Trojan horse: tecnologia, indagini e garanzie di libertà

A CURA DI RINALDO ROMANELLI
(COMPONENTE DELLA GIUNTA U.C.P.I., AVVOCATO DEL FORO DI GENOVA)

Il "Focus" si propone di offrire al lettore una serie di spunti e di osservazioni critiche da diverse angolazioni prospettiche (il giudice, l'investigatore, l'avvocato, il tecnico, il professore) in merito al tema dell'utilizzo del captatore informatico quale strumento investigativo.

L'argomento è relativamente "nuovo", posto che è stato portato agli onori della cronaca dalla recente sentenza delle Sezioni Unite "Scurato", malgrado tale tecnica di indagine sia in uso ormai da alcuni anni (da quando e con quali modalità e quantità di impiego è argomento che, tra gli altri, sarà trattato dagli autori che hanno offerto il loro contributo a questo "contenitore").

La prospettiva non vuole essere quella di una nota di commento alla pronuncia del Supremo Collegio (benché molte osservazioni muovano necessariamente dalle argomentazioni in essa contenute) e neppure quella di un trattato che copra ogni aspetto della complessa materia, bensì un'occasione di riflessione e di confronto di idee, non sempre convergenti, in merito alle potenzialità, all'impiego pratico, all'efficacia, che il captatore offre, ai rischi che comporta, alle garanzie ed alle libertà che comprime, qualche volta travolgendole.

Il tema non è, pertanto, circoscritto all'uso del captatore per l'esecuzione di intercettazioni di comunicazioni tra presenti in ambito domiciliare (questione cui è limitato l'intervento del Supremo Collegio), ma si estende agli altri possibili numerosi impieghi operativi dello strumento (con uno sguardo anche ai regimi vigenti in Francia e Portogallo).

La questione impone, in fondo, una riflessione di carattere generale circa la relazione tra teconologia e libertà e una constatazione in merito al rapporto tra legge ed evoluzione tecnologica.

Sotto il primo aspetto il punto sul quale è necessario ragionare senza infingimenti è: fino a che punto lo Stato può controllare la vita del cittadino?

Il progresso scientifico, in questo caso in campo informatico, ma non solo, offre strumenti sempre più efficaci che consentono un penetrante controllo mirato (intercettazioni telefoniche, ambientali, di flussi di dati, localizzazione Gps ecc.) ed un constante e non meno invasivo tracciamento diffuso di dati (movimentazioni bancarie, prelievi bancomat, modalità di utilizzo di carte di credito, telepass, segnalazioni antiriclaggio, registrazione di acquisto di titoli di trasporto nominativi, riprese video di telecamere a circuito chiuso, tracce della navigazione *internet*, dati presenti su *smartphone* e *computer* non previamente intercettati, ma analizzabili a seguito di sequestro, ecc.), cui si può attingere quando sorge l'esigenza investigativa.

È forse il caso di cominciare a prendere atto che non tutto quello che è tecnologicamente possibile acquisire risulta anche compatibile con i principi di libertà che sono garantiti dalla Costituzione e sono alla base del patto che unisce la società civile in un Stato democratico?

Il punto è il senso del limite, che talvolta sembra mancare.

Sotto il secondo profilo, non si può che prendere atto che la legge è costretta ad inseguire un'evoluzione

scientifica che si presenta sempre più rapida ed imprevedibile e nel lasso temporale tra la disponibilità del nuovo mezzo investigativo e l'intervento del legislatore, la tutela dei diritti del cittadino è affidata ad un'interpretazione giurisprudenziale spesso più attenta ad esigenze vere o presunte di sicurezza sociale, che non alle garanzie costituzionali dell'indagato.

Uno sguardo viene dato, dunque, in chiusura anche alle prospettive *de jure condendo* che si identificano ora in una norma di delega da poco approvata dalla Commisione Giustizia del Senato (inserita nel DDL S2067 sulla rifrma del processo), pensata proprio a seguito dell'arresto delle Sezioni Unite, che si prefigge di disciplinare l'utilizzo del captatore informatico (limitatamente però alle intercettazioni di comunicazioni o conversazioni tra presenti, senza trattare le altre possibili modalità di impiego a fini investigativi) ed un disegno di legge (C3762) presentato alla Camera nell'aprile di quest'anno – appena il mese successivo rispetto all'ordinanza della Sesta Sezione che ha rimesso la questione alle Sezioni Unite – più ampio, che riguarda anche il sequestro da remoto di dati diversi dal traffico telematico e telefonico.

Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite

di Edmondo Pio
(Giudice presso il Tribunale di Torino)

Con la recente sentenza 28.04-1.07.2016 n. 26889, affrontando il problema della legittimità delle intercettazioni effettuate a mezzo di "*captatore informatico*" (ossia disposte attraverso l'installazione di virus informatici attivati su computer o smartphone che, conseguentemente, consentirebbero la captazione delle conversazioni, anche tra presenti, "seguendo" indistintamente tutti gli spostamenti dell'utilizzatore del dispositivo elettronico), la Corte di Cassazione a Sezioni Unite ha affermato che:

a)deve escludersi *de iure condito* 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 l. 203/91 (conv. D. L. 152/91); in tale caso, precisa la Corte, non potrebbe nemmeno invocarsi la sanzione della inutilizzabilità dei risultati derivanti dall'attività di captazione "*essendo la stessa riservata a gravi patologie degli atti del procedimento e del processo e non ad ipotesi di adozioni di provvedimenti contra legem*" (punto 6 motivazione);

