di Lorenzo Savastano*

Ulisse entra nel Castello: l'impiego dei Trojan horse nei reati contro la Pubblica Amministrazione

Dallo scorso 31 gennaio, la Legge n. 3/2019 consente l'impiego di captatori informatici, già sperimentati con successo nell'ambito della lotta al crimine organizzato, nel contrasto ai reati commessi da pubblici ufficiali nell'esercizio delle proprie funzioni. Uno strumento investigativo che,tuttavia, per dispiegare efficacemente i decisivi effetti procedurali di cui è capace, necessita di essere contestualizzato e coordinato con la novellata e potenziata disciplina delle intercettazioni ambientali

1. Nuove armi contro la corruzione

La possibilità dell'impiego dello strumento dei cd. *captatori informatici* nel contrasto ai reati contro la Pubblica Amministrazione commessi da pubblici ufficiali[1], introdotta dalla Legge n. 3/2019[2] è il portato di una consapevolezza crescente acquisita dall'ordinamento giuridico nazionale sia dell'efficacia di tale pool investigativo sia – parallelamente – della perniciosità e dell'enorme costo sociale che i delitti di tal genere comportano[3].

Una presa di coscienza che, come tradizionalmente accade nella storia legislativa italiana, prende l'abbrivio dalla giurisprudenza di legittimità (in particolare dalla Sentenza della Corte di Cassazione, Sezioni Unite, n. 26889/2016, cd. *Scurato*, di cui in avanti si fornirà rassegna), per poi trovare consacrazione in una serie di profonde modifiche normative apportate alla disciplina codicistica delle intercettazioni *ambientali* dalla cd. riforma Orlando (i.e. D. Lgs. 216/2017[4]). Un tessuto normativo in cui, infine, il legislatore della riforma di gennaio ha potuto agevolmente collocare le disposizioni volte ad utilizzare i *trojan horse* nei reati corruttivi e di malversazione commessi dai pubblici ufficiali nell'esercizio delle proprie funzioni, mediante, come vedremo, la parificazione giuridica della citata categoria di reati ai delitti di criminalità organizzata, non necessariamente di matrice mafiosa, o caratterizzati dalla finalità di terrorismo, rimessi alla competenza esclusiva delle Procure distrettuali.

Una scelta normativa che, proceduralmente, riverbera i propri effetti non solo sulla tipologia di motivazioni necessarie per l'autorizzazione dello strumento delle intercettazioni mediante *captatore informatico*, ma soprattutto sulle concrete modalità di svolgimento e selezione dei luoghi in cui le stesse possono attivarsi.

2. La definizione di captatore informatico

Preliminarmente occorre precisare che un *captatore informatico* (comunemente noto come *"trojan horse"*) identifica *"una categoria di malware le cui funzionalità sono nascoste all'interno di un software apparentemente legittimo facendo sì che l'installazione avvenga in modo inconsapevole da parte dell'utente permettendo in questo modo il controllo da remoto del computer"*[5]. Più laicamente, un *Trojan* è definibile come un programma informatico installato su un dispositivo target (come un *notebook*, un *tablet* o uno *smartphone*), a distanza ed in modo occulto, mediante il suo invio con una mail, un sms o un'applicazione di aggiornamento.

Rifuggendo gli aspetti più squisitamente tecnici del fun-

zionamento, il *software* in commento è costituito da due moduli principali: il server, ovvero un programma di piccole dimensioni che infetta il dispositivo *target, "bucandone"* il sistema di sicurezza informatica; ed il *client*, ossia l'applicativo che il *virus* utilizza per il controllo remoto di detto dispositivo. Uno strumento tecnologico di questo tipo, permette lo svolgimento di varie attività investigative, fra cui, a titolo esemplificativo, la captazione di tutto il traffico dati in arrivo o in partenza dal dispositivo *infettato* (e.g. navigazione internet e/o posta elettronica), attivazione del microfono o della *webcam*, con conseguente possibilità di intercettare i colloqui o carpire immagini nello spazio circostante il soggetto latore del dispositivo *bersagliato*. Non solo, l'impiego di un *captatore* consente altresì l'effettuazione di vere e proprie perquisizioni dell'*hard disk* e di fare copia (totale e parziale) delle unità di memoria del sistema informatico target o di decifrare ogni comunicazione digitata sulla tastiera (in funzione di *keylogger*) e/o di visualizzare ciò che appare sullo schermo (*screenshot*) collegato al sistema.

