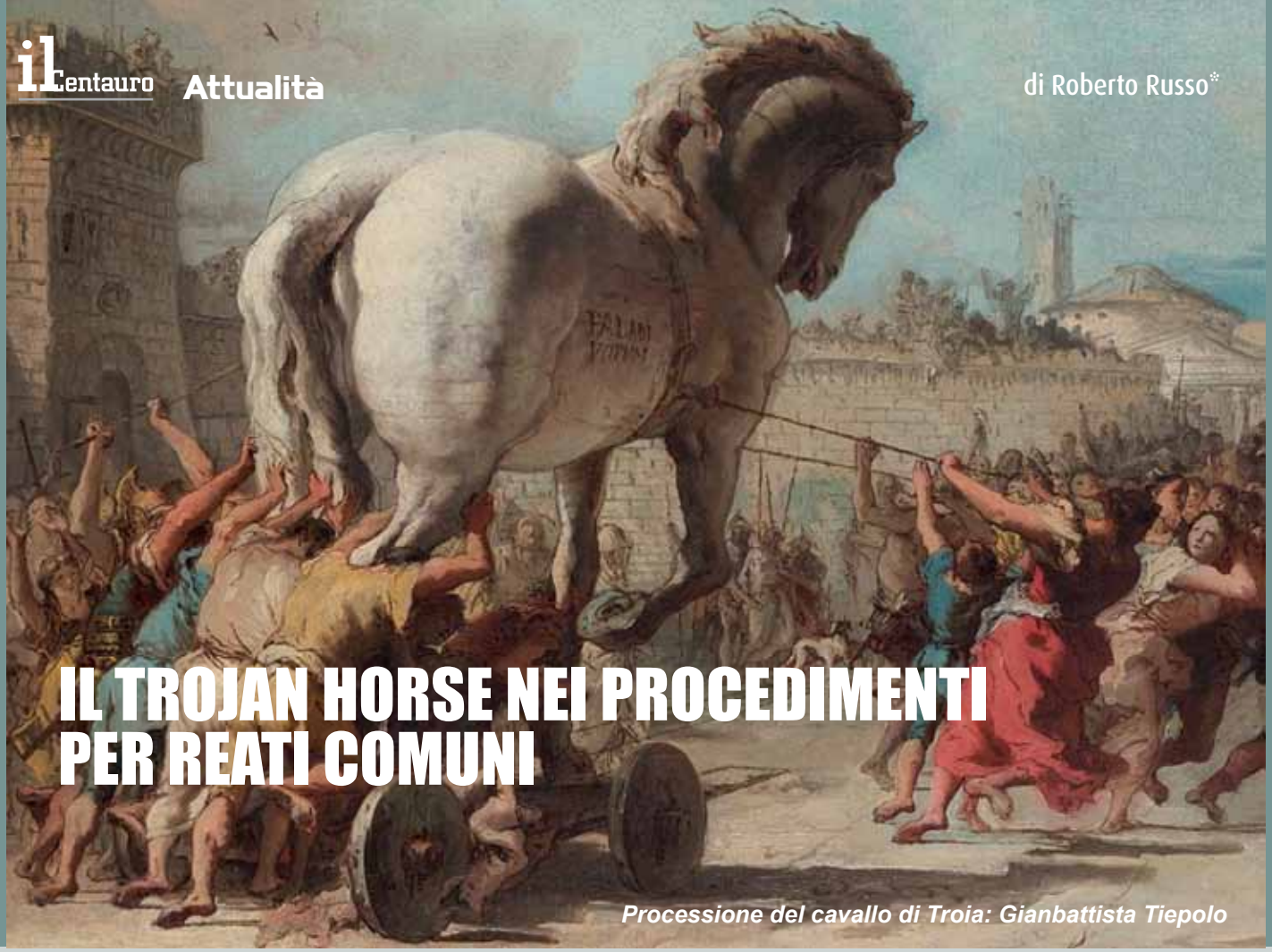
di Roberto Russo*

IL TROJAN HORSE NEI PROCEDIMENTI PER REATI COMUNI



Processione del cavallo di Troia: Gianbattista Tiepolo

Per i procedimenti penali iscritti dopo il 31 agosto 2020 il legislatore con il D.Lgs 29.12.2017, n. 216 ha previsto la possibilità di impiegare il virus informatico del tipo trojan horse, denominato "captatore informatico", anche per i reati comuni, pur se con determinati limiti.
Tale possibilità in precedenza era prevista solo per i reati elencati nell'art. 51, 3° co. bis e 3° co. quater (tipicamente quelli di criminalità organizzata e i reati associativi più gravi). Questo apre scenari di notevole interesse e aumenta non di poco le potenzialità investigative di questo strumento, fino a poco tempo fa riservato ai reati più gravi.

