diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Trojan horse e limiti dell'intercettazione ambientale

Autore: armando mele
In: Diritto penale

I dubbi della sentenza Musumeci, il compromesso della sentenza Scurato, la disciplina minimalista della legge Orlando.

Il captatore informatico: aspetti tecnici e giuridici

Il 3 agosto 2017 è entrata in vigore la **legge 103/2017**, che ha apportato modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario. La **riforma Orlando** ha previsto l'introduzione di novità sia processuali che sostanziali ed ha regolamentato l'ingresso ufficiale nel nostro ordinamento giuridico – come nuovo strumento d'indagine - del c.d. **captatore informatico**.

I captatori – nel linguaggio degli informatici – sono dei **virus che conquistano i diritti di amministrazione del device in cui vengono inseriti assumendone il controllo totale**. La novella legislativa sembra aver inteso il "**trojan**" come un mero strumento di intercettazione – una sorta di cimice supertecnologica – senza però considerare il suo potenziale praticamente illimitato. Il **captatore informatico** infatti, bypassando la vulnerabilità degli antivirus, **entra direttamente nel sistema "target**" diventando il dominus del device. Esso è in grado, a discrezione dell'utilizzatore, di accendere la webcam, di attivare il microfono e di captare conversazioni VoIp (Voice over Internet Protocol) così da eludere le cifrature dei linguaggi di determinati software (su tutti Skype) comportandosi come un intercettatore ambientale, di leggere qualsiasi dato venga archiviato all'interno del cellulare (dagli indirizzi in rubrica, agli sms, ai messaggi whatsupp, agli appunti salvati nelle note), di visualizzare le fotografie, di registrare la "tracciabilità" del possessore del cellulare funzionando da GPS, di fungere da key logger, ovvero di catturare segretamente tutto ciò che viene digitato nel dispositivo, potendo quindi risalire anche ad eventuali password o numeri di carte di credito. Con il "trojan" è inoltre possibile riversare sul dispositivo dell'investigatore l'intero contenuto del device in cui viene inoculato (anche gli screen shot dei siti web che vengono visitati) potendo inoltre "uploadare" ogni tipo di file sullo stesso dispositivo che lo ospita[1].

Basta un click per distruggerlo, senza che sia in alcun modo possibile rinvenire sue eventuali tracce, ed è improbabile che possa essere scoperto da anti - spyware dato che la sua presenza si maschera: è completamente assente sia nella lista dei processi attivi così come nelle connessioni attive[2].

Siamo dunque in presenza di un **software dalle potenzialità sterminate** in grado, se utilizzato dai

privati, di inoculare ransomwere, e capace, se utilizzato dall'Autorità Giudiziaria, di mettere a nudo e di scoprire praticamente tutto del "bersaglio infettato".

Il "**virus di Stato**", nelle sue infinite implicazioni applicative, non sembra trovare asilo in nessuna delle categorie probatorie del codice del 1988 e arduo compito del giurista risulta quello di sollevare dubbi ed eccezioni o di legittimarne le attività degli investigatori che, sotto la pressione delle Procure, all'interno di queste zone franche, sanno di poterne fare uso in maniera incontrollata ai fini immediati delle determinazioni conclusive delle indagini o delle misure cautelari, seppur consapevoli di non poterle poi usare al processo. Il tutto al cospetto di tutele che il processo penale richiede ma che sembrerebbero non essere state affatto prese in considerazione[3].

Di fronte a tale incalcolabile intrusività del "cavallo di Troia" siamo sicuri che l'**equilibrio tra le esigenze investigative e il diritto alla riservatezza** sia stato rispettato o che forse, nonostante gli interventi giurisprudenziali nonché l'ultima novella legislativa, urga un ulteriore bilanciamento?