3. I principi ed il *background* della Sentenza Scurato

Il percorso che condotto all'ammissibilità dell'impiego dei *captatori informatici* nelle investigazioni di polizia – e la conseguente utilizzabilità delle fonti di prova così ottenute all'interno dei relativi procedimenti penali – si innesta concettualmente nelle maglie esegetiche della Sentenza della Corte di Cassazione, riunita a Sezioni Unite, n. 26889/2016 (anche nota come Sentenza *Scurato*), in cui gli ermellini – interrogati sulla validità delle fonti prova raccolte mediante tali strumenti – affermarono due cardinali *principi di diritto, scilicet*:

- *"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 (ad es., personal computer, tablet, smartphone, ecc.) – anche nei luoghi di privata dimora ex articolo 614 codice penale, pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa"*. Tuttavia, nel rispetto dei canoni di proporzione e ragionevolezza, a fronte della forza intrusiva del mezzo impiegato, la Suprema Corte evidenziava come occorresse – nel caso concreto – che la qualificazione del fatto come inquadrabile in un contesto di criminalità organizzata, fosse ancorata a "*sufficienti, sicuri ed obiettivi elementi indiziari*" (*cfr*. punto n. 11 della Sentenza "Scurato"), non potendosi degenerare in un uso meramente esplorativo dello strumento in parola;

- *"Per reati di criminalità organizzata devono intendersi non solo quelli elencati nell'articolo 51, commi 3-bis e 3-quater, codice di procedura penale, ma anche quelli comunque facenti capo a un'associazione per delinquere, ex articolo 416 codice penale, correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato"* (*cfr*. punto n. 16 della Sentenza "Scurato").

L'intervento della Suprema Corte, dunque, apriva esplicitamente all'impiego dei *Trojan horse* a scopi investigativi (e dunque alla piena utilizzabilità probatoria degli elementi in tal modo acquisiti), seppur limitatamente a delitti ascrivibili a fenomeni di criminalità organizzata, tassonomia a cui veniva comunque fornita una definizione ampia e non circoscritta a soli ambienti mafiosi.

4. Le modifiche alla disciplina delle intercettazioni del 2017

I principi giurisprudenziali elaborati dalla richiamata Sentenza *Scurato* hanno trovato un primo importante riconoscimento normativo con la cd. riforma Orlando, in cui si è agito sul cuore della disciplina codicistica delle intercettazioni *ambientali* (al cui *genus* appartengono le captazioni in commento), sancendo la piena possibilità del ricorso ai cd. *agenti intrusori* informatici su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale (ovvero nei luoghi di privata dimora), l'intercettazione è consentita solo se *vi è fondato motivo* di ritenere che ivi si stia svolgendo l'attività criminosa. A corredo di tale facoltà, inoltre, sì la riforma del 2017 ha chiarito 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"*, ovvero a tutte le fattispecie criminose avocate alla competenza del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente (cd. Direzione Distrettuale Antimafia, D.D.A.), caratterizzate dalla presenza di un sodalizio criminale (art. 416 c.p.), anche di stampo mafioso (416 bis c.p.), o dalla finalità di terrorismo[6]. In tali casi, pertanto, l'impiego del *trojan* potrà avvenire anche nei luoghi di privata dimora e senza l'esplicitazione – nelle motivazioni del decreto – del fondato motivo di ritenere ivi sia *in fieri* l'attività delittuosa;
- è obbligatoria l'indicazione specifica nel decreto autorizzativo delle ragioni che rendono necessario l'uso del *captatore*. Il decreto deve inoltre includere, quando autorizza intercettazioni collegate a delitti non compresi nell'elenco dei commi 3-*bis* e 3-*quater* dell'articolo 51 c.p.p., i luoghi e il tempo in cui è consentita la captazione dei segnali vocali mediante l'attivazione del microfono (nuovo primo comma dell'articolo 267 c.p.p.);
- nei casi d'urgenza, in cui è il pubblico ministero ad autorizzare interinalmente le intercettazioni tra presenti, può essere disposta l'intercettazione mediante l'inserimento di un captatore su un dispositivo elettronico portatile, ma solo nei procedimenti per i delitti di competenza della Procura distrettuale, imponendo al contempo al PM una motivazione aggravata che dia conto dell'impossibilità di procedere per le vie ordinarie (nuovo comma 2-bis dell'art. 267 c.p.p.)[7].

In merito, poi, alla decisiva questione dell'utilizzabilità processuale dei dati captati dal *Trojan horse*, la riforma Orlando ha escluso l'utilizzabilità a fini di prova dei risultati delle intercettazioni per reati diversi da quelli cui si riferisce il decreto autorizzativo, fatta eccezione per il caso in cui siano indispensabili per l'accertamento di delitti per i quali sia obbligatorio l'arresto in flagranza

(nuovo comma 1 *bis* dell'articolo 270 c.p.p.). Inoltre, il nuovo comma 1-*bis* dell'articolo 271 ha sancito l'inutilizzabilità dei dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore nel dispositivo target e di ogni altro dato acquisito oltre i limiti di luogo e di tempo fissati nel decreto autorizzativo.
Da un punto di vista marcatamente operativo, infine, il nuovo testo dell'articolo 89 c.p.p. prevede che, in caso di uso del captatore informatico, il verbale delle operazioni indichi il tipo di programma impiegato (conforme ai requisiti tecnici stabiliti con decreto del Ministro della Giustizia) e i luoghi in cui si svolgono le comunicazioni e conversazioni. A tal fine, il nuovo comma 3-bis dell'art. 268 del c.p.p., dispone che "*per le operazioni di avvio e di cessazione delle registrazioni con captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti*", l'ufficiale di polizia giudiziaria possa avvalersi di idonei ausiliari di polizia giudiziaria (ovvero fornitori privati di servizi di computer forensic) di cui all'articolo 348, comma 4 del c.p.p..

