PREMESSA

Non si può negare quanto l'evoluzione tecnologica abbia influenzato - e continui ad influenzare- il modo di vivere, di comunicare e di interagire nelle relazioni interpersonali. Non è un caso, infatti, se anche le tradizionali forme di manifestazione del crimine si avvalgono sempre più spesso della tecnologia informatica per la commissione dei reati. Se si prende atto di questo, è facile comprendere che non attribuire agli inquirenti strumenti altrettanto sofisticati per la repressione di simili forme di criminalità, significherebbe arrendersi ad un processo penale incapace di accertare i fatti di reato.

Il captatore informatico rappresenta il futuro delle investigazioni, ma allo stesso tempo è una delle "armi" più pericolose presenti sul mercato e come tale, per evitare conseguenze devastanti sul piano della sicurezza informatica, va regolamentato sia a livello nazionale che internazionale.

Le nuove modalità di comunicazione e di interazione, e più in generale il progresso tecnologico che costantemente travolge la materia in esame, rendono necessario un approfondimento critico sull'argomento, rappresentando per la giustizia penale un'opportunità, ma anche un problema.

Il presente elaborato si pone l'obiettivo di ricostruire, a partire dall'avvento fino al suo completo inserimento nel quadro normativo, la complessa vicenda del captatore informatico, e di verificare se gli auspicati interventi del legislatore siano idonei a regolare, nel rispetto dei principi Costituzionali e sovranazionali, l'uso di strumenti che, per quanto siano di notevole ausilio per l'indagine penale, devono fare i conti con la tutela dei diritti fondamentali.

La prospettiva di analisi si snoda su due profili; da un lato sul piano esegetico, si ricostruisce l'evoluzione normativa, e dall'altro, sul piano pragmatico, si analizza come questo strumento sia stato interpretato dalla prassi giudiziaria. Il titolo allude, infatti, alla sempre più costante asimmetria tra norma e prassi, tra il dover essere previsto dal codice e quello che realmente è negli uffici giudiziari quando ci si confronta con l'impiego di strumenti di questo genere, nonché più in generale con il tema delle intercettazioni.

Nonostante sia stato ampiamente impiegato nella pratica, è solo negli ultimi anni che le autorità giudiziarie hanno compreso l'effettiva potenzialità dei captatori informatici, ovvero di *virus* dall'elevata capacità invasiva, che, inoculati nei dispositivi elettronici, permettono lo svolgimento di numerose attività d'indagine. È stato, infatti, l'ampio utilizzo dello strumento nella prassi giudiziaria ad aver spinto, nell'anno 2016, le Sezioni Unite con la Sentenza "Scurato" a prendere posizione. L'intervento della Cassazione, che ha condotto allo "sdoganamento" del "*malware* di Stato", ha rappresentato un passaggio fondamentale nella storia delle intercettazioni. Al legislatore, invece, sembrano essere sfuggite le capacità del *trojan* almeno fino al 2017, quando introduce formalmente il captatore informatico nel codice con la Riforma Orlando.

La ricerca è condotta adottando un metodo di tipo logico- razionale; la struttura segue un ordine cronologico, finalizzato ad evidenziare i diversi passaggi che hanno portato alla definizione normativa del *trojan*. Pertanto, dopo che il tema sarà stato introdotto, si passerà all'analisi dei principali interventi giurisprudenziali in materia per poi focalizzarsi su quello che rappresenta il nucleo centrale della tesi.

L'elaborato è articolato in tre capitoli. Il primo capitolo - che ha la funzione di introdurre il tema - dopo aver affrontato la definizione di captatore informatico ed evidenziato le sue potenzialità, procede ad una ricostruzione, seppure breve, della disciplina generale delle intercettazioni. Nel ricostruire, anche storicamente, l'utilizzo del captatore informatico, si dà atto dell'ampia diffusione che questo strumento ha avuto nella prassi giudiziaria – che a sua volta spiega l'intervento delle Sezioni Unite Scurato - e dei problemi applicativi che ne scaturiscono.

