di Maria Milia

ESTESO L'UTILIZZO DEL TROJAN PER LE INTERCETTAZIONI TRA PRESENTI ANCHE AI DELITTI CONTRO LA P.A.

Maria MILIA è Sostituto Procuratore della Repubblica presso il Tribunale di Marsala Ha conseguito il master di II livello in Scienze della sicurezza presso l'Università degli Studi "La Sapienza" di Roma.È autrice di pubblicazioni in materia di procedura penale.

Legge 9 gennaio 2019, n. 3

La nuova legge Anticorruzione apporta modifiche al Codice di procedura penale agli articoli 266 e 267. In particolare prevede che l'utilizzo del trojan su dispositivo elettronico portatile per intercettazione tra presenti possa essere utilizzata anche "per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4".

I. Come è noto, le captazioni disposte, a distanza ed in modo occulto, attraverso l'istallazione di programmi informatici (conosciuti con i nomi *trojan horse* o *spy-software* o, nella pronunce giurisprudenziali, come captatore informatico), su *computer*, *tablet* o *smartphone* (c.d. *target*), per mezzo del loro invio con una *mail*, un *sms* o un'applicazione di aggiornamento, consentono di acquisire tutto il traffico dei dati in arrivo o in partenza dal dispositivo infettato e di trasmetterli, per mezzo della rete *internet*, in tempo reale o ad intervalli prestabiliti, ad altro sistema informatico in uso agli investigatori.
In realtà molto più ampie e penetranti sono le potenzialità di detti strumenti, in quanto essi consentirebbero altresì di attivare il microfono e/o la *web camera* del bersaglio, di perquisirne l'*hard disk* e di fare copia delle unità di memoria del suo sistema informatico, di carpire ciò che viene digitato sulla sua tastiera e di visualizzarne lo schermo.
Diventa dunque profilo vulnerabile, in termini di segretezza delle conversazioni e comunicazioni, l'ormai quotidiano uso di strumenti informatici del tipo di quelli sopra indicati e utilmente sfruttabile, ai fini investigativi, il dato di comune esperienza che sempre meno ci si separa da detti strumenti elettronici.

Risulta allora immediatamente percepibile come un'intercettazione captativa "portatile", al pari dei dispositivi sui quali viene attivata, incida maggiormente nella sfera privata del soggetto rispetto a un'intercettazione tradizionale.
Anche il tipo di captazione in argomento va ricondotto nell'ambito delle intercettazioni c.d. "ambientali", soggette alla disciplina dell'art. 266, comma 2, c.p.p., inclusa la necessità che, qualora si svolgano all'interno di luoghi di privata dimora, vi sia fondato motivo di ritenere che ivi sia in atto un'attività criminosa.

Ciò avrebbe comportato – come sottolineato da parte della giurisprudenza di legittimità – che la captazione "da remoto", tramite il c.d. agente intrusore all'interno di un dispositivo elettronico portatile, fosse autorizzata con un decreto che individuasse con precisione i luoghi in cui espletare l'attività captativa (*arg. ex* Cass., Sez. VI, n. 27100 del 26/05/2015, Rv. 265654 – 01).
È risultata, da subito, evidente la difficoltà di individuare *ex ante* luoghi circoscritti interessati dalla peculiare attività captativa su dispositivi portatili, tanto da dare vita a contrasti che hanno reso necessario l'intervento della Suprema Corte di Cassazione, a Sezioni Unite, che si è pronunciata con la nota sentenza Scurato (Cass. Sez. U, n. 26889 del 28/04/2016, Rv. 266905 – 01), ritenendo,

per ragioni tecniche, incompatibile l'intercettazione mediante captatore informatico nelle indagini per reati in relazione ai quali la disciplina normativa è differente a secondo che la captazione avvenga o meno all'interno dei luoghi di privata dimora, dovendo il decreto autorizzativo relativo ad una intercettazione domiciliare individuare i luoghi ove essa debba svolgersi, sebbene detta specificazione - secondo la Suprema Corte – rilevi ai fini delle sole modalità esecutive del mezzo di ricerca della prova (non assurgendo a condizione di legittimità dell'intercettazione).