b)limitatamente ai procedimenti per delitti di criminalità organizzata è, invece, consentita l'intercettazione di conversazioni e comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (personal computer, tablet, smartphone, etc..) anche nei luoghi di privata dimora di cui all'art. 614 c.p., anche se ivi non si stia svolgendo l'attività criminosa ed "*a prescindere dalla preventiva individuazione ed indicazione dei luoghi in cui la captazione deve essere espletata*" (punto 10 motivazione), a condizione che il giudice, nell'autorizzare le particolari intercettazioni "tra presenti" in oggetto motivi adeguatamente le proprie determinazioni;

c)per "*delitti di criminalità organizzata*" si deve intendere "*non solo quelli elencati nell'art. 51 commi III bis e III quater c.p.p., ma anche quelli comunque facenti parte a un'associazione per delinquere ex art. 416*

cod pen., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato".

Nell'articolata motivazione la Corte, dopo aver richiamato talune iniziative parlamentari finalizzate ad introdurre una normativa ad hoc che disciplinasse specificamente l'utilizzo nelle indagini penali di un software simbolicamente definito "*trojan horse*" o captatore informatico-agente intrusore, e dopo aver ribadito la "*tenuta costituzionale*" della disciplina delle intercettazioni ambientali cd. "tradizionali" (art. 266 c. II c.p.p.), ha in particolare affermato l'irrilevanza (nei casi consentiti) di una espressa indicazione del luogo ove deve essere svolta l'attività di captazione (questione che, com'è noto, costituiva il *thema decidendum* prospettato nell'ordinanza di rimessione della VI sezione penale), rilevando tale indicazione limitatamente alla motivazione del decreto nella quale il giudice deve indicare le situazioni ambientali oggetto della captazione "*e ciò solo ai fini della determinazione delle modalità esecutive del mezzo di ricerca della prova che avviene mediante la collocazione fisica di microspie*" (punto 5 motivazione).

In realtà, l'uso del captatore informatico quale "*naturale modalità di attuazione delle intercettazioni al pari della collocazione di microspie*" (punto 10 motivazione) di questo particolare mezzo di ricerca della prova rappresenta "una" delle molteplici potenzialità di azione che potrebbero essere valorizzate dagli organi di investigazione, di prevenzione e sicurezza.

Oltre, infatti, alla possibilità di captazione di conversazioni telefoniche-telematiche e/o tra presenti, si pensi alla possibilità di "ingresso" informatico in altri sistemi ed a distanza, di apprensione di documenti informatici, anche dati, fino alla captazione di immagini (mediante attivazione di web-cam).

Va peraltro evidenziato che, nella pratica quotidiana giudiziaria, le modalità tecniche con le quali avvengono le operazioni di intercettazione attiva non prevedono, in genere, un'attivazione permanente e continuativa – neppure tecnicamente possibile né utile perché determinerebbe un repentino esaurimento della batteria del telefono monitorato e un consumo abnorme di traffico dati che esaurirebbe in breve tempo il volume consentito all'utente e che, soprattutto, aumenterebbe la possibilità di disvelamento dell'attività di indagine da parte del soggetto monitorato – bensì attraverso un comando da remoto attivato di volta in volta dagli operatori del soggetto che fornisce il servizio di intercettazione, su richiesta della p.g. operante (a seconda delle esigenze investigative da perseguire), che, attraverso il monitoraggio telefonico tradizionale e la localizzazione del telefono, è in grado di individuare il luogo ove il dispositivo si trova nonché le persone con cui il soggetto monitorato ha intenzione di incontrarsi.

Le esperienze giudiziarie maturate nel campo delle indagini in procedimenti di criminalità organizzata e terrorismo confermano la centralità dell'acquisizione delle informazioni a mezzo di intercettazione di comunicazioni e di flussi telematici.

Costituisce dato di esperienza il ricorso abituale, da parte delle organizzazioni criminali, a comunicazioni criptate di vario genere (whatsapp; skype; ecc.), la riduzione all'essenziale delle strutture organizzative (spesso dislocate su ambiti territoriali molto ampi e "transanzionali") e, conseguentemente, il ricorso sistematico a comunicazioni via web, ad es., per l'avvicinamento, il reclutamento, l'indicazione in termini generali delle modalità operative nonché, infine, l'utilizzo delle comunicazioni web anche in termini "offensivi" (hakeraggio; penetrazione di sistemi informatici protetti, etc.).

Appare pertanto evidente l'importanza del tema della accessibilità da parte dell'autorità giudiziaria a tali nuove modalità di comunicazione; la straordinaria velocità con cui mutano le tecnologie di comunicazioni è pari al progresso con cui si sviluppano le tecniche di elusione di ogni captazione possibile che si affidano alla impenetrabilità degli apparecchi utilizzati, alla inaccessibilità di particolari reti di comunicazione o alla adozione di sistemi di criptazione dei messaggi scambiati.

In questo senso si è, pertanto, sostenuto che l'adozione dei virus informatici nell'ambito delle intercettazioni di conversazione consente più che un potenziamento, un recupero della efficacia "perduta" o compromessa delle tecniche attuali.

Ad esempio, e sempre traendo spunto dalla esperienza giudiziaria, molte applicazioni di uso comune si avvalgono della criptazione che avviene in origine e alla fine della comunicazione, con sistemi diversi a seconda del produttore dello strumento ma che hanno in comune l'impossibilità di avere le chiavi di entrata e di uscita, che non sono in possesso di coloro che comunicano.