Intercettazione ambientale: i dilemmi della sentenza Musumeci e raccordo di congiunzione con la sentenza Prisco

Il provvedimento giurisprudenziale che offre i primi e maggiori spunti di riflessione sul tema, inquadrando la criticità della disciplina, è certamente la **sentenza Musumeci** (Cass. Sez. 6, n. 27100 del 26/05/2015) con la quale la Suprema Corte, in un processo di mafia, ha proclamato la **inutilizzabilità delle intercettazioni captate tramite trojan** in considerazione del fatto che, nel caso in esame, il decreto del Giudice per le Indagini Preliminari non aveva, derogando l'art. 266 co II c.p.p., precisamente indicato il luogo nel quale si autorizzava la registrazione di conversazioni tra presenti[1]; generando un eccesso di surveillance capace di seguire il soggetto in qualunque luogo esso si fosse trovato con una evidente violazione della libertà e della segretezza delle comunicazioni[2]. Con la sentenza Musumeci sono stati per la prima volta introdotti dei dubbi sull'utilizzo del trojan che, a ben vedere, è apparso subito non come una semplice intercettazione di comunicazione tra presenti ex art. 266 co II c.p.p. ma come un'autentica intercettazione itinerante capace di seguire l'intercettato in ogni luogo[3]. Si è così iniziato ad intravedere, dunque, la necessità di una specificazione della localizzazione o comunque di una precisazione della portata nell'utilizzo di tale strumento che, se non in considerazione di reati appartenenti al binario parallelo nel processo penale che è quello inerente la criminalità organizzata, apparve di portata assolutamente straripante per i reati comuni. La stessa sentenza, inoltre, riaffrontando la questione concernente l'attivazione, da remoto, della telecamera del telefono cellulare e quindi l'effettuazione di videoriprese, confermava inevitabilmente le stesse opinioni già espresse con la sentenza Prisco (Sez. U. 28-3-2006, n. 26795).

In suddetto provvedimento, le Sezioni Unite avevano in particolare affermato che videoregistrazioni in luoghi pubblici o aperti o esposti al pubblico, non realizzate nel corso di un procedimento penale,

Diritto & Diritti ISSN 1127-8579

andassero incluse nella categoria probatoria dei documenti ex art. 234 c.p.p. Tali captazioni, però, se effettuate da organi di Polizia Giudiziaria, anche di spontanea iniziativa, diventano automaticamente assoggettate alla disciplina ex art. 189 c.p.p. delle prove atipiche, in quanto non assimilabili nel genus delle intercettazioni di comunicazioni e di captazioni. In buona sostanza, tale Corte affermò che le videoregistrazioni di comportamenti non comunicativi realizzate in un domicilio privato, rappresentando prove atipiche, risultavano proibite in quanto acquisite in contrasto all'art. 14 Cost; se, però, le intercettazioni avevano ad oggetto comportamenti comunicativi, anche se in luoghi di privata dimora, risultavano ammesse in quanto assimilabili, per via interpretativa, alle intercettazioni ambientali ex art. 266, co. 2, c.p.p.

La famosa **sentenza Prisco**, sulla base delle predette considerazioni, si era tra l'altro soffermata anche sul caso in cui la videoregistrazione fosse avvenuta in un luogo che seppur utilizzato per attività riservate e private, non rientrava nel concetto di domicilio come, ad esempio, le riprese effettuate dalla polizia giudiziaria in un bagno pubblico. In dottrina si è affermato che tali spazi vanno considerati come "luoghi riservati caratterizzati dalla mancanza della stabilità di escludere chiunque altro" dato che tale diritto persiste solo se il titolare è presente sul luogo (privè di una discoteca..)[4]. Si tratta di ambienti che, seppur non potendo rientrare nella stessa categoria del domicilio privato, si caratterizzano per una aspettativa di riservatezza che è sicuramente superiore a quella prevista nei luoghi pubblici. Da ciò si è desunto che i luoghi riservati, nonostante le differenze rispetto ai domicili privati, non presentano, esclusivamente dal punto di vista dei presupposti giustificativi e dei requisiti specifici del decreto autorizzativo, che entrambi richiedono, modifiche apprezzabili e quindi in tali luoghi una eventuale limitazione va consentita anche in assenza di una espressa disciplina legislativa, purché, però, vi sia un provvedimento dell'autorità giudiziaria, fornito di congrua motivazione[5].

Data l'esauriente e precisa esposizione delle Sezioni Unite, il tema delle videoregistrazioni non è apparso, ad oggi, bisognevole di un'integrazione né giurisprudenziale né legislativa anche se, a ben vedere, persistono ancora dubbi sulla questione dei comportamenti comunicativi[6] la cui natura, ad ogni modo, può essere considerata solo ed esclusivamente dopo la visualizzazione.