La sentenza in argomento ha infatti definito tale metodologia investigativa come intercettazione "itinerante" del tipo "ambientale", caratterizzata dal fatto che l'attività di captazione segue tutti gli spostamenti nello spazio dell'utilizzatore, rilevando come il limite di ammissibilità delle intercettazioni domiciliari per i reati comuni – rappresentato dalla necessità, ai sensi dell'art. 266 comma 2 c.p.p., che nel luogo oggetto di captazione si stia svolgendo attività criminosa – in ragione delle peculiari "modalità esecutive" che imporrebbero anche per esse l'indicazione di un luogo circoscritto *ex ante* in cui debba avvenire la captazione, ne renderebbe impossibile il legittimo uso, data la natura particolare dello strumento probatorio, e renderebbe impossibile il controllo del giudice sulla ricorrenza del predetto requisito, quantomeno al momento dell'autorizzazione della predetta intercettazione (e ciò anche qualora, durante il materiale svolgimento delle operazioni, venisse interrotta la captazione nel caso di ingresso in un luogo di privata dimora).
Indicazione specifica del luogo di privata dimora in cui esse si svolgeranno che invece non è richiesta per le intercettazioni tra presenti da espletare in luoghi diversi da quelli indicati dall'art. 614 c.p., per le quali basta che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti dove essa va eseguita.

Ciò in quanto in tali casi – come già rilevato da pronunce precedenti a quella in esame – l'ambiente in cui deve avvenire l'intercettazione rileva come "tipo" e l'eventuale suo concreto mutamento non ha conseguenze sulla utilizzabilità delle conversazioni captate, purché anche il nuovo ambiente appartenga alla tipologia originariamente autorizzata (tra le molte, Cass., Sez. II, n. 17894 del 29/04/2014, RV. 259255); e "la modifica dell'ambiente da intercettare, purché omogeneo a quello autorizzato, attenendo alla fase esecutiva del provvedimento, non richiede la rinnovazione del decreto" (v. Cass., Sez. V, n. 44997 del 28/10/2011, Rv. 251443 – 01).
Per converso, la Suprema Corte ha rilevato come solo per le intercettazioni relative a procedimenti di criminalità organizzata (regolate dalla norma speciale derogatrice di cui all'art. 13 del decreto-legge n. 152 del 1991, convertito dalla legge n. 203/91) l'indicazione del luogo risulta irrilevante, dal momento che, in tal caso, le captazioni delle conversazioni nei luoghi di privata dimora non sono soggette ad alcuna disciplina in deroga rispetto a quella che regola le intercettazioni in altri luoghi, potendo esse avvenire in ambienti pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa, sicché nessun conseguenza discenderebbe dall'impiego della particolare modalità tecnica del "virus informatico".
In altri termini – secondo i giudici di legittimità – deve escludersi la possibilità di intercettazioni nei luoghi indicati dall'art. 614 c.p. con il mezzo del captatore informatico al di fuori della disciplina derogatoria di cui all'art. 13 della legge n. 203 del 1991, perché non potrebbe essere assicurato il rispetto dei limiti della disciplina codicistica.
Ed in considerazione della forza intrusiva del mezzo usato, al fine di circoscriverne l'effettivo uso ai procedimenti di criminalità organizzata, la giurisprudenza di legittimità successiva alla pronuncia delle Sezioni Unite, richiedeva che la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, risultasse ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso.

Il richiamo dei principi sanciti dalle Sezioni Uniti nella sentenza Scurato, come sopra sintetizzati, risulta fondamentale perché – come meglio si vedrà a breve – ancora ad oggi e fino all'integrale entrata in vigore delle norme di cui agli articoli 266 e 267 c.p.p., come modificate dal d. l. n. 216 del 2017, la disciplina attualmente applicabile alle intercettazioni eseguite mediante captatore informatico, anche per i reati contro la pubblica amministrazione, è quella derivante dall'interpretazione che delle norme codicistiche in tema di intercettazioni – nella formulazione antecedente alle modifiche apportate dall'art. 4 d. l. 216/2017 non ancora vigenti – aveva fornito la predetta pronuncia, applicandola al testo normativo modificato dall'art. 6 del cd. decreto intercettazioni e dalle norme di cui alla l. 3/2019, disposizioni queste ultime già entrate in vigore.