Ciò rende la comunicazione non intercettabile, e l'esperienza insegna che questi metodi di comunicazione criptati (WhatsApp; Skype ecc.) sono utilizzati anche dalle organizzazioni criminali e/o terroristiche per le ordinarie comunicazioni.

Il ricorso all'intercettazione a mezzo "virus" spesso costituisce l'unico strumento in grado di captare le conversazioni criptate dopo la decriptazione, acquisizione che avviene mediante la captazione della comunicazione subito dopo la decriptazione, quando giunge sul dispositivo, oppure subito prima nel caso di comunicazione in uscita.

Quali ulteriori potenzialità di tale strumento, si è sottolineato che essendo il virus in grado di invadere ogni parte del dispositivo e dunque di acquisire ogni tipo di informazione in esso contenuta (si tratti di immagini, documenti, messaggi ecc..), ciò finirebbe con il realizzare una sorta di perquisizione informatica, cui seguirebbe l'apprensione del contenuto (e cioè il suo sequestro).

Al tempo stesso, poiché il virus, in alcune sue strutturazioni, pervade l'intero dispositivo, esso consentirebbe anche operazioni "offensive", dalla distruzione o alla sostituzione di *files*, all'invio di comunicazioni, all'installazione di programmi ulteriori e così via, attività e operazioni che, tuttavia, fuoriescono dal concetto di intercettazione per quanto "lato".

Tali "potenzialità" (la disamina delle quali va, però, ben oltre il pronunciamento della Suprema Corte e l'oggetto del presente scritto) non consentono, tuttavia, di pervenire ad un giudizio ostativo *tout court* dell'istituto in oggetto.

Al contrario, proprio con riferimento alla preoccupazione che l'utilizzo di tale strumento possa produrre esiti lesivi, o mettere in pericolo, la dignità umana o beni di pari valore costituzionale la Suprema Corte afferma (richiamando quanto considerato dalla Procura Generale nella memoria redatta per la Camera di Consiglio del 28.04.16, anch'essa pubblicata) che tale "*pericolo*" ben può essere "neutralizzato" con gli strumenti di cui dispone l'ordinamento "*ad esempio facendo discendere dal principio personalistico enunciato dall'art. 2 della Costituzione e dalla tutela della dignità della persona che ne deriva, la sanzione di inutilizzabilità delle risultanze di specifiche intercettazioni che nelle loro modalità di attuazione e/o nei loro esiti abbiano acquisito <in concreto> connotati direttamente lesivi della persona e della sua dignità*" (punto 10.1 motivazione).

Ciò che conta qui mettere in rilevo, concludendo questa breve riflessione, è che lo strumento si è dimostrato di straordinaria importanza nelle indagini di criminalità organizzata di stampo mafioso e di terrorismo.

Tuttavia, proprio a fronte dell'estremo dinamismo tecnologico dello strumento adoperato e della rapidissima evoluzione delle contrapposte tecnologie di captazione ed elusione delle comunicazioni, deve essere sempre tenuto presente il quadro dei principi a cui l'interprete e l'operatore del diritto devono comunque attenersi.

È infatti di tutta evidenza che l'impiego del software debba assicurare il rispetto delle garanzie che presidiano la riservatezza della vita privata, la cui compressione deve avvenire solo in un'ottica di attento bilanciamento dei contrapposti interessi di rilievo costituzionali (l'inviolabilità del domicilio, l'inviolabilità e la segretezza della corrispondenza e di ogni altra forma di comunicazione, la libertà delle persone e della loro sfera privata, ma anche l'interesse dello Stato a perseguire e reprimere i più gravi fenomeni di commissione dei reati a tutela della sicurezza nazionale e della incolumità dei cittadini), in termini strettamente necessari ed indispensabili per garantire le più elementari e vitali esigenze della sicurezza privata e collettiva.

La Suprema Corte (che più volte nel corso della motivazione richiama i principi, ed i precedenti, costituzionali e sovranazionali *in subiecta materia*) ha, innanzi tutto, sottolineato (e ribadito) il principio che il

ricorso a tale nuova "modalità" di investigazione tecnologica non è di per sé contrario alla Costituzione e/o ad altre fonti sovranazionali (*in primis*, l'art. 8 CEDU sub punto 10.2 motivazione; si vedano, altresì, gli artt. 7-8 Carta dei Diritti Fondamentali, l'art. 16 TFUE e l'art. 39 TUE).

L'attenzione deve allora spostarsi, più che sulla legittimità in sé dello strumento di indagine delle intercettazioni con captatore informatico (affermata nella decisione citata), sulle idonee precauzioni procedurali (in sede di autorizzazione dell'intercettazione e di successive proroghe) che devono presiedere alla delibazione dei presupposti, dei limiti (anche temporali) ed al concreto utilizzo di tale strumento.

Ad esempio, sia in sede di richiesta che nel provvedimento autorizzativo, potranno essere specificate le modalità operative che consentano di parametrare l'attività di captazione con le esigenze investigative in concreto da perseguire, o si potrà prevedere l'attivazione, da remoto, del "*trojan*" solo per la captazione di comunicazioni che avverranno alla presenza dell'indagato e/o di altri determinati soggetti individuati, o ancora si potrà prevedere la captazione solo in luoghi predeterminati con l'esclusione di altri (contribuendo, quindi, ad attenuare i rischi per la privacy di "terzi").

