Elettroniche (c.c.e.), istituito con il D.lgs. 1° agosto 2003, n. 259 in attuazione della direttiva europea 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica si deve l'effettiva, nonché prima, introduzione nel nostro ordinamento del concetto di "prestazioni obbligatorie" per gli operatori di telecomunicazioni verso l'Autorità Giudiziaria.

6 I sistemi informativi preposti alla gestione centralizzata dell'elenco dei target configurano il relativo modulo *software* presente sulle centrali di commutazione, il quale controlla tutte le numerazioni in entrata e/o uscita e che, individuata una utenza target in transito, provvede ad attivare l'intercettazione telefonica vera e propria.

7 Ci si riferisce alla modalità di captazione nota come M.D.N. (man in the midle), in ragione della posizione che l'organo investigativo assume rispetto al flusso delle comunicazioni, ovvero al centro dei due poli della conversazione.

comunicazioni intercettate. Ebbene, a differenza di ciò che è previsto per i gestori di rete che operano nel territorio italiano – siano essi "strutturati" (TIM, Wind, Vodafone, H3G) che "virtuali" (Postemobile) – tutti tenuti al rilascio del protocollo di decodifica – gli operatori che convogliano il traffico sui protocolli internet, mediante *server* non allocati sul territorio italiano (quali *whatsapp, telegram, facebook, wiber*), non sono tenuti a tale prestazione.

I flussi dati delle conversazioni vengono, comunque, intercettati, anche se gestiti da soggetti non allocati sul territorio italiano, atteso che essi viaggiano in internet per il tramite degli operatori di rete che gestiscono l'utenza *target*; l'assenza, tuttavia, del protocollo di decodifica rende i dati intercettati non visibili e, di fatto, inutili ai fini d'indagine. **Non stupisca, quindi, la sentita necessità degli organi di investigazione di annullare le cennate criticità modulando diversamente la strategia di indagine**.
Il risultato è stato quello di variare il baricentro delle attività tecniche, trascinandolo dal centro a monte dei poli della comunicazione, ovvero nel cuore del dispositivo utilizzato, così da privare di utilità pratica i protocolli di decodifica. I**n altri termini quando un messaggio di testo inviato, ad esempio, per il tramite di *Whatsapp*, viaggia in rete esso è cifrato; nell'istante, tuttavia, in cui viene scritto o letto esso appare in chiaro**.

Tale è la funzione del *trojan*, noto anche come "virus di Stato", *malware* installato *on site*, all'interno di un dispositivo *target* (da qui, l'allegorico "*trojan horse*"), ed il cui compito è quello di effettuare un monitoraggio costante della utenza "bersaglio", ovunque si trovi il soggetto che ne abbia la disponibilità, così da bypassare l'assenza dei protocolli di decodifica. Il monitoraggio del *target* potrà avvenire, quindi, attivando da remoto il microfono, così da trasformare il dispositivo in un registratore vocale permanente, ovvero attivando, sempre da remoto, la videocamera, così da rendere il dispositivo uno strumento di pedinamento, osservazione e controllo ininterrotto. Non appare possibile, in questa sede, analizzare compiutamente e dettagliatamente uno strumento, quale il *trojan autoinstallante*, complessivamente molto articolato e complesso.
Il *virus* informatico, difatti, offre innumerevoli utilità: basti pensare, a mero titolo esemplificativo, alla possibilità di poter copiare le *password* di accesso alle *mail* del *target*, alla opportunità di poter monitorare costantemente le *chat* anche mediante *screenshot*, al vantaggio di poter accedere alla rubrica ed alla messaggistica pregressa. Temi vertiginosi che qui, dunque, possono solo essere accennati.

Ciò posto appare evidente quali e quante possano essere le implicazioni che una tale modalità di captazione offra sul piano processuale. Intuibile, altresì, la frizione con i valori di libertà e segretezza delle comunicazioni riconosciuti dalla Carta costituzionale, il cui esatto contemperamento richiede chiara la nozione di intercettazione. Orbene, il codice di rito, se da un lato, distingue le intercettazioni delle comunicazioni telefoniche (art. 266, comma I c.p.p.), da quelle ambientali (art. 266, comma II c.p.p.) e da quelle telematiche (266-*bis* c.p.p.), dall'altro, tuttavia, **non fornisce una definizione del concetto di intercettazione, limitandosi a determinarne i limiti di ammissibilità** (art. 266 c.p.p.), **i presupposti e le forme del provvedimento (art. 267 c.p.p.), le modalità di esecuzione, nonché l'utilizzabilità dei risultati nello stesso procedimento (art. 271 c.p.p.) ovvero in procedimenti diversi**.
Definire, nel silenzio del legislatore, la nozione di intercettazione è stata, pertanto, un'operazione estremamente complessa. È stato necessario attendere, infatti, quasi tre lustri dalla data di entrata in vigore del codice Vassalli perché il panorama giurisprudenziale (fino a quel momento eccessivamente incerto) venisse stabilizzato dalla ormai famosa sentenza Torcasio della Corte di Cassazione[8], nel corpo della quale, magistralmente, **sono stati elencati i tre presupposti necessari affinché una registrazione di conversazione potesse essere qualificata quale intercettazione**, e in quanto tale subordinata al regime di cui agli artt. 266 ss c.p.p., e non al diverso regime processuale della prova documentale previsto dall'art. 234 c.p.p.