II. Il legislatore, intervenuto con la c.d. Riforma Orlando (decreto legislativo n. 216 del 29 dicembre 2017, emanato dal Governo in attuazione della Legge delega n. 103/2017, pubblicato in Gazzetta Ufficiale l'11 gennaio 2018 e che avrebbe dovuto trovare applicazione 180 giorni dopo l'entrata in vigore del decreto stesso, cioè a partire dal 26 luglio 2018) a disciplinare anche l'utilizzo dei *trojan* a fini investigativi penali, prima delle più recenti modifiche apportate con la c.d. legge Spazzacorrotti, superava le suddette conclusioni delle Sezioni Unite del 2016, con particolare riferimento alla teoria della c.d. "intercettazione ambientale itinerante" ed all'asserita incompatibilità – motivata da ragioni tecniche – fra uso del captatore e applicazione della disciplina codicistica.
In particolare, ai sensi dell'art. 9 comma 1, della nuova normativa sopra richiamata sono applicabili dal 26 gennaio 2018 (data di entrata in vigore del decreto n. 216/2017, cosiddetto Decreto Intercettazioni), le disposizioni speciali dell'art. 6 d.lgs. n. 216/2017, che prevede al primo comma l'estensione per i reati contro la pubblica amministrazione della disciplina derogatoria dell'art. 13 del d.l. n. 152/1991, conv. in legge n. 203/1991, ed al comma secondo ribadiva (in quanto ormai abrogato), anche nelle indagini per i reati contro la pubblica amministrazione, la necessità che le intercettazioni domiciliari si svolgessero nei luoghi in cui vi era motivo di ritenere che si stesse svolgendo l'attività criminosa.
Tuttavia la disciplina generale sul captatore, contenuta nell'art. 4 del citato decreto, non è allo stato applicabile per effetto dei successivi interventi normativi che ne hanno posticipato il momento di entrata in vigore.

Il d.lgs. n. 216/2017 distingue fra intercettazioni domiciliari ed extradomiciliari e fra procedimenti per reati comuni e per reati di criminalità organizzata. È previsto che l'utilizzo dei captatori per i delitti previsti all'art. 51, comma 3 *bis* e *quater*, c.p.p. (reati associativi e con finalità di terrorismo) sia sempre consentito senza alcuna limitazione e, per quelle domiciliari, anche a

prescindere dal fatto che si abbia motivo di ritenere che in tali luoghi si stia svolgendo l'attività criminosa, ai sensi del nuovo comma 2 *bis* dell'art. 266 c.p.p., mentre per gli altri reati rientranti nelle previsioni dell'art. 266 c.p.p., per le intercettazioni domiciliari eseguite tramite captatore, ai sensi dell'art. 266, comma 2, c.p.p. (ammesse sempre e solo se vi sia motivo di ritenere che nei luoghi domiciliari si stia svolgendo l'attività criminosa), si richiede l'indicazione, nel provvedimento autorizzativo, del luogo di attivazione del microfono (al fine di controllare la ricorrenza della predetta condizione).
Il testo normativo in esame prescrive inoltre che, nel decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, vengano indicate "le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonché, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3 *bis* e 3 *quater* , i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono" (art. 267, comma 1, c.p.p., come modificato dall'art. 4 d.lgs. n. 216/2017).