Un ultimo accenno va svolto con riferimento alla nozione di "*delitti di criminalità organizzata*".

Nella citata memoria la Procura Generale aveva ricondotto tale nozione al disposto di cui all'art. 407 c. II lett. a) c.p.p. o, alternativamente, all'esito di una ricognizione sistematica desumibile dai dati normativi già presenti nell'ordinamento (art. 270 *bis* c.p., art. 416 *bis* c.p. e 74 dpr 309/90).

L'opzione interpretativa seguita dalla Suprema Corte nella decisione in oggetto, include in tale concetto non solo i reati elencati nell'art. 51 commi III *bis* e III *quater* c.p.p., ma anche quelli "*comunque facenti parte a un'associazione per delinquere ex art. 416 cod pen., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato*".

Il principio non è nuovo, essendo già stato affermato in precedenza (sempre a Sezioni Unite) in tema di disciplina della sospensione feriale e termini (SSUU 22.3-11.5.05 n. 17706), ed accolto anche da decisioni a sezioni semplici (Cass. Pen. VI sez. 19.03.13 n. 28602).

In una prospettiva *de iure condendo*, ci si chiede, tuttavia, se l'uso dello strumento investigativo *de quo* debba essere esteso anche in caso di indagini avverso un'associazione a delinquere tesa alla perpetrazione di reati-fine di modesta gravità ed, al contrario, se non sia da valutare l'opportunità di estendere l'uso di tale strumento investigativo in caso di indagini per reati non associativi, o non commessi in un contesto di criminalità organizzata, ma anch'essi di rilevante gravità (es. art. 575 c.p., ma non solo).

Il Trojan – Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento d'intercettazione

di Marco Zonaro
(Consulente iscritto all'albo dei Periti del Tribunale di Roma)

La Suprema Corte, affrontando l'argomento del c.d. "captatore informatico", con la nota sentenza del 28 aprile 2016, l'ha definito come dotato di *"formidabile invadenza"* e mai locuzione poteva essere più azzeccata. In realtà non so quanto i Giudici della Corte di Cassazione abbiano una reale contezza delle effettive potenzialità di questo formidabile strumento d'intercettazione di comunicazioni e di acquisizione di dati in-

formatici (in realtà la sentenza ne affronta solo gli aspetti legati alla possibilità di captazione di conversazioni tra presenti), ma di certo ne hanno colto in pieno lo spirito innovativo che rivoluziona e stravolge il concetto stesso d'intercettazione. Infatti, prima o poi doveva accadere che la tecnologia al servizio delle indagini penali mettesse a disposizione degli investigatori dispositivi idonei a contrastare il continuo evolversi degli strumenti di comunicazione e di messaggistica che risultavano non intercettabili mediante i tradizionali impianti installati preso le sale CIT delle Procure. Negli ultimi anni abbiamo assistito alla nascita di applicativi per computer e telefoni smartphone che consentono, non solo la comunicazione verbale tra due o più persone, ma, anche lo scambio di file e di dati e lo scambio di materiale multimediale (foto, video, messaggi vocali, file di testo, fogli elettronici e ogni sorta di file informatico) in totale sicurezza e garanzia per la privacy degli utenti. Applicativi come il popolarissimo strumento di messaggistica istantanea Whatsapp, o il suo antagonista Telegram, il famosissimo Skype, il Messenger di Facebook, Instagram, così come molti altri, non sono intercettabili con i tradizionali mezzi attualmente in uso alle Procure; tali applicativi, infatti, non sfruttano infrastrutture di telecomunicazione dedicate bensì utilizzano, per il loro funzionamento, la rete internet ed i relativi protocolli di trasferimento dati. Cerchiamo di fare un po' di chiarezza con qualche esempio: una comunicazione telefonica che intercorre tra due utenti (indipendentemente che siano utenti di rete mobile o fissa), è intercettabile grazie alla collaborazione dell'Operatore di telefonia a cui appartiene l'utente bersaglio che "devia", duplicandola, la conversazione al sistema d'intercettazione installato presso la Procura richiedente. Lo stesso concetto è valido per tutte le intercettazioni di conversazioni tra presenti, sia che avvengano con microspie funzionanti su rete radiomobile GSM/UMTS (come se fossero dei normali telefoni cellulari), sia che vengano captate con microspie digitali in radiofrequenza, il cui segnale venga poi instradato su rete telefonica. Dunque, in questi casi l'intercettazione è possibile perché il segnale vocale (o il testo nel caso di SMS/MMS e FAX), transita su reti direttamente gestite dagli Operatori di telefonia. Le cose cambiano quando il messaggio transita attraverso la rete internet ed è cifrato all'origine come nel caso degli applicativi di messaggistica istantanea che ho citato precedentemente. Poco cambia se il mezzo fisico di trasporto è sempre quello dell'Operatore di telefonia a cui è abbonato l'utente, in quanto, in questo caso è il protocollo di comunicazione a non essere direttamente gestito e controllato. La navigazione in internet avviene grazie ad un meccanismo di "impacchettamento" delle informazioni che poi vengono inviate a destinazione; ogni singolo pacchetto di dati contiene al suo interno sia "l'indirizzo" del mittente che quello del destinatario. I pacchetti di dati in rete possono viaggiare sia "in chiaro", ossia leggibili da chiunque li intercetti, oppure "cifrati", ossia leggibili solo ed esclusivamente da chi ne possieda la chiave di decrittazione. I sistemi di messaggistica istantanea Whatsapp, Telegram, Skype, ecc. cifrano i propri dati in modo da assicurare i loro utenti che le loro comunicazioni non possano essere violate o lette da chi non ne sia l'esclusivo destinatario. Ciò significa che chiunque riuscisse ad intercettare il flusso di pacchetti costituenti un messaggio (compreso l'Operatore di telefonia al quale l'utente si appoggia per usufruire dei servizi internet), si ritroverebbe in mano una serie di informazioni digitali assolutamente inutilizzabili in quanto non decifrabili. Il c.d. "captatore informatico", a fini investigativi, nasce dunque principalmente con questo scopo: intercettare le comunicazioni verbali derivanti dall'utilizzo di sistemi di messaggistica altrimenti non intercettabili; eh si, perché questi sistemi cifrano tutte le informazioni solo all'atto di uscire dal telefono ma al suo interno esse sono in chiaro e quindi facilmente leggibili. In realtà, poi, si è visto come il "captatore informatico" fornisca una serie di possibilità operative in quanto, di fatto, consente all'investigatore, da remoto, di assumere il controllo del telefono o del computer infettato. Vediamo quali sono alcune importanti operazioni eseguibili grazie all'inoculazione e all'utilizzo del "Trojan":