Il secondo capitolo – ovvero il corpo della tesi – passa in rassegna i diversi interventi normativi che, dopo anni di tentativi falliti, si sono susseguiti sul tema delle intercettazioni tramite *trojan*, oggi al centro del dibattito politico. Partendo dalla riforma Orlando, l'attenzione viene riposta sulle principali novità del d.lgs. 216/2017. Seguiranno poi i riferimenti alle più recenti riforme in materia.

Il terzo – ed ultimo - capitolo si sofferma su come gli altri Paesi si siano confrontati con questo "genio informatico". La comparazione giuridica in più sistemi permette da un lato di comprendere più profondamente le regole di diritto

proprie del singolo ordinamento giuridico, e dall'altro di scoprire se e come i diversi sistemi si siano vicendevolmente influenzati.

CAPITOLO PRIMO

LE AVANGUARDIE TECNOLOGICHE NEL PROCESSO PENALE: IL CAPTATORE INFORMATICO

1. ALLA RICERCA DI UNA DEFINIZIONE: IL CAPTATORE INFORMATICO

Per captatore informatico[1] si intende un *software* (o, più correttamente, un *malware*[2]) che, in maniera occulta, si infiltra in dispositivi informatici come *smartphone*, *tablet* e *personal computer*, e con comandi attivati da remoto[3], esporta i dati ivi contenuti[4]. Non è un caso se suddetto strumento è definito anche "*virus trojan*" o "*trojan horse*"; la denominazione, infatti, prende il nome dal mito greco del cavallo di Troia, al quale è assimilato per la caratteristica di servirsi di un *escamotage* per celare le reali intenzioni. Così come il cavallo di Troia, grazie all'ingegno di Ulisse, riuscì ad entrare dentro le mura di Troia e, con l'inganno, ad

[1] Termine talvolta sostituito con le varianti "virus informatico", "virus *trojan*", "captatore informatico", "agente intrusore", "virus di Stato" o con la definizione più minuziosa di "agente intrusore informatico".

[2] "Il termine *malware* è il risultato di una crasi tra i termini *malicious* (malevolo) e *software* (programma) e identifica una categoria di programmi che, per esemplificazione, potremmo definire come *software* dannoso. All'interno della macro categoria in esame esistono diversi sottoinsiemi fra cui virus, worm e *trojan* che, spesso, vengono erroneamente utilizzati come sinonimi, sebbene identifichino tipologie di *malware* con distinti meccanismi di funzionamento" Cfr. F. DITARANTO, R. RUGGIERI, V. CUPELLI, *Nuove tecniche di investigazione nell'era digitale: il "malware di Stato*", in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 2017, vol.18, n.57, pp.113-169.

[3] "ll *trojan* horse utilizza una tecnica informatica conosciuta come *Remote Control System* (RCS), la quale – come si evince dalla definizione – permette un controllo totale da remoto del sistema infettato, consentendo così agli investigatori di acquisire un ampio materiale conoscitivo, potenzialmente consistente in ogni atto quotidiano della vita di un soggetto" Cfr. O.CALAVITA *L'Odissea del Trojan Horse. Tra potenzialità tecniche e lacune normative*, in *Riv. dir. pen. contemp*., 2018, 11, p.48.

[4] Cfr. W. NOCERINO, *Il captatore informatico: un Giano bifronte. Prassi operative vs risvolti giuridici*, in *Cass. pen*., 2020, n.2, p.824

espugnarla; allo stesso modo il predetto *virus* riesce ad entrare, all'insaputa dell'utente, nell'apparecchio che si vuole intercettare ed ad acquisire qualsiasi dato vi trovi[5].