È stato al riguardo osservato come nessuna analoga indicazione *ex ante* sia richiesta anche per le intercettazioni extradomiciliari, secondo la nuova prescrizione di cui all'art. 267, comma 1, c.p.p. (non ancora applicabile ai sensi dell'art. 9, comma 1, d.lgs. n. 216/2017), potendosi operare anche attraverso l'attivazione e la disattivazione del microfono presente nel dispositivo portatile. Sebbene la necessità di simile specificazione sembrerebbe discendere dalla particolare natura dello strumento utilizzato che altrimenti sfuggirebbe a valutazioni anticipate sulla possibilità che vengano violati i divieti di cui sopra (M. Bontempelli, *Il captatore informatico in attesa della riforma*, in Dir. pen. cont., 20 dicembre 2018, p.9).
La previsione dell'art. 267, comma 1, c.p.p. rafforza l'onere motivazionale del giudice per le indagini preliminari richiedendogli di indicare "le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini".
Nel comma 1 *bis* dell'art. 270 c.p.p. viene poi prevista l'inutilizzabilità, ai fini di prova, dei risultati conseguiti con il captatore informatico, per i reati diversi da quelli oggetto del provvedimento autorizzativo, "salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza".

È stata evidenziata la distanza che viene, in tal modo, tracciata rispetto all'utilizzabilità dei risultati conseguiti mediante le intercettazioni cc.dd. tradizionali che, sotto la vigenza dell'art. 270, comma 1, c.p.p., facendo perno su un'interpretazione restrittiva della locuzione "procedimenti diversi" (nei quali è esclusa l'utilizzabilità dei risultati delle predette intercettazioni, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza), era stata estesa – per consolidata giurisprudenza di legittimità (v. Cass., Sez. III, n. 28516 del 20.06.2018, RV. 273226; anche Cass., Sez. Un., n. 32697 del 23.07.2014, RV. 259776) – alle "indagini strettamente connesse e collegate sotto il profilo oggettivo, probatorio e finalistico al reato in ordine al quale il mezzo di ricerca della prova è stato disposto» (cfr. sul punto O. Calavita, *L'odissea del* trojan horse - *Tra potenzialità tecniche e lacune normative*, in Dir. pen. cont., 11/2018, p. 74 e ss., anche per ulteriori rimandi).

Ai sensi dell'art. 267, c. 2 *bis*, c.p.p. il pubblico ministero, inoltre, potrà disporre l'intercettazione tra presenti, a mezzo del captatore in via d'urgenza, solo per i reati di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.; ma, oltre alla consueta necessità che sussista "fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio per le indagini", viene introdotta la necessità di indicare "le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice".
Infine la violazione dei limiti di tempo e di luogo indicati nel decreto autorizzativo viene espressamente sanzionata con l'inutilizzabilità dei dati acquisiti (a seguito dell'introduzione del comma 1 *bis* dell'art. 271 c.p.p. ad opera dell'art. 4, c. 1, lett. e, n. 1, del d.lgs. n. 216/2017).

Attengono invece all'aspetto tecnico le modifiche apportate dal decreto in esame all'art. 89 disp. att. c.p.p., il cui comma 2 *ter* prevede che, nei casi previsti dal comma 2 *bis* (che disciplina proprio l'installazione e l'intercettazione attraverso captatore informatico in dispositivi elettronici portatili), "le comunicazioni intercettate sono trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente verso gli impianti della procura della Repubblica. Durante il trasferimento dei dati sono operati controlli costanti di integrità, in modo da assicurare l'integrale corrispondenza tra quanto intercettato e quanto trasmesso e registrato".

Dal tenore della suddetta norma sembrerebbe dunque sufficiente il mero trasferimento e non anche la memorizzazione di detti dati all'interno dei *server* della Procura della Repubblica (cfr. M. A. Senor, C*ome funzionano i* trojan *di Stato? - Analisi delle norme e indicazioni operative*, in www.altalex.com, 22 gennaio 2018).
Come è noto – secondo la disciplina generale, come interpretata in maniera consolidata dalla giurisprudenza di legittimità – condizione necessaria per l'utilizzabilità delle intercettazioni è che l'attività di registrazione – che, sulla base delle tecnologie attualmente in uso, consiste nella immissione dei dati captati in una memoria informatica centralizzata – a**vvenga nei locali della Procura della Repubblica mediante l'utilizzo di impianti ivi esistenti,** mentre non rileva che negli stessi locali vengano successivamente svolte anche le ulteriori attività di ascolto, verbalizzazione ed eventuale riproduzione dei dati così registrati, che possono dunque essere eseguite "in remoto" presso gli uffici della polizia giudiziaria (Cass., Sez. U, n. 36359 del 26/06/2008, Rv. 240395).