- **Attivazione remota del microfono del dispositivo**: in questa modalità l'apparato infettato si comporta come una microspia ambientale captando conversazioni di parlatori e rumori ambientali d'intensità sufficiente in relazione alla sensibilità del microfono dell'apparato.
- **Attivazione remota delle fotocamere presenti sul dispositivo:** in questa modalità il dispositivo invia

all'operatore le immagini che vengono catturate dalla o dalle videocamere (qualora ve ne sia installata più di una – ad es. sui telefoni smartphone), alternativamente.

- **Archiviazione di tutte le immagini ed i filmati presenti nelle gallerie:** questa opzione consente di estrapolare dal dispositivo controllato tutti gli elementi multimediali presenti nelle gallerie immagini e video e di archiviarli sul server di ascolto.
- **Lettura ed archiviazione di tutte le chat relative ai sistemi di messaggistica istantanea:** questa opzione consente di leggere tutti i messaggi scambiati, con altri utenti o gruppi di utenti, mediante applicativi di "instant messaging" quali Whatsapp, Telegram, Hangouts, Skype, Messenger e molti altri. Tutte le conversazioni ed i relativi allegati multimediali possono essere scaricati sul server di ascolto.
- **Lettura ed archiviazione della rubrica dei contatti memorizzati sul dispositivo.**
- **Lettura ed archiviazione della cronologia e dell'elenco delle chiamate memorizzate sul dispositivo.**
- **Attivazione della funzione di localizzazione del dispositivo:** mediante questa funzione è possibile attivare il ricevitore GPS del dispositivo che mostrerà, su di una piantina planimetrica, la sua posizione con precisione inferiore ai 20 metri.
- **Lettura ed archiviazione di tutti i messaggi di posta elettronica memorizzati sul dispositivo:** per ogni singolo account di posta elettronica configurato l'operatore può individuare le email inviate e ricevute ed archiviarle sul server d'ascolto.

Quelle elencate sono le principali funzioni che un "captatore informatico" può fornire se correttamente inoculato in un dispositivo mobile o in un personal computer. Le modalità d'inoculazione sono diverse e sovente avvengono da remoto. La probabilità che l'inoculazione vada in porto da remoto è inferiore alla probabilità di successo per un'inoculazione che avvenga con la disponibilità fisica del dispositivo. Inoltre la probabilità di successo di un'inoculazione su un dispositivo mobile è decisamente inferiore rispetto alla percentuale di successi che si ottengono mediante l'inoculazione su personal computer. In pratica il "captatore informatico" altro non è che un piccolo programma software che, una volta entrato nel dispositivo bersaglio, pone in atto delle azioni tali da consentire il suo controllo senza che l'utente ne abbia coscienza: i programmi che agiscono in tal modo, in gergo informatico, sono chiamati "malware" (abbreviazione di MALicius softWARE) e vengono, nel linguaggio comune, definiti "virus" in quanto alcune tipologie di essi hanno eccezionali capacità propagative. Della famiglia dei "malware" appartengono varie tipologie di virus tra cui i c.d. "Trojan Horse"; volendo dare una spiegazione forse un po' semplicistica, ma reale, su cosa sia un Trojan Horse potremmo dire che è un software malevolo che maschera la sua vera identità al fine di sembrare utile per il funzionamento del dispositivo o comunque interessante per l'uso che l'utente ne potrebbe fare. Ciò allo scopo di persuadere l'inconsapevole vittima ad installarlo. Normalmente il Trojan viene diffuso utilizzando tecniche d'Ingegneria sociale, ad esempio inducendo la vittima ad aprire l'allegato di una email apparentemente proveniente da indirizzi conosciuti, oppure a collegarsi su pagine web appositamente create o ancora ad effettuare il download di aggiornamenti per la sicurezza del dispositivo. Nel caso del Trojan ad uso investigativo l'agente intrusore agisce come una backdoor ossia "aprendo" una o più porte di comunicazione del dispositivo stesso verso il server d'ascolto e consentendo così il controllo dell'apparato. Contrariamente a quanto fanno molti virus e worm, i Trojan non tentano di iniettarsi in altri file o di propagarsi su altri dispositivi. Il controller, una volta andata a buon fine l'inoculazione del Trojan, agisce dal proprio computer inviando al dispositivo infettato istruzioni specifiche, costringendolo ad eseguire le operazioni suaccennate. Il controller è anche in grado di porre il Trojan in quiescenza o di costringerlo ad autodistruggersi non lasciando tracce nel dispositivo. La trasmissione dei dati, dal dispositivo infettato al server ricevente, non avviene in maniera diretta ossia non è effettuata mediante un collegamento di tipo end-to-end. Infatti, trattandosi, come abbiamo detto, di trasmissione di dati a pacchetto, dove ogni singolo pacchetto di dati trasmesso contiene sia l'indirizzo I.P. del mittente che quello del ricevente, è necessario far sì che un'eventuale analisi del dispositivo