5. I captatori nel contrasto ai reati contro la Pubblica Amministrazione

Sull'impalcatura procedurale disegnata dalla riforma del 2017, la nuova Legge n. 3/2019 (recante: "*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 movimenti politici*"), interviene significativamente sull'impiego di captatori informatici nel contrasto ai delitti compiuti da pubblici ufficiali contro la Pubblica Amministrazione. La potenza della novella normativa è apprezzabile, in particolare nell'ampliamento dei casi in cui è sempre consentito ricorrere alle intercettazioni ambientali mediante l'utilizzo di *captatori informatici*, inclusi cioè i luoghi di abituale dimora e senza necessità di specificare il *fondato motivo* di ritenere che "*ivi si stia svolgendo l'attività criminosa*". La cd. Legge Spazza-corrotti affianca, difatti, alle ipotesi precedentemente analizzate (afferenti fenomeni di criminalità organizzata), anche "*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*" (nuovo ultimo periodo del comma 2-*bis* dell'art. 266 c.p.p.)[8].

Specularmente, è stata aggiunta in seno al primo comma del richiamato art. 267 c.p.p., la precisazione che nel decreto che autorizza l'intercettazione tra presenti mediante inserimento di *captatore informatico* su dispositivo elettronico portatile, indicante le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini, non occorra la specificazione dei luoghi ed il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono, qualora si proceda non solo per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*, ma 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*". In tal modo, come agevolmente inferibile, lo stigma normativo alle condotte illecite dei pubblici ufficiali si è realizzato mediante la parificazione di queste ai reati rimessi alla competenza della D.D.A., ovvero ai delitti di criminalità organizzata, anche quelli non connotati dalla cd. aggravante mafiosa, o caratterizzati dalla finalità di terrorismo.

6. Lo stratagemma del Cavallo nel Castello

Il celebre episodio del *Cavallo di Troia,* escogitato dai guerrieri achei capeggiati da Agamennone per espugnare – dopo un conflitto decennale – la leggendaria città di Priamo, è una facile ma fascinosa metafora a cui abbiamo voluto cedere nel titolo del presente contributo. La lotta ai comportamenti illeciti attuati dai pubblici ufficiali contro i principi di lignaggio costituzionale di imparzialità e buon andamento della Pubblica Amministrazione, tuttavia, è una battaglia che riporta ad atmosfere meno epiche e ben più tetre. Una gestione scellerata ed infedele della *Cosa Pubblica*, rievoca – difatti – le ambientazioni tormentate e cupe del *Castello* immaginato dallo scrittore praghese Franz Kafka, simbolo di uno Stato iper-burocratizzato, inutilmente complicato e piegato agli interessi particolari dei propri funzionari corrotti. Piace, allora, credere che la neo-riforma abbia voluto mettere nelle mani delle forze di polizia uno strumento potente ed astuto per introdursi nei palazzi pubblici ed estirparne il germe della corruzione qualora esso si presenti. Consentendo ad Ulisse non solo di infiltrarsi in una roccaforte a protezione della collettività, ma soprattutto di vincere, - anche stavolta - una decisiva guerra di civiltà. ■

Capitano della Guardia di Finanza,

1- Disciplina racchiusa all'interno del Capo I, Libro II, Titolo II del Codice Penale (rubricato: "Dei delitti contro la Pubblica Amministrazione").
2 - Recante: "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 movimenti politici".
3 - Per un approfondimento sulla tematica in oggetto, si rinvia a: V. GIGLIO, I captatori informatici a tre anni di distanza dalla sentenza Scurato delle Sezioni unite penali, in Filodiritto – Rivista giuridica telematica (www.filodiritto.it) del 24 aprile 2019; G. MERLO, L'invasione dei Trojan – i file "malevoli" amati dalle procure, in Il Dubbio del 23 aprile 2019; M. BONTEMPELLI, Il captatore informatico in attesa della riforma, in Diritto Penale Contemporaneo (www.dirittopenalecontemporaneo.it) del 20 dicembre 2018.
4 - Attuativo della Legge di delega nr. 103/2017.
5 - Definizione attinta dal sito ufficiale del CERT Nazionale Italia (www.certnazionale.it).
6 - Vedasi il nuovo comma 2 bis dell'articolo 266 c.p.p..
7 - Sul punto: V. GIGLIO, op. cit..
8 - Si veda l'art. 1, comma 4 della Legge n. 3/2019.