A voler essere precisi il citato D.Lgs. 216/2017 aveva previsto l'impiego del captatore per "le operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 dicembre 2019", ma il D.L. 30/12/2019, n. 161 ha modificato tale termine prevedendone l'applicazione ai procedimenti penali iscritti dopo il 30 aprile 2020 e tale termine è stato ulteriormente spostato dal D.L. 30/04/2020, n. 28 che ha previsto quello definitivo del 31 agosto 2020. Ma andiamo con ordine, cosa è?

Il trojan horse

Giuridicamente definito nell'art. 266 c.p.p. "**captatore informatico**" è un mezzo investigativo potentissimo che consente di trasformare un apparato elettronico dotato di connessione internet in una "microspia", con ciò intendendo un apparato per effettuare intercettazioni tra presenti, le c.d. "intercettazioni ambientali". Ma non solo, anzi molto di più.
Il *trojan* altro non è che un software, in particolare un *malware*, un virus della tipologia *trojan horse* che consente di prendere il completo controllo di un, mobile o fisso, e svolgere quasi qualsiasi tipo di operazione: da bloccare, modificare e cancellare i dati a mettere ko il sistema informatico. Ai fini di polizia giudiziaria il *trojan* si usa per accedere alle informazioni dell'apparato – tipicamente un telefono del tipo *smartphone* – nel quale viene inoculato. La denominazione captatore informatico nasce dalle prime sentenze nelle quali viene

definito tale (Sez. 5, n. 16556 del 14/10/2009, dep. 2010, Virruso, Rv. 246954) o "agente intrusore" (Sez. 6, n. 27100 del 26/05/2015, Musumeci, Rv. 265654). Tale software viene installato in un dispositivo (un computer, un tablet o uno smartphone), di norma a distanza e in modo occulto, mediante l'invio di una mail, un sms o un'applicazione di aggiornamento. Il software è costituito da due moduli principali: il server - programma di piccole dimensioni che infetta il dispositivo bersaglio - e il client - l'applicativo che il virus usa per controllare detto dispositivo.
Una volta inoculato il *trojan* consente:
- di captare il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia web mail, che outlook);
- di attivare il microfono e apprendere per tale via i colloqui intorno al dispositivo ovunque egli si trovi;
- di mettere in funzione la fotocamera, permettendo di carpire le immagini;
- di perquisire l'hard disk e di copiare l'unità di memoria del sistema informatico preso di mira;
- di decifrare ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*);
- di aggirare gli antivirus in commercio.

I dati raccolti sono poi inviati in tempo reale o ad intervalli prestabiliti ad altro sistema informatico in uso agli investigatori, tipicamente sfruttando la connessione wi-fi appena disponibile così da non gravare sul *bundle* dati dell'indagato, che potrebbe altrimenti allarmarsi notando un consumo anomalo.
Considerato che attualmente la comunicazione avviene ormai prioritariamente mediante connessione internet, sia per i costi inferiori, sia per taluno per ridurre il rischio di essere intercettato, tale sistema investigativo diventa fondamentale e apre nuove possibilità.
Utilizzando il *trojan* è possibile, come detto, anche cogliere i dialoghi tra presenti, ed in tal caso le intercettazioni diventano "ambientali". Il telefono cellulare, il *tablet* ed anche un *notebook*, infatti, sono divenuti oggetti che accompagnano ogni nostro movimento e ci seguono in ogni luogo, sicché il loro uso come mezzi di intercettazione permette di sottoporre l'individuo ad un penetrante controllo della sua vita.
Il *trojan* può essere impiegato sia per le intercettazioni tra presenti sia per le altre attività sopra descritte, motivo per il quale, generalmente si richiede l'autorizzazione all'intercettazione telematica, prevista dall'art. 266 bis e in parallelo, all'intercettazione di conversazioni tra presenti.
Tipicamente, una volta installato il virus, può essere poi attivata o disattivata una singola funzione. Come si vedrà di seguito, il decreto che autorizza l'uso del captatore per l'intercettazione di comunicazioni tra

presenti, deve indicare i luoghi e il tempo. Ciò non vuol dire che andrà disattivato una volta finito il periodo autorizzato, ma resterà "silente" per la successiva attivazione come microfono.