infettato non consenta di risalire all'indirizzo I.P. del server ricevente. A tal fine, le società che producono il Trojan fanno sì che tra il bersaglio e il server ricevente s'interpongano una serie di ulteriori server, chiamati Proxy, che svolgono la funzione di "nascondere" il reale indirizzo I.P. del server destinatario dei dati così intercettati dal telefono o dal PC infettato. In merito al funzionamento del Trojan ed alle sue potenzialità già tanto si è detto, tuttavia vi sono alcuni aspetti che riguardano le sue modalità operative, che non sono stati ancora oggetto di adeguati approfondimenti. Il primo di essi riguarda proprio il concetto stesso di "controllo" del bersaglio, ossia la concreta possibilità di accedere ai dati del dispositivo infettato e di estrapolarli. Al di là della configurazione giuridica dell'atto, che non è materia tecnica, è necessario considerare che un qualunque prelievo di dati informatici eseguito con questa modalità, dev'essere realizzato nel rispetto di alcuni principi propri dell'ambito della Digital Forensics che sono:

- L'immodificabilità del contenuto della memoria del dispositivo target.
- La conformità dei dati acquisiti con i dati originali.
- La corretta conservazione dei dati acquisiti.

Per quanto concerne il primo punto appare evidente che le operazioni di controllo del dispositivo e di estrapolazione dei dati contenuti nella sua memoria non devono subire alterazioni di alcun genere; l'area di memoria dei dati utente deve restare integra; nessun dato deve poter subire alterazioni e nessun nuovo dato deve poter essere inserito nel dispositivo infettato. Per garantire la correttezza delle operazioni compiute potrebbe essere predisposto, ad esempio, un documento sul quale descrivere tutte le operazioni eseguite fin dall'istante d'inoculazione del Trojan. Questo documento potrebbe essere predisposto in modo tale da non poter essere modificato a seguito dell'inserimento di un nuovo evento e dovrebbe essere firmato digitalmente ad ogni successiva modifica.

Per quanto concerne il secondo punto la questione si presenta alquanto complessa. Infatti, nelle normali operazioni di acquisizione di dati informatici da supporti di memoria digitali, sia che esse vengano compiute ai sensi dell'art. 359 c.p.p. che ai sensi dell'art. 360 c.p.p. la procedura prevede che si possa dimostrare l'identità del dato acquisito con il dato originale, ossia con il dato che rimane memorizzato nel supporto in sequestro. Nel caso dell'utilizzo del Trojan, acquisire in maniera sia parziale che totale i dati presenti sul dispositivo infettato, dimostrando a posteriori la conformità del risultato dell'estrapolazione, risulta alquanto difficoltoso. Ciò in considerazione del fatto che il dispositivo (telefono o PC infettato dal virus) non è in sequestro e quindi non è fisicamente disponibile a chi esegue l'operazione. Inoltre, vi è da considerare che il dispositivo in questione continua ad operare normalmente e quindi continua a ricevere e fare telefonate, scattare foto, navigare in internet, modificando così, dinamicamente, il suo contenuto nel tempo. Tuttavia questo problema potrebbe essere comunque risolvibile ipotizzando, ad esempio, l'implementazione nel sistema d'intercettazione ricevente, di una certificazione dei dati acquisiti, mediante firma digitale, dell'impossibilità di una loro modifica a posteriori e della creazione di un log-report anch'esso certificato e non modificabile, ad ogni record memorizzato.

I dati acquisiti debbono poi essere archiviati su supporti non riscrivibili unitamente ai report-log creati, sia per le fasi di controllo del dispositivo che per le fasi di acquisizione dei dati.

La trasparenza delle operazioni eseguite mediante inoculazione di un Trojan è dunque un requisito fondamentale per un suo corretto impiego. Allo stato attuale, ma questo è solo un mio pensiero, ritengo che il suo utilizzo, senza dover ricorrere a società private, ossia delegando esclusivamente la P.G., sia alquanto improbabile. Come si è detto, infatti, l'inoculazione del Trojan prevede un notevole lavoro a monte di ingegneria sociale; essa richiede, caso per caso, uno studio specifico sul bersaglio. Ogni inoculazione rappresenta una sfida è a se stante e, soprattutto, l'evoluzione tecnologica in ambito di riservatezza e protezione dei dati personali – unitamente alla volontà dei service provider e dei costruttori dei dispositivi di assicurare il proprio cliente circa la tutela della sua privacy – fanno sì che, per poter disporre di tecnologie d'investigazione che