L'elaborazione delle Sezioni Unite nella sentenza Scurato

Considerando la delicatezza dell'argomento, nonostante non vi siano invero state numerose pronunce sul punto, la questione delle **intercettazioni ambientali tramite trojan** è stata ben presto rimessa alla valutazione delle **Sezioni Unite** che, con una soluzione di prudente saggezza, hanno elaborato una risposta non esaustiva ma di intelligente compromesso.

Con la **sentenza n. 26889/2016** (Pres. Canzio, Rel. Romis) è stato sostanzialmente affermato che l'**utilizzo del trojan è inammissibile**, **salvo che nei procedimenti per delitti di criminalità organizzata**. La meglio conosciuta **sentenza Scurato** (dal nome del ricorrente) – facendo leva sull'idea

Diritto & Diritti ISSN 1127-8579

del doppio binario del processo penale e bypassando alcune garanzie del domicilio - ha reso **legittimo l'utilizzo del captatore informatico in tutti i procedimenti per reati in forma associata** escludendo, in buona sostanza, il semplice concorso di persone nel reato. Al contempo, è stato vietato l'utilizzo del mezzo per reati differenti in quanto, non essendo possibile prevedere i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto, verrebbero travalicate le garanzie della condizione di legittimità richiesta ex art 266, comma II, c.p.p. Da una parte, dunque, si è rimarcata l'esistenza nel nostro processo penale di un "doppio binario" (aspetto evidente nel nostro ordinamento soprattutto in materia di intercettazioni) ma, forse, si è data una definizione fin troppo lata di criminalità organizzata[1] – comprendendo, in pratica, tutte le ipotesi nelle quali vi è la costituzione di un apparato organizzativo, la cui struttura assume un ruolo preminente rispetto al singolo partecipante - e dall'altra, ancora una volta, non sono state considerate le immense potenzialità del "virus di Stato". Basti pensare, ad esempio, che - a prescindere dalla definizione che se ne voglia dare dell'attività - il captatore realizza una vera e propria perquisizione on – line: un'attività che, secondo gli schemi del nostro codice di rito, dovrebbe prevedere una relazione tra l'individuo e l'Autorità (quantomeno garantire la consegna all'interessato del decreto di autorizzazione) ma che la Suprema Corte non ha minimamente considerato.

L'intervento del legislatore

La "toppa" giurisprudenziale necessitava di un **intervento del Legislatore** che, con la **l. 103/2017**, ha dedicato un breve ed insufficiente capitolo alla problematica del "troyano".

La **disciplina minimalista** dettata nella riforma Orlando, nonostante gli sforzi profusi nel decreto attuativo della "delega Orlando" (d.lgs 216/2017), lascia molto insoddisfatti, in quanto il problema sembra essere stato ampiamente sottovalutato.

La **maggior parte delle funzioni del captatore informatico non è stata infatti normata** e si è considerato esclusivamente il suo uso come "cimice". In buona sostanza la novella legislativa ha ritenuto che l'unica funzione utilizzabile del trojan sia quella di attivare il microfono. La legge Orlando, inoltre, ha abbandonato lo schema del "doppio binario" rendendo ammissibile il trojan in qualsiasi procedimento penale. Lo stringente presupposto dell'indicazione del luogo e del tempo delle intercettazioni, non necessario per i reati di criminalità organizzata, è stato infatti superato sulla base della considerazione che il malware è attivabile e disattivabile da remoto[2]. Spetterà dunque **all'Autorità Giudiziaria** il delicato compito (per non dire arduo o quasi impossibile) di non fornire "autorizzazioni in bianco"[3] e di indicare in largo anticipo l'individuazione dei luoghi di attivazione della "cimice" con predeterminata precisazione preventiva del suo spegnimento in celle non autorizzate. La rivoluzione sull'utilizzo del trojan, per giunta, consente, sulla scorta del dettato del 266 co II cpp, anche di invadere l'ambiente domiciliare privato ogni qual volta si ritiene che in esso si stia svolgendo l'attività criminosa oggetto dell'indagine o comunque se si procede per reati previsti ex artt. 51 commi 3 bis e quater c.p.p.