La sentenza del 2003 definisce intercettazione *"l'apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio*". Essa limita, dunque, ed in modo significativo, il campo applicativo della suddetta normativa al contemporaneo sussistere di tre distinti presupposti:

1. *"i soggetti devono comunicare tra loro, con il preciso intento di escludere estranei dal contenuto della comunicazione, e secondo modalità tali da tenere quest'ultima segreta"*;
2. *"è necessario l'uso di strumenti tecnici di percezione (elettro-meccanici o elettronici), particolarmente invasivi ed insidiosi, idonei a superare le cautele elementari che dovrebbero garantire la libertà e segretezza del colloquio e a captarne i contenuti"*;
3. *"l'assoluta estraneità al colloquio del soggetto captante che, in modo clandestino, consenta la violazione della segretezza della conversazione"*;

Alla luce di tali coordinate giurisprudenziali deve leggersi la distinzione operata dal codice tra intercettazioni della comunicazioni telefoniche (c.d. intercettazioni tra assenti), intercettazioni delle comunicazioni ambientali (c.d. intercettazioni tra presenti) e intercettazioni tra sistemi informatici o telematici (c.d. intercettazioni telematiche). **Una netta distinzione da cui deriva una, altrettanta netta ed evidente, separazione che il codice impone tra la disciplina delle intercettazione tra persone distanti (intercettazioni telefoniche) e la disciplina delle intercettazione tra presenti (intercettazioni ambientali), nel momento in cui queste ultime avvengano in luoghi di privata dimora**. Distinzione che trova, evidentemente, la sua giustificazione nei diversi interessi costituzionali tutelati: nelle intercettazioni tra persone distanti viene in rilievo il diritto costituzionale alla libertà e segretezza delle comunicazioni (art. 15 Cost.), nelle intercettazioni tra presenti che avvengano in luoghi di privata dimora viene in rilievo, anche, il diritto alla inviolabilità del domicilio (art. 14 Cost.)[9].
Alla qualificata garanzia, comune a tutte le tipologie di intercettazioni, della doppia riserva di legge e di giurisdizione, ovvero ai presupposti dei gravi indizi di reato e della assoluta indispensabilità alla prosecuzione delle indagini (art. 267 c.p.p.), il legislatore

8 Cass. pen., Sez. Un., 26 maggio 2003, n. 36747, in Guida dir., 2015, n. 41, p. 83.

9 Principi ribaditi, attesa la progressiva attrazione della materia dei diritti nell'orbita del sistema *multilevel* di interpretazione, dalle norme convenzionali che tutelano il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, a fronte di ingerenze di una pubblica autorità (art. 8 C.E.D.U.).

affianca, dunque, con riferimento alle sole intercettazioni tra presenti in luoghi di privata dimora, un filtro ulteriore e più stringente: **la captazione "domiciliare" è consentita sempre che sussista il fondato motivo che nel luogo di privata dimora si stia svolgendo l'attività criminosa**. Un argine posto a presidio di un interesse costituzionale – quello della inviolabilità del domicilio – compromesso in aggiunta a quello della libertà e segretezza delle comunicazioni. **In siffatta cornice si inscrive la questione decisa dalla Corte di Cassazione nella sentenza in commento, chiamata a verificare la utilizzabilità di captazioni ambientali ottenute per il tramite del *trojan*.** Lo scoglio ermeneutico affrontato dalla Corte attiene, infatti, alla compatibilità delle descritte modalità operative del *software - trojan* con la disciplina delle intercettazioni ambientali come sopra illustrate.

Le sezioni Unite, tuttavia, sono state chiamate a pronunciarsi con riferimento ad un procedimento relativo a delitti di criminalità organizzata, che come noto, godono di un regime derogatorio per ciò che concerne le attività di intercettazione ambientale, per le quali la legge non opera distinzione in ordine al luogo in cui le stesse sono svolte. Deroga che ha creato non poche perplessità sull'ambito di estensione del principio enunciato nella sentenza in commento. Il principio di diritto elaborato è il seguente: *"limitatamente ai procedimenti per delitti di criminalità organizzata è consentita l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (personal computer, tablet, smartphone) anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attiivtà criminosa.*