Non tutti i captatori informatici hanno la stessa capacità "intrusiva": si possono trovare *software* che a modico prezzo danno la possibilità a chiunque, quali genitori o *partner*, di accedere all'altrui dispositivo per sottrarne le informazioni, ma esistono anche *software* estremamente avanzati il cui impiego è consentito solo alle Forze dell'ordine e ai Governi. Il *software* del captatore informatico si compone di due elementi principali; vi è infatti un *server* che infetta il dispositivo bersaglio,e un *client*, costituito dall'applicativo che il *virus* usa per monitorarlo occultamente[6]. Sul dispositivo target, che verrà controllato da remoto, è istallato un modulo *software* di tipo *server*, in grado di ricevere e di eseguire istruzioni specifiche eseguite dal *client*, ovvero un calcolatore dotato del modulo *software* per l'invio dei comandi al server e la ricezione delle risposte da quest'ultimo. Il programma *client* (*controller*) è in grado di far eseguire al dispositivo controllato qualsiasi operazione[7].

L'operazione di "innesto" avviene attraverso l'istallazione di un *trojan* nel dispositivo bersaglio.

Il *malware* può essere inoculato sia fisicamente, attraverso l'inserimento di un supporto rimovibile (ad esempio una *pen drive* USB[8]); sia virtualmente, attraverso l'invio telematico di un codice infetto[9].

Non è possibile stabilire *sic et simpliciter* quale tra le due modalità sia preferibile rispetto all'altra, piuttosto la scelta va effettuata tenendo conto delle circostanze del caso in questione. Istallare fisicamente il *malware* è un'operazione sicuramente più economica ed efficace, ma questa strada non è percorribile

---

[5] Cfr. M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* in *Riv. trim. dir. Pen. Contemp.*, 2018, fasc.2, p.23

[6] *Cass. pen*. sez. un., 28 aprile 2016, n.26889

[7] Si veda G. GIOSTRA – R. ORLANDI, *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli, 2018, p. 220.

[8] O. CALAVITA*, op. cit.,* p.52

[9] Cfr. A. CONTALDO,M. IASELLI,R. ONEDA,F. PELUSO,E. TUCCI,G,VACIAGO, *L'informatica per il giurista*, Maggioli Editore, 2019, pp. 327-330

laddove non si conosca con certezza l'ubicazione del *device*; tale tipologia di inoculamento permette, tuttavia, una maggiore accuratezza nella scelta del bersaglio da attaccare, evitando il rischio di colpire altri *device* eventualmente connessi nella rete. L'istallazione virtuale del *malware* è un'operazione più sofisticata; può essere effettuata attraverso l'apertura di una pagina web, o attraverso il *download* di un file presente nell'allegato di un'*e-mail* oppure all'interno di un presunto aggiornamento del *software*.

Una volta istallato, il *software* deve poi essere connesso ad una rete mobile (per inviare ininterrottamente i dati delle attività su quel dispositivo), deve essere invisibile (non deve essere rilevato da antivirus o da controlli effettuati sui processi di sistema attivi), non deve alterare il funzionamento del dispositivo né aumentare i costi di connessione (per non destare sospetti) e non deve entrare in conflitto con le normali operazioni del dispositivo infetto[10]. Per questo motivo, va messo in evidenza che le modalità tecniche attraverso le quali avvengono le operazioni di intercettazione attiva non prevedono un'attivazione ininterrotta e permanente dell'applicazione, ciò per evitare un repentino esaurimento della batteria del telefono monitorato e un consumo importante del traffico dati (che causerebbe, non solo un esaurimento, in breve tempo, del volume consentito all'utente, ma, di conseguenza, anche un aumento della possibilità di rendere nota l'attività d'indagine al soggetto monitorato[11]). Oggi la maggior parte dell'investimento per lo sviluppo di un *software* di questo tipo è previsto per garantire l'invisibilità, ovvero per renderlo occulto.

1.1 LE ETEROGENEE FUNZIONALITÀ DEL *MALWARE*

Una volta che il *trojan* infetta il *device*, inizia una nuova fase, quella del *software* spia (cd.*spyware*).

---

[10] G. ZICCARDI, *Parlamento Europeo, captatore informatico e attività di Hacking delle Forze dell'Ordine: alcune riflessioni informatico - giuridiche,* in *Arch. Pen*., 2017, fasc.1, pp.239-254

[11] Cfr. E. PIO*, Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla Difesa*, 2016, Vol.1, p.159

L'elenco delle attività che possono essere svolte mediante il captatore è molto esteso; le operazioni possono essere suddivise, sulla base della tipologia, in tre categorie: attività di acquisizione delle informazioni scambiate sul dispositivo; attività di controllo dell'hardware del dispositivo; attività di controllo dei contenuti (cartelle e *file*).