Gli articoli che ne prevedono l'impiego

Ai sensi dell'art. 266 c.p.p. l'intercettazione di conversazioni o comunicazioni telefoniche [c.p.p. 295] e **di altre forme di telecomunicazione** è prevista[1] per i seguenti reati (oltre che per ricercare coloro che sono stati dichiarati latitanti ex art. 295 c.p.p.):
a) **delitti non colposi** per i quali è prevista la pena dell'ergastolo o della **reclusione superiore nel massimo a cinque anni** determinata a norma dell'articolo 4[2];
b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'articolo 4;
c) delitti concernenti sostanze stupefacenti o psicotrope;
d) delitti concernenti le armi e le sostanze esplosive;
e) delitti di contrabbando;
f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono;
f-bis) delitti previsti dall'articolo 600-ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1 del medesimo codice, nonché dall'art. 609-undecies (4);
f-ter) delitti previsti dagli articoli 444, 473, 474, 515, 516, 517-quater e 633, secondo comma, del codice penale;
f-quater) delitto previsto dall'articolo 612-bis del codice penale;
f-quinquies) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.

Per gli stessi reati è consentita **l'intercettazione di comunicazioni tra presenti**, che può essere eseguita anche mediante l'inserimento di un **captatore informatico** su un dispositivo elettronico portatile.

Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale[3], l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa (*eccezione per i reati 51 commi 3 bis e 3-quater c.p.p., vale a dire i reati di criminalità organizzata, in materia di stupefacenti, contrabbando, terrorismo, etc*[4]) per i quali non vige tale limitazione.
Per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, l'impiego del captatore è previsto anche nei luoghi indicati dall'articolo 614 c.p, previa indicazione delle ragioni che ne giustificano l'utilizzo[5].
Ai sensi dell'art. 267 c.p.p. Il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dall'art. 266. L'autorizzazione è data con decreto motivato quando vi sono **gravi indizi di reato e l'intercettazione è assolutamente indispensabile** ai fini della **prosecuzione** delle indagini. **Il decreto** che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le specifiche 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, e dai delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4, (quindi per reati c.d. comuni) **i luoghi e il tempo, anche indirettamente determinati**, in relazione ai quali è consentita l'attivazione del microfono.

Qui c'è la sostanziale differenza, il decreto del GIP, e quindi la richiesta della P.G. e del P.M. devono contenere l'indicazione dei luoghi e del periodo per i quali si richiede l'attivazione del captatore informatico per procedere ad un'intercettazione tra presenti.
La necessità di indicare i luoghi e il tempo rende la norma di non agevole applicazione sia per la mancanza di parametri oggettivi sia per le difficoltà di poter indicare preventivamente dove e quando si eseguirà, seppure il testo della riforma, consapevole di tali difficoltà, abbia preveduto che l'indicazione "*dei luoghi e del tempo*" possa avvenire "*anche indirettamente*".

La determinazione di luogo e tempo

Ma cosa si intende per "anche indirettamente determinati"?
Facciamo un passo indietro. La P.G. può richiedere l'autorizzazione all'utilizzo del captatore informatico per i procedimenti iscritti dopo il 31 agosto 2020 per i reati per i quali siano consentite le intercettazioni telefoniche, quindi quelli del 266 c.p.p. prima richiamati. Quando si tratta di reati comuni, sarà inoltre necessario dimostrare che tale strumento sia indispensabile ai fini della prosecuzione delle indagini e indicare i luoghi e il tempo della richiesta, ovvero dove e quando si ritiene possa svolgersi l'attività criminosa. Ma come fa la P.G. a poter indicare tali elementi? Tipicamente o mediante un'attività di osservazione e pedinamento, dalla quale si evinca lo svolgimento del reato, ovvero mediante l'apprensione della notizia di dove e quando potrebbero incontrarsi i protagonisti, tipicamente se emerge dalle normali intercettazioni o altre fonti. In altre parole, se si danno appuntamento. L'elemento di criticità rimane il fattore tempo, ovvero quello necessario a preparare una richiesta per il