Resta il dubbio se la Cassazione abbia voluto limitare l'uso del *trojan* ai soli procedimenti di criminalità organizzata, implicitamente negandone la legittimità laddove esso venga impiegato nei procedimenti per delitti comuni, **ovvero si sia limitata a prendere posizione solo ed esclusivamente sulla questione oggetto di remissione**, lasciando a future decisioni il tema della utilizzabilità dei risultati di intercettazione mediante *trojan* nei procedimenti per i delitti da ultimo menzionati.
Chi scrive è della opinione che la Corte abbia voluto limitare il proprio *dictum* ai soli procedimenti per delitti di criminalità organizzata, perché così richiesto nella ordinanza di remissione, senza voler implicitamente negare la legittimità del *trojan* laddove impiegato nei procedimenti per delitti comuni, fermo restando, attenendosi al percorso motivazionale seguito, che l'utilizzo del *virus* autoinstallante per le investigazioni afferenti i procedimenti di criminalità comune impone una prescrizione ulteriore, da contenersi nel decreto autorizzativo, **avente ad oggetto l'indicazione del luogo in cui le attività di captazione possono essere avviate; luogo che, salvo il sussistere del presupposto di legge, non potrà ricadere, pena l'inutilizzabilità, nei luoghi di privata dimora**. Sarà, quindi, onere del p.m. nella richiesta e del g.i.p. nel decreto di autorizzazione indicare i luoghi nei quali il dispositivo potrà essere attivato da remoto, luoghi che dovranno essere diversi da quelli di privata dimora, pena la sanzione processuale sopra indicata.

Ragionare diversamente significherebbe privare i procedimenti per delitti di criminalità ordinaria, che si badi bene sono, nella stragrande maggioranza dei casi, i precursori dei procedimenti per delitti di criminalità organizzata, di uno strumento di indagine di eccellente capacità investigativa, atteso che come sopra detto, il 90 % delle conversazioni viaggia su canali cifrati.
L'auspicio è, comunque, che l' ammissibilità del *trojan* nei procedimenti per delitti di criminalità comune venga affrontato e risolto, a stretto giro, dal Giudice della nomofilachia e ciò all'evidente fine di eliminare quel margine di incertezza che, ancora oggi, serpeggia tra gli interpreti del diritto, nella certa convinzione che i futuri *dicta* della Corte di Cassazione sapranno tenere in debito conto, da una parte, il rispetto di diritti costituzionalmente garantiti agli individui, quali la riservatezza delle comunicazioni e la inviolabilità del domicilio, e dall'altra gli altrettanto rilevanti interessi della sicurezza e dell'ordine pubblico, mai come oggi in condizione di assoluto pericolo.

Si aprirà, certamente e comunque, un fronte di elevata criticità quanto meno in punto di prova del luogo in cui è stato attivato il *trojan* e, quindi, del luogo in cui è stata eseguita l'attività di captazione, al fine di stabilire se trattasi di luogo di privata dimora, con conseguente inutilizzabilità dei risultati acquisiti, ovvero in luogo non di privata dimora, con conseguente utilizzabilità dei relativi risultati di prova acquisiti. **Non appare, tuttavia, ancora chiaro a chi spetterà l'onere di provare che una data conversazione si sia svolta o meno in un luogo di privata dimora**, fermo restando che l'inutilizzabilità è un risultato a favore dell'indagato ed in quanto tale la relativa eccezione e la relativa prova dovrà essere fornita dalla difesa, con rischi in punto di inversione del meccanismo dell'onere della prova che nel sistema processuale penale italiano è a carico del p.m. Sul punto appare utile riportare quanto affermato nella ordinanza di remissione Musumeci in nota citata nella parte in cui afferma *"in ogni caso deve riconoscersi che non sempre sarà immediatamente evidente che si tratti di intercettazione eseguita in uno dei luoghi indicati dall'art. 614 c.p., sicchè appare essenziale l'apporto della difesa nell'indicare le conversazioni inutilizzabili"*.

Sono questioni che la giurisprudenza prossima dovrà affrontare e risolvere a salvaguardia delle attività investigative in corso. Ed invero, fatti salvi i casi di osservazione diretta ad opera della P.G., o di informazione fornita da testimone o desumibile dallo stesso contenuto della conversazione intercettata, sarà veramente arduo, se non tecnicamente impossibile, fornire prova esatta del luogo in cui è svolto il colloquio intercettato. **L'individuazione esatta della luogo in cui è stata catturata una conversazione potrebbe ottenersi attivando, ad esempio, da remoto il localizzatore G.P.S.**, presente su quasi tutti i dispositivi mobili di ultima generazione, così da avere un dato di georeferenziazione di assoluta precisione, fermo restando che l'attivazione da remoto della localizzazione sarebbe visibile dal *target*, visualizzandosi la relativa icona sul *display* del cellulare, con ovvie implicazioni in termini di segretezza della investigazioni in corso.

In conclusione la Corte di Cassazione, con la pronuncia in commento, lungi dall'aver fornito la quadra del tema in analisi ha, semplicemente, fissato le prime linee guida sul tema delle intercettazione mediante virus autoinstallante, da una parte ammettendone la legittimità, dall'altra limitandola ai procedimenti per delitti di criminalità organizzata.
Si attendono in futuro nuove pronunciamenti che diano le soluzione ai numerosi quesiti che la cennata sentenza ha, comunque, lasciato irrisolti. ©