Nel primo gruppo rientrano le attività finalizzate all'acquisizione delle informazioni che transitano attraverso il dispositivo bersaglio: telefonate in entrata e in uscita (ivi comprese quelle di *Skype*), videoconferenze, scambi di comunicazioni (effettuate tramite *WhatsApp*, *Telegram* e *Messenger*, SMS, *e-mail*), immagini, video, memorizzazione dei pulsanti premuti sulla tastiera (cd.*keylogger*).

Nel secondo gruppo rientrano tutte le attività che consentono di prendere il possesso dell'*hardware* e di attivare funzioni, quali microfono, telecamera e *GPS*, in grado di trasformare il dispositivo in uno strumento capace di fotografare e riprendere l'ambiente circostante. Nel terzo gruppo rientrano quelle attività capaci di modificare lo stato del dispositivo, ovvero le operazioni che consentono di cancellare le informazioni e di inserirne di nuove[12]. Quando si parla di captatore informatico in ambito investigativo, si è soliti distinguere tra due diverse modalità operative: quella di *online search* e quella di *online surveillance*[13]. I programmi appartenenti alla prima categoria permettono un monitoraggio costante delle attività in rete compiute, in entrata o in uscita, da un dispositivo informatico; la seconda si caratterizza per consentire l'acquisizione, mediante copia, di dati contenuti all'interno delle memorie di un dispositivo informatico, nella maggior parte dei casi un *personal computer*[14]. Se, sul piano scientifico, il captatore informatico rappresenta un notevole traguardo tecnologico, la sua applicazione

[12] "Non va sottovalutato il rischio che il captatore informatico possa essere previamente impostato per cancellare anche il tracciamento delle operazioni dallo stesso eseguite, senza perciò lasciare nemmeno tracce nel suo passaggio" Cfr. L. FILIPPI, *La delega in materia di uso del captatore informatico*, in G. SPANGHER (a cura di), *La riforma Orlando*, Pacini Giuridica, 2017, p.155

[13] Cfr. M. GRIFFO, *op. cit*., p.24; E. M. MANCUSO, *La perquisizione on-line*, in *Jusonline,* n. 3, 2017, pp. 414 ss.

[14] Cfr. S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen*., 2014, n.1, pp. 188-192

nella fase investigativa solleva diverse perplessità. Le varie funzionalità del captatore, delineate in precedenza, consentono, se applicate nel procedimento penale, una pluralità di attività. In primo luogo, dunque, attraverso l'inoculamento del *malware* è possibile acquisire il contenuto di comunicazioni o conversazioni tra due o più persone (attività riconducibile alle operazioni di *online surveillance*); l'attivazione del *software* può anche consentire di espletare un' attività di ricerca nel dispositivo, identificabile in una vera e propria perquisizione da remoto (cd operazioni di *online search*).

Maggiori profili di criticità si rinvengono nella possibilità che attraverso lo strumento informatico si possono acquisire comunicazioni e conversazioni; in tal caso, infatti, l'attività è ascrivibile alla categoria delle intercettazioni. È importante evidenziare che il virus *trojan* consente di intercettare sia comunicazioni effettuate per mezzo dello stesso dispositivo sorvegliato (art.266 c.p.p. co.1), sia normali comunicazioni tra presenti, effettuate senza l'ausilio di strumenti di trasmissione a distanza del suono o dell'immagine (art.266 c.p.p. co.2). Tuttavia, le tecnologie informatiche oggi disponibili consentono lo svolgimento di attività che si spingono oltre l'attività di intercettazione. La capacità di accedere ai dispositivi in uso dal soggetto indagato, consente di perquisire il dispositivo target per ricercare in modo intensivo informazioni di interesse all'interno delle memorie di massa e degli archivi posti al di fuori del dispositivo (cd. *cloud*)[15]. Si tratta delle "perquisizioni *online*[16]", con le quali l'investigatore ha accesso alla vita digitale dell'indagato, quindi non solo ai dati aventi carattere comunicativo. Non comportando una intrusione fisica in una privata dimora, le "perquisizioni a distanza" non minacciano il domicilio; questa è la ragione per cui questa ipotesi fuoriesce dal raggio d'azione degli art.14 e 15