restino al passo con tali evoluzioni, siano necessari cospicui investimenti in ricerca e sviluppo che solo aziende private, economicamente motivate, possono affrontare. Affidare alla sola P.G. lo sviluppo e la gestione di queste nuove tecnologie altamente invasive è certamente possibile e, forse, offrirebbe anche maggiori garanzie, ma rende necessaria la creazione di specifici reparti, dotati di soluzioni software ed hardware sempre all'avanguardia, di personale altamente specializzato, e conseguentemente, dello stanziamento, permanente, di fondi sufficienti. L'affidamento dello sviluppo del servizio a imprese esterne e della sua fruizione da parte della Polizia Giudiziaria, resta, ad oggi, la sola alternativa per l'utilizzo del Trojan a patto di adozione di severe specifiche operative, di un efficace controllo da parte dell'Autorità Giudiziaria, e della possibilità, per le Difese, di verificare, a posteriori, la correttezza e la trasparenza di tutte le operazioni compiute.

"Captatori informatici": per un ponte tra diritto e informatica

di Daniele Minotti
(Avvocato del Foro di Genova)

Ancora una volta, risulta evidente che il legislatore non riesce a stare al passo con la tecnologia.

È questa una prima conclusione, di carattere generale, che si può trarre dalla lettura della pronuncia delle Sezioni Unite sui "captatori informatici"[1]; soltanto, appunto, l'ennesima conferma.

Il ritardo, di per sé, non sarebbe il peggiore dei mali. Ma quando appare evidente che il *gap* è sovente colmato con scarsa attenzione per i diritti dell'uomo, al di là della sterile riproduzione di norme costituzionali e di Carte sovranazionali, allora la situazione diventa intollerabile.

Ciò va sempre evitato, specie quando ci si ritrova di fronte a sperequazioni in favore di una parte, normalmente dell'accusa.

Né il legislatore, né l'interprete – per giungere alla soluzione corretta – possono, però prescindere da un'adeguata conoscenza tecnica del problema; e ciò passa anche per un'analisi della terminologia usata correntemente, vera e propria chiave di volta dell'impianto.

Cosa sono, dunque, i "captatori informatici" di cui si discute?

Si tratta di programmi per sistemi informatici, installati surrettiziamente (per forza di cose) su dispositivi informatici (dispositivi mobili come smartphone e tablet, ma anche computer tradizionali e tutto quanto può essere definitivo sistema informatico). Essi sono destinati allo svolgimento di attività investigative, normalmente (ma non sempre, come vedremo) della famiglia delle intercettazioni.

Il nostro àmbito, dunque, è quello dei mezzi di ricerca della prova.

Molti interpreti sembravano, in un primo momento, particolarmente affezionati alla locuzione "*trojan* di

[1] Corte di Cassazione, sezioni unite penali, sentenza 28 aprile 2016 (dep. 1° luglio 2016), n. 26889, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=1220

Stato", che sottolinea da un lato la provenienza pubblica, non privata, dall'altro la modalità di inoculazione surrettizia, proprio come quella, mitologica, del cavallo di Troia.

Ma è chiaro che, quando si fa esclusivo riferimento alle mentite spoglie di un programma, delle funzionalità del programma stesso non si spiega alcunché. Ne consegue che la locuzione è sostanzialmente inutile, anzi fuorviante.

Anche il termine "virus", che evidenzia la propagazione "virale" del programma su una cascata di dispositivi, ma non ci spiega cosa farebbe, non è appropriata. Peraltro, nessun programma investigativo è scritto per diffondersi su altre apparecchiature.

Invero, da un punto di vista tecnico e considerate le molteplici peculiarità che si esporranno oltre, sembra più corretto il termine, onnicomprensivo, "*malware*". Si tratta di un neologismo informatico che unisce i termini *malicious* (maligno) e software e che, per la sua ampiezza, è in grado di coprire tutti i programmi utilizzati per interferire sul normale funzionamento del dispositivo.

Perché il punto è esattamente quello: l'illegalità, di base, di questi strumenti.

Non si deve mai perdere di vista questo orizzonte: l'installazione, surrettizia, di programmi in un sistema informatico già di per sé può costituire violazione del domicilio informatico (art. 14 Cost. e il correlato reato di accesso abusivo a sistema informatico o telematico ex art. 615-ter c.p., ad esempio) se non, in caso di attivazione di proprie funzionalità, fatti di intercettazioni e perquisizioni illegali (art. 15 per la violazione della corrispondenza), ecc.

Tornando agli aspetti più strettamente terminologici, la giurisprudenza, invece, sembra aver optato per una locuzione indipendente, svincolata dal linguaggio dell'informatica.

In particolare, sembra molto diffusa la locuzione "captatore informatico"[2]. Si tratta, però, di una scelta assai riduttiva. È pertinente al caso, di intercettazioni, preso in esame dalle Sezioni Unite, ma il pericolo è che possa costituire la base per indebite generalizzazioni.

Invero, non è possibile regolare tutti i mezzi di ricerca della prova informatica partendo dal paradigma dell'intercettazione.

L'espressione più corretta, tra quelle utilizzate in giurisprudenza, appare, pertanto, quella di "agente intrusore informatico" in quanto fa perno su tre concetti semplici e diretti: l'agire, l'intrusione, l'àmbito informatico[3].

Un programma per dispositivi informatici (non importa se mobili o fissi) è in grado di prendere completamente il comando della macchina, da remoto, divenendo un vero e proprio telecomando nelle mani di chi può maneggiarlo.