Diritto & Diritti ISSN 1127-8579

Mentre con la sentenza Scurato le Sezioni Unite avevano riservato l'uso del captatore solo per i reati di criminalità organizzata, con la **riforma Orlando il trojan diviene invece utilizzabile per qualsiasi reato e, a determinate condizioni, può introdursi anche nei domicili privati**. Vi è così un abbandono dell'idea del doppio binario del trojan (a differenza di quanto invece non accaduto in altri ordinamenti come la Germania) e una specificazione del concetto di criminalità organizzata che individua – diversamente da quanto non era stato fatto con la Scurato – solo nei reati di competenza distrettuale quelli di maggior apprensione sociale per i quali è possibile attenuare le garanzie ex artt. 267 cpp. Alla stregua di tali ultimi crimini, però, sono inoltre stati considerati anche i reati contro la P.A.: ratio da andare presumibilmente a rintracciare nell'opacità dei suddetti crimini nei quali il rischio di una punizione generale, che coinvolge maggiori concorrenti, crea, proprio come per le associazioni a delinquere, una rigida impenetrabilità nel crimine perforabile solo mediante una forte intrusività.

Perplessita' e rischi

Tralasciando il tema della utilizzazione dei risultati del trojan in altri procedimenti che, comunque, presenta notevoli criticità in merito all'esplicazione del comma I bis dell'art. 270 c.p.p. (non appaiono chiari i limiti di utilizzazione e la connessione con i meri spunti investigativi), e quello della sua disciplina sanzionatoria (sarà davvero realizzata la richiesta normativa della meticolosa individuazione di spazi in cui poter intercettare o ritroveremo mere formule di stile nei decreti autorizzativi? In caso di elencazione precisa degli luoghi, in assenza di file di log che individuino con precisione la localizzazione del trojan, la difesa potrà invece contestare la genuinità delle operazioni?), sembra opportuno specificare che l'inoculazione del "virus di Stato" sarà possibile esclusivamente per i dispositivi elettronici portatili mentre non sarà attuabile l'intercettazione tramite computer "fissi". Ad una prima analisi, data la strana omissione, potremmo immaginare si sia trattata di una semplice "dimenticanza" del Legislatore che, forse suo malgrado, di fronte a un dettato della riforma così chiaro, avrebbe innalzato una specifica barriera difficilmente superabile. Con maggiore attenzione, però, si potrebbe probabilmente convenire che non si sia trattata di una omissione bensì di una valutazione molto cinica: se il malware viene introdotto in un in un computer fisso rispetto alle intercettazioni non cambia molto, se invece il virus viene inoculato in uno smartphone la lesione diventa molto più penetrante e la sorveglianza – considerando che i cellulari sono divenuti appendici del nostro corpo[4] – molto più intrusiva[5].

Altro punto spinoso è certamente anche la previsione ex art. 268 co. III bis la quale prevede che per le operazioni di intercettazione le Procure potranno servirsi di "impianti appartenenti a privati" con l'ausilio di "persone idonee". Una dichiarazione tanto generica quanto pericolosa, considerando che le maggiori aziende italiane che vendono tecnologie di sorveglianza (pensiamo ad Area ed Esitel) sono state indagate per gestione illecita di conversazioni telefoniche. Senza contare, infine, che fra gli hacker è nota la c.d. funzione di "blackdoor" che consente al produttore del software di monitorare le attività dell'utente, ovvero di spiare chi spia. Ovviamente, le aziende produttrici negano l'esistenza di tale funzione ma è facile comprendere verso quali rischi si va incontro.

Diritto & Diritti ISSN 1127-8579

Insomma, la riforma legislativa sembra aver curato solo pochi aspetti che riguardavano vecchi problemi legati all'utilizzo del captatore informatico senza porsi interrogativi – invero ancora troppi - che lasciano perplesso il tecnico informatico e il giurista, concedendo un eccesso di poteri nelle mani delle Procure che, con l'ariete dei "cavalli di Troia", potranno inevitabilmente sfondare molte garanzie dei cittadini i quali paradossalmente, a pochi giorni dall'entrata in vigore del Regolamento sui General Data Protection Regulation, devono sempre più temere una deriva orwelliana.