[15] L. FILIPPI, *La delega in materia di uso del captatore informatico*, *op.cit*., p.151

[16] "Le perquisizioni *online* non appaiono riconducibili alle perquisizioni informatiche, con le quali condividono solo il nome, ma dalle quali si differenziano per finalità, struttura e garanzie; né sembrano sussumibili sotto la disciplina delle intercettazioni telematiche, ritenuta inadeguata a ricomprendere le molteplici funzioni dell'agente intrusore." Così M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali,* Giuffrè, 2017, p.57

Cost.[17] In alcuni ordinamenti, le potenzialità che derivano dall'utilizzo ai fini investigativi delle nuove tecnologie non sono passate inosservate e hanno portato all'affermazione di diritti un tempo sconosciuti; per esempio, in Germania agli inizi del 2008 la Corte Costituzionale riconosce per la prima volta un nuovo diritto personale alla segretezza ed inviolabilità delle informazioni contenute nei sistemi tecnologici[18].

Tra le varie funzioni del *trojan* rientrano le attività di *keylogger* e *screenshot.* I *keylogger* consentono di registrare quanto l'utente digita sulla tastiera del dispositivo, per poi inviare i dati ad un sistema di controllo. In questo modo gli inquirenti ottengono una molteplicità di informazioni, prime tra tutte le credenziali di accesso ai servizi informatici in cui l'utente ha effettuato il login. Lo *Screenshot,* invece, cattura i dati che compaiono sullo schermo dell'indagato in tempo reale. Tra gli altri impieghi operativi del *virus* informatico, è interessante evidenziare la possibilità di effettuare delle "videoriprese investigative"[19], che attraverso l'impiego della *webcam* istallata sul dispositivo, permette un controllo continuo della persona sottoposta alle indagini, in qualsiasi momento e luogo si trovi. Le videoriprese, se integrate con l'attivazione del sistema di *GPS*, consentono un pedinamento avanzato della persona che ha in uso il dispositivo. Pur rinviando al proseguo della trattazione l'analisi delle diverse pronunce giurisprudenziali, è interessante far riferimento ad una sentenza della Corte di Cassazione[20] relativa ad una vicenda in cui il captatore è stato impiegato con la funzione di *keylogger*. L'intervento dei giudici di legittimità trae origine da un'indagine relativa ad un'organizzazione che importava ingenti quantitativi di cocaina dal Sud – America. Gli inquirenti captarono la corrispondenza elettronica

---

[17] L. GIORDANO, *La disciplina del "captatore informatico",* in T. BENE (a cura di) *L'intercettazione di comunicazioni*, Cacucci editore, 2018, pp.247 e ss.

[18] Si fa riferimento alla sentenza 27 febbraio 2008 del *Bundesverfassungsgericht*, 1 BvR 370/07 – 595/07, sulla quale si sofferma R.FLOR, *Brevi riflessioni a argine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*, in *Riv. trim. dir. pen. Ec*.;