P.M., che dovrà poi eventualmente fare sua e mandare al G.I.P., che dovrà poi valutarla (per i reati comuni non può procedere il P.M. in via d'urgenza). Una volta eventualmente approvata bisognerà procedere con la fase dell'inoculazione del virus, se si tratta della prima attivazione. Questo rende tale strumento di complessa applicazione, tenuto conto che dall'apprensione della notizia di un appuntamento o dell'osservazione dello stesso potrebbe passare un lasso di tempo molto ristretto, non sufficiente a ottenere il decreto e procedere con la parte tecnica.
L'esempio classico potrebbe essere quello di una conversazione telefonica captata al mattino in cui i sodali si danno appuntamento ad una data ora per incontrarsi in un ufficio o in un ristorante. In tal caso luogo e tempo sarebbero perfettamente determinati ma bisognerebbe "correre" per farsi rilasciare il decreto in tempo utile.
E se invece l'appuntamento fosse del tipo "ci vediamo stasera a cena solito posto"? In tale caso luogo e tempo sarebbero determinati indirettamente, ben potendo indicare nella richiesta di poter attivare il captatore in una fascia oraria tipica per la cena e nel luogo ove si incontreranno per cenare. Così come, avuta notizia di un viaggio in auto, ben si potrebbe indicare come luogo l'automezzo che verrà impiegato (anche se non noto, in tale caso verrebbe determinato indirettamente quale "quello che verrà utilizzato) e come tempo quello impiegato per fare il viaggio, nell'ipotesi in cui si possa presumere che durante il viaggio pianifichino il reato in commissione.
Resta pacifico che la difficoltà maggiore sarà la prima attivazione, perché sarà necessario "convincere" l'indagato a installare il virus, ma sono aspetti tecnici-professionali che esulano dall'argomento in trattazione ed è bene restino appannaggio degli operatori.
E' bene ricordare che in ogni caso, i risultati delle intercettazioni ottenute mediante captatore sono utilizzabili soltanto per i reati per i quali è intervenuta l'autorizzazione e non per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.
Altro elemento di sicuro interesse è che il virus, dopo l'inoculazione può rimanere silente e venire attivato come captatore solo al momento del bisogno, previa emissione del decreto del G.I.P.. Il non dover procedere ad una nuova inoculazione per ogni attivazione consente un innegabile risparmio di tempo ed evita inutili rischi che l'indagato si "mangi la foglia".

Il decreto autorizzativo dovrà pertanto menzionare:
- l'indispensabilità dello strumento e l'impiego (ad esempio captare le conversazioni durante un incontro programmato);
- che il reato per cui si procede rientra tra quelli di cui all'art. 266 c.p.p.;
- i luoghi e il tempo per il quale si autorizza la captazione.

Le possibili criticità

• l'art. 270 prevede che si possa installare il captatore su dispositivi elettronici **portatili**. Questo elemento è sicuramente limitativo, escludendo l'ammissibilità dell'utilizzo degli elementi di prova acquisiti su dispositivi fissi o comunque costringere giudici e giurisprudenza a forzare l'utilizzo anche in questi casi;
• con gli apparati dotati di cifratura, si pensi ai telefoni encrochat, ai telefoni cifrati BQ Acquaris[6], il captatore informatico risulta insoddisfacente, rendendosi necessarie nuove tecniche di hacking. Sarebbe stato pertanto opportuno in previsione futura inserire nell'articolo la locuzione "attività di captazione informatica" così da offrire copertura alle future tecniche investigative; ■

**** Ten.Col. della Guardia di Finanza***

1 - Art. 103 c.p.p. Non è consentita l'intercettazione relativa a conversazioni o comunicazioni dei difensori, degli investigatori privati autorizzati e incaricati in relazione al procedimento, dei consulenti tecnici e loro ausiliari, né a quelle tra i medesimi e le persone da loro assistite
2 - Per determinare la competenza si ha riguardo alla pena stabilita dalla legge per ciascun reato consumato o tentato. Non si tiene conto della continuazione, della recidiva e delle circostanze del reato, fatta eccezione delle circostanze aggravanti per le quali la legge stabilisce una pena di specie diversa da quella ordinaria del reato e di quelle ad effetto speciale
3 - abitazione altrui o altro luogo di privata dimora o nelle appartenenze di essi
4 - delitti, consumati o tentati, di cui agli articoli 416, sesto e settimo comma, 416, realizzato allo scopo di commettere taluno dei delitti di cui all'articolo 12, commi 1, 3 e 3-ter, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 600, 601, 602, 416-bis, 416-ter, 452-quaterdecies e 630 del codice penale, nonchè delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'articolo 74 del testo unico approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, dall'articolo 291-quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43 e delitti consumati o tentati con finalità di terrorismo
5 - Prima della modifica del D.L. n. 161/2019 invece i delitti dei p.u. o incaricati di p.s. contro la P.A. sottostavano alle stesse regole dei delitti ex 51 comma 3 bis e 3 quater.
6 - Vengono volutamente citate solo tecnologie già superate;