[1] È parso concreto il rischio che il P.M. potesse configurare come partecipazione ad una associazione per delinquere quella che in realtà era una semplice partecipazione concorsuale godendo, così, del regime più permissivo concesso dalla legislazione speciale (AMATO G., Reati di criminalità organizzata in Guida dir. N. 34-35/2016 p 76 ss.).

[2] Sul punto, però, è stato affermato che un'intercettazione continuativa potrebbe provocare un consumo abnorme della batteria e causare il rischio di essere scoperti (PIO E., Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite, in Parola alla difesa, n. 1/2016, p. 164).

[3] CAMON A., Cavalli di Troia in Cassazione, in Arch. nuova proc. pen. n 1/2017, p. 93.

[4] La Corte Suprema statunitense ha affermato che se un marziano sbarcasse sulla terra e si guardasse attorno, molto probabilmente concluderebbe che il cellulare è una parte del corpo umano (Riley v. California, 13 – 132 and United States v. Wurie 13 – 212, Us Supreme Court, 25.06.2014 in www.supremecourt.gov. pag. 9).

[5] TESTAGUZZA A., Exitus acta probat. "Trojan" di Stato: la composizione di un conflitto, in Arch. Pen. (web), n. 2/2016, p. 6.

[1] "nel decreto del Gip (decreto n.315/2014) non si fa riferimento alla possibilità che il detto strumento venga utilizzato anche all'interno delle private dimore dei soggetti intercettati e, comunque, non vi è alcuna indicazione dei luoghi e dei tempi della predetta captazione" (Cass. Sez. 6, n. 27100/2015).

[2] Cass., Sez. VI, sent. 11 dicembre 2007, dep. 11 aprile 2008, n. 15369, Pres. Lattanzi, Rel. Fidelbo, Imp. Sitzia C.E.D. 239634; Sez. V, sent. 6 ottobre 2011, dep. 15 febbraio 2012, n. 5956, Pres. Marasca, Rel. Oldi, Imp. Ciancitto

[3] Affermava infatti la Corte: "occorre osservare che l'attivazione del microfono dà luogo ad un'intercettazione ambientale, onde occorre interrogarsi sulla legittimità della stessa"; a tale domanda rispondeva che "La norma costituzionale (art. 15 Cost.) pone infatti il fondamentale principio secondo il quale la libertà e la segretezza delle comunicazioni sono inviolabili, ammettendo una limitazione soltanto per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge. Ne deriva che le norme che prevedono la possibilità di intercettare comunicazioni tra presenti sono di stretta interpretazione,

Diritto & Diritti ISSN 1127-8579

ragion per cui non può considerarsi giuridicamente corretto attribuire alla norma codicistica una portata applicativa così ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si sposti. Viceversa, l'unica opzione interpretativa compatibile con il dettato costituzionale è quella secondo la quale l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati ab origine e non in qualunque luogo si trovi il soggetto".

[4] TONINI P., Manuale di procedura penale (Giuffrè, Milano, 2017) pag. 397.

[5] Si veda, Cass. Sez I 10 luglio 2007, Susini.

[6] SCALFATI A., Le indagini atipiche (Giappichelli, Torino, 2014) p. 161 ss.

[1] TORRE M., Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali (Giuffrè, Milano, 2017), p. 25 ss.; ABBAGNALE M.A., In tema di captatore informatico, in Arch. Pen. (web), n. 2/2016, p. 1.

[2] ATERNO, Digital forensics (investigazioni informatiche), in Digesto pen., Agg. VIII (Torino, 2014) p. 217; TORRE M., Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali, in Dir. pen. proc. 2015, p. 1163.

[3] Sul punto CURTOTTI D., Le intercettazioni tra presenti con captatore informatico in Baccari-Bonzano-La Regina-Mancuso, Le recenti riforma in materia penale (Cedam, Padova, 2017) p. 30 ss.

https://www.diritto.it/trojan-horse-limiti-dellintercettazione-ambientale/

Diritto & Diritti ISSN 1127-8579