[19] GIOSTRA- ORLANDI*, Op.cit.,* p.223

[20] Cass., Sez.IV, 28 giugno 2016, n.40903

di alcuni imputati che intrattenevano una corrispondenza elettronica con i complici sudamericani[21]. Mentre le *e-mail* in corso di scambio vennero acquisite con un provvedimento di intercettazione di flussi telematici in entrata e in uscita dai *computer* ai sensi dell'art.266-*bis* c.p.p., maggiori problemi riguardavano le comunicazioni lasciate in "bozza" e quelle inviate e ricevute in precedenza. Per queste ultime gli investigatori si procurarono le credenziali di accesso tramite il *trojan* che, inoculato nei *computer*, permetteva di conoscere quanto veniva digitato sulla tastiera; in questo modo entravano direttamente nelle caselle di posta elettronica, apprendendone il contenuto. La Corte ha ricondotto le *e-mail* pervenute o inviate al destinatario ed archiviate nelle caselle della posta elettronica nella categoria delle intercettazioni, trattandosi di un flusso di dati già avvenuto ed essendo irrilevante la mancanza del presupposto della loro apprensione contestualmente alla comunicazione. Non ha ricompreso, invece, nel materiale intercettabile le *e-mail* "bozza", non inviate al destinatario, ma conservate nell'*account* di posta, le quali potrebbero essere acquisite per mezzo di un sequestro di dati informatici. Secondo la Cassazione "*L'uso del trojan è stato limitato all'acquisizione delle password di accesso agli account di posta elettronica. Ottenute queste password, gli inquirenti hanno avuto anch'essi accesso ai vari account e hanno preso visione a) dei messaggi che venivano via via inviati o ricevuti; b) dei messaggi che venivano salvati nella cartella "bozze". Di conseguenza, si è usato il programma informatico così come si è da sempre usata la microspia per le intercettazioni telefoniche o ambientali*". Parte della dottrina non ha ritenuto condivisibile la posizione della Cassazione, sostenendo che il *software* sarebbe stato adoperato, non per estrarre il contenuto delle comunicazioni, ma per visualizzare quanto digitato sui *computer*. Pertanto, l'attività compiuta configurerebbe un'ispezione o una perquisizione, piuttosto che rientrare nel concetto di intercettazione[22].

[21] Cfr. L. GIORDANO, *L'intercettazione delle e-mail (già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze",* in www.ilpenalista.it, Milano, 2016.

[22] Cfr. M. GRIFFO, *Op.cit.,* p.27-30

2. LA DISCIPLINA DELLE INTERCETTAZIONI DI COMUNICAZIONI E CONVERSAZIONI

Come si è avuto modo di sottolineare, il *virus* di Stato consente un controllo profondo della vita di ogni singolo individuo. Nonostante le enormi potenzialità, tuttavia, il legislatore ha provveduto a regolamentare - come si vedrà nel corso della trattazione - soltanto uno dei possibili impieghi dello strumento, ovvero l'intercettazione di conversazioni e comunicazioni tra presenti. Si rende opportuno inquadrare questa forma di captazione che rappresenta uno dei principali mezzi di ricerca della prova.

Il legislatore non offre una definizione di intercettazione, e di conseguenza, questa rappresenta il risultato di una lunga elaborazione giurisprudenziale che ne ha colto i punti salienti. Per intercettazione s'intende una forma di "*captazione, ottenuta mediante strumenti tecnici di registrazione, del contenuto di una conversazione e/o di una comunicazione segreta tra due o più persone, quando l'apprensione medesima è operata da parte di un soggetto che nasconde la sua presenza agli interlocutori*"[23]. La ragione per cui il legislatore non definisce l'intercettazione, sotto il profilo concettuale, troverebbe la sua ragione giustificativa nella necessità di adattare l'istituto in questione ai progressi dell'evoluzione tecnologica nel settore delle captazioni[24]. Un'attività di questo genere, che fonda la sua forza nell'interesse alla giustizia, non potrebbe trovare cittadinanza nel nostro ordinamento giuridico se non nei limiti di uno dei diritti fondamentali della persona, ovvero nella libertà di corrispondenza, prevista dall'art.15 della Cost., il quale sancisce che "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie previste dalla legge." La Carta fondamentale contiene sia una riserva di giurisdizione, poiché soltanto un provvedimento del giudice può autorizzare un'attività di intercettazione, che una riserva di legge rinforzata, dal momento che comunque

[23] Definizione tratta dalla sentenza della sentenza della Cass., Sez. Un., 28 maggio-24 settembre 2003, TORCASIO, in Guida dir., 2003, 42, 49.

[24] A. SCALFATI, *Manuale di diritto processuale penale*, Giappichelli editore, 2018, p. 316