È stato tuttavia chiarito che detta condizione necessaria per l'utilizzabilità delle intercettazioni può ritenersi rispettata anche se i *file* audio registrati non siano trasmessi automaticamente dagli apparecchi digitali adoperati per le captazioni tra presenti ma siano periodicamente prelevati dalla polizia giudiziaria incaricata delle operazioni e riversati "a mano" nel *server* dell'ufficio requirente (cfr. Cass., Sez. I, n. 52464 del 08/11/2017, Rv. 271541 – 01), essendo dette modalità di consegna solo conseguenza degli strumenti di registrazione utilizzati non rilevanti ai fini dell'osservanza delle regole sull'utilizzo degli impianti.
Pertanto, si potrebbe ritenere che le condizioni alle quali l'art. 268, comma 3, c.p.p. subordina l'utilizzabilità delle intercettazioni siano rispettate quando le attività di ascolto traggono origine dal riversamento dei *file* audio nel *server* dell'Ufficio requirente (*arg. ex* Cass., Sez. II, n. 52016 del 21/11/2014, Rv. 261625 – 01).
L'entrata in vigore delle disposizioni introdotte con il decreto del 2017 è stata più volte posticipata, dapprima, dal d.l. n. 91/2018, conv. in l. n. 108/2018, anche nella parte sull'utilizzo del captatore, ai sensi del quale la nuova regolamentazione troverà applicazione "alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019" (art. 9 comma 1 d.lgs. n. 216/2017, come modificata dal d.l. n. 91/2018, conv. in l. n. 108/2018) e, successivamente, **con l'art. 1 c. 1139 l. 145/2018, che ne ha differito l'applicazione "alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019**".

III. Ma ancor prima che potesse dispiegare, *in toto*, la sua efficacia la normativa sin qui richiamata, è intervenuta in materia la l. 9 gennaio 2019 n. 3, appellata come Spazzacorrotti, avente ad oggetto "Misure per il contrasto dei reati contro la Pubblica Amministrazione nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e dei movimenti politici", pubblicata sulla Gazzetta Ufficiale Serie Generale n. 13 del 16/01/2019 e costituita da un unico articolo articolato in 30 commi, che ha apportato rilevanti modifiche al decreto legislativo 216 del 29 dicembre 2017.
Tra le ragioni alla base dell'intervento legislativo in argomento è stata individuata la presa di coscienza che i reati quali la corruzione costituiscono un fenomeno che necessitava di un intervento riformatore, anche perché generatore di costi illeciti integranti un elemento di valutazione delle prospettive di investimento (G. Spangher, *Il sottosistema dei reati dei p.u. contro la pubblica amministrazione,* in www.giustiziainsieme.it, 19 febbraio 2019).

Con la legge Spazzacorrotti si assottiglia la distanza di metodo tra le indagini, condotte con strumenti informatici invasivi quali i *trojan horse,* relative a reati per criminalità organizzata e terrorismo e quelle per tipologie di reati puniti con la reclusione non inferiore nel massimo a cinque anni, segnatamente quelli dei pubblici ufficiali contro la pubblica amministrazione, escludendo, dunque, i delitti commessi dai privati contro la pubblica amministrazione.
Viene infatti abrogato il comma 2 dell'art. 6 del d.lgs. 216/2017 che stabiliva: "L'intercettazione di comunicazioni tra presenti nei luoghi indicati dall'art. 614 del codice penale non può essere eseguita mediante l'inserimento di un captatore informatico su dispositivo elettronico portatile quando non vi è motivo di ritenere che ivi sia stia svolgendo l'attività criminosa".
All'art. 266, comma 2 *bis*, introdotto dall'art. 4 del c.d. decreto intercettazioni, che prevedeva che "l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3 *-bis* e 3 *–quater*", sono aggiunte, infine, le seguenti parole: ", e per i delitti dei pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4" .
Parallelamente, all'articolo 267, comma 1, terzo periodo, vengono effettuati ulteriori innesti (inserendo dopo "all'articolo 51, commi 3-bis e 3-quater," le seguenti previsioni "e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4,"), richiedendo al giudice – a differenza che per i reati di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p. –, qualora si proceda per i suddetti reati, l'ulteriore onere motivazionale consistente nella necessità di indicare tempo e luoghi, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono.
Altro aspetto di non omogeneità rispetto alla disciplina normativa dettata per i delitti di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p. si rinviene poi nell'impossibilità per il pubblico ministero di disporre in via d'urgenza l'intercettazione mediante captatore informatico (art. 267 c. 2 *bis* c.p.p.).

Si è anche osservato come, poiché l'art. 1, comma 84, lett. *e*, n. 1, l. 103/2017 prescrive che "l'*attivazione del microfono* avvenga solo in conseguenza di apposito comando inviato da remoto" e l' art. 1, comma 84, lett. e, n. 2, l. 103/2017 si riferisce espressamente alla "*registrazione audio"* che deve essere avviata dalla polizia giudiziaria, sembrerebbe trovare spazio solo la registrazione audio (cfr. sul punto O. Calavita, *L'odissea del* trojan horse, cit., p. 69 e ss., anche per ulteriori rimandi).
Se poi venissero effettuate pure riprese video di comportamenti, è stato ipotizzato il ricorso anche in questo caso alla soluzione offerta dalla sentenza delle Sezioni Unite Prisco (Cass., Sez. Un., 28 luglio 2006, n. 26795), dovendosi distinguere tra comportamento comunicativo ovvero non comunicativo (O. Calavita, *L'odissea del* trojan horse, cit. p. 70 e ss., anche per ulteriori rimandi).

Segnatamente, nel caso in cui la ripresa audio-video capti comportamenti comunicativi (condotte di due soggetti che dialogano) troverebbe applicazione la disciplina delle intercettazioni. Invece, in caso di riprese di comportamenti non comunicativi (azioni, atteggiamenti e simili) sarebbe necessario distinguere in base al luogo in cui viene svolta la registrazione visiva. In caso di videoregistrazioni in luoghi pubblici, ovvero aperti o esposti al pubblico, eseguite dalla polizia giudiziaria, anche d'iniziativa, così come all'interno dei luoghi dove non si svolge la vita privata, esse andrebbero incluse nella categoria delle prove atipiche, soggette alla disciplina dettata dall'art. 189 c.p.p. e, trattandosi della documentazione di attività investigativa non ripetibile, possono essere allegate al relativo verbale e inserite nel fascicolo per il dibattimento (qualora invece non fossero effettuate nell'ambito del procedimento penale esse costituirebbero documenti ai sensi dell'art. 234 c.p.p.). Le riprese video di comportamenti non comunicativi non potrebbero invece essere eseguite all'interno del "domicilio", in quanto lesive dell'art. 14 Cost., in assenza di una disciplina che ne regoli la limitazione e, in quanto prova illecita, non potrebbe trovare applicazione la disciplina dettata dall'art. 189 c.p.p. (cfr. Corte Cost. n. 135 del 2001).

Nonostante le già rilevate potenzialità dei *trojan*, la scelta da ultimo effettuata dal legislatore sembrerebbe essere stata quella (in ragione dell'incidenza che essi hanno in *pejus* su diritti fondamentali e, quindi, della loro non estensibilità senza una esplicita previsione normativa) di limitarne l'utilizzo come strumento informatico atto ad intercettare le conversazioni tra presenti mediante l'attivazione da remoto del microfono del dispositivo previamente infettato, da adoperare soltanto su dispositivi portatili.
In altri termini non vengono disciplinati (e, pertanto, dovrà ritenersi, non sono ammessi) usi diversi da quello appena ricordato, come ad esempio, perquisizioni *on-line* o intercettazioni di messaggi in uscita con il controllo a distanza del *software* di comunicazione (es. programmi *e-mail*, *Messenger*, *WhatsApp*). Né possono essere controllati con captatori informatici i *computer* fissi (R. Orlandi, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in Riv. it. dir. proc. pen., 2018, pp. 544-545).

In sintesi, la disciplina dettata per le intercettazioni mediante uso del captatore informatico nell'ambito di un procedimento per delitti commessi da pubblici ufficiali contro la pubblica amministrazione puniti con pena non inferiore nel massimo a cinque anni, a seguito della combinazione degli interventi normativi sopra sintetizzati, prevede che potranno effettuarsi intercettazioni telefoniche e ambientali – anche all'interno dei luoghi di privata dimora e anche se non vi sia motivo di ritenere che in essi si stia svolgendo l'attività criminosa – sia tradizionali che mediante *trojan* qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini dello svolgimento delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20.
Tuttavia non si può ad oggi ritenere che le operazioni di captazione tramite *virus* informatico siano regolate dalle (e secondo le) modifiche normative sopra sintetizzate, in quanto la tecnica dell'innesto normativo praticato all'interno degli artt. 266 e 267 c.p.p., adottata dalla l. 3/2019, fa sì che le mere parole aggiunte "e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4" (già pienamente efficaci) arricchiscano statuizioni normative non ancora vigenti e contenenti la compiuta regolamentazione *in parte qua* del captatore. Ma, ciononostante, si può comunque ritenere che sia attualmente possibile fare ricorso allo strumento del captatore informatico anche per le indagini concernenti i reati dei pubblici ufficiali contro la pubblica amministrazione.
Ed invero, ai sensi degli artt. 6 e 9 del d.lgs. 216/2017 , dell'art. 2, comma 1, del decreto-legge 91/2018 poi convertito in legge e infine del comma 1139 dell'art. 11 della legge di Bilancio 2019, tali disposizioni sull'uso del *trojan horse* nelle indagini, inserite nella legge Spazzacorrotti, non sono soggette al rinvio "a dopo il 31.07.2019" della loro entrata in vigore, come per altri articoli del decreto 216/2017, e quindi sono divenute pienamente operative alla data del 31.01.2019 quando la legge 3/2019 è entrata in vigore.

Così come il citato art. 9 del decreto intercettazione non ha posticipato l'entrata in vigore della previsione dell'art. 6 del medesimo decreto, compreso il comma primo relativo all'estensione delle disposizioni di cui all'art. 13 del decreto-legge 13 maggio 1991, n. 1152, convertito con modificazioni dalla legge 12 luglio 1991, n. 203, ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni.
Ciò comporta che, venuta meno – per effetto delle modifiche apportate all'art. 266 comma 2 bis c.p.p. dalla legge Spazzacorrotti e dell'abrogazione del comma 2 dell'art. 6 d.lgs. 216/2017 – la rilevanza del luogo in cui si svolge la captazione anche nei procedimenti per reati contro la pubblica amministrazione individuati secondo i parametri sopra richiamati, l'estensione a questi ultimi della norma speciale derogatrice di cui all'art. 13 del d.l. n. 152 del 1991 (convertito dalla l. n. 203 del 1991), che non contiene una disciplina peculiare ed in deroga per le captazioni delle conversazioni nei luoghi di privata dimora rispetto agli altri luoghi, renderà legittimo anche per detti reati l'impiego della particolare modalità tecnica del "virus informatico", in applicazione di quanto affermato dalle Sezioni Unite nella sentenza Scurato sopra analizzata.

Se, infatti, anche per le intercettazioni ambientali nei procedimenti per tali reati è divenuto irrilevante il luogo in cui esse si svolgono – analogamente a quanto previsto dall'art. 13 d. l. 152/1991 – può applicarsi il principio espresso dalle Sezioni Unite nel 2016 secondo cui, in detti casi, "è consentita l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un captatore informatico in dispositivi elettronici portatili – anche nei luoghi di privata dimora *ex art*. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa". Inoltre, nell'attesa dell'entrata in vigore delle norme di cui agli artt. 266 e 267 c.p.p., così come modificate dal d. lgs. 216/2017, in questi procedimenti il giudice non dovrà neppure, allo stato, indicare tempo e luoghi, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono, che potrà effettuarsi – come appena osservato – in luoghi "pure non singolarmente individuati". ©