Sistemi di sicurezza permettendo (comunque sempre più sofisticati, per volere degli stessi produttori di sistemi operativi), può fare realmente ciò che vuole, ne dà atto pure la Cassazione.

Si pensi, per parlare del caso classico trattato dalla nota giurisprudenza, all'attivazione del microfono (intercettazione ambientale) o alla captazione del segnale telefonico già all'interno del dispositivo (intercettazione telefonica) o di altre (ove non coincidenti) comunicazioni (intercettazione telematica, anche col "monitoraggio" della tastiera – in questo caso si parla di "*keylogger*").

Anche le telecamere del dispositivo possono essere attivate dall'"intrusore", così rendendo possibile intercettazioni ancora più invasive di quelle limitate all'audio.

[2] Corte di Cassazione, sezione V penale, sentenza 14 ottobre 2009 (dep. 29 aprile 2010), n. 16556 in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=1228

[3] Corte di Cassazione, sezione VI penale, sentenza 26 maggio 2015 (dep. 26 giugno 2015), n. 27100 in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=1201

Nello stesso semplice modo, per individuare più accuratamente la posizione del dispositivo (dunque, eventualmente, il possessore) rispetto alla tradizionale attivazione delle celle, è possibile attivare specifiche radio di geolocalizzazione (GPS e GLONASS, per esempio) e trarne i relativi dati.

Il catalogo delle "*features*" di un agente intrusore informatico è teoricamente illimitato anche se, pur poco nota e di scarsa applicazione (almeno ufficialmente), la più invasiva è certamente quella che consente di consultare file e inviare ogni possibile comando al dispositivo, come se lo stesso fosse tra le mani dell'operatore.

Qualcosa di molto vicino alle ispezioni e perquisizioni informatiche (con conseguenti sequestri), ma non del tutto coincidente.

Non v'è chi non veda quanto tutto ciò si ponga ben al di là della semplice intercettazione (ambientale, telefonica o telematica che sia) trattata in giurisprudenza; e quanto, conseguentemente, ci si trovi di fronte all'imbarazzante inadeguatezza della parte codicistica dedicata, oggi, ai mezzi di ricerca della prova.

Non pochi, anche tra i gli Autori di questa pubblicazione, hanno evidenziato tale realtà che si risolve non in una mera "aticipità" del mezzo (lecito, se risolvibile in ciò), ma in una vera e propria incostituzionalità del sistema (a fronte dei richiamati diritti di rango costituzionale e del mai trascurabile art. 8 CEDU).

Se, insieme a tutto quanto appena detto, si rammenta che, per una deprecabile "dimenticanza" del legislatore del 2008[4], la violazione delle regole sui mezzi di ricerca della prova "informatici" non patisce alcuna sanzione processuale, si comprende come, allo stato, il sistema non possa più reggere.

La storia del diritto dell'informatica ci insegna che, spesso, nel disciplinare la materia il legislatore ha optato per l'uso della metafora per trasportare più agevolmente categorie e regole del tangibile nel mondo dei bit.

Ciò è evidente nella legge 547/93 sui reati informatici che ha introdotto le intercettazioni "informatiche" e, soprattutto, nella relazione governativa del disegno di legge che l'ha generata[5] dove si parla apertamente, per fare un esempio, di "domicilio informatico" estensione di quello "tradizionale" riconducibile sotto la già esistente copertura costituzionale dell'art. 14.

La tecnologia aveva già prodotto una frattura che non poteva più essere colmata e controllata con leciti strumenti interpretativi.

Un metodo analogo si è osservato quando si è deciso di intervenire in tema di indagini informatiche, precisamente con la legge 48/2008.

Ancora una volta, la tecnologia aveva evidenziato il preoccupante distacco dalla legalità di certe procedure investigative imponendo un atto che ha affiancato, ai tradizionali mezzi di ricerca della prova da cui si è tratto il calco, quelli riferiti all'àmbito informatico da inserire nel medesimo *corpus* codicistico.

Da tempo, anche in tema di agenti intrusori informatici, si è raggiunto un analogo punto di rottura che, considerati anche certi affanni, non può più essere gestito, anche dal più abile interprete.

È chiaro, pertanto, che la materia merita un legislatore tempestivo, preparato e attento nel cogliere similitudini e differenze tra i vecchi e i nuovi strumenti.

Il diritto deve saper stare al passo con la tecnologia affinché essa sia strumento di crescita sociale e personale, non di subdola violazione dei diritti dell'uomo

[4] Ci si riferisce alla legge 18 marzo 2008, n. 48, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno".

[5] Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia. – "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (XI Legislatura, divenuto Legge 23 dicembre 1993, n. 547) in Penale.it, http://www.penale.it/legislaz/rel_ddl_2773_XI_leg.htm

Il captatore informatico nell'attuale panorama investigativo: riflessi operativi

di Fabrizio Perna
(Ufficiale dei carabinieri in Palermo)

L'evoluzione sempre più rapida dei fenomeni criminali necessita di un analogo adeguamento degli strumenti normativi e di contrasto. La tendenza a rincorrere l'emergenza, tuttavia, in talune ipotesi ha generato soluzioni paradossali, consentendo l'utilizzo di tecniche assai sofisticate per compiere determinate attività sulla rete ma non prevedendo analoghe operazioni al di fuori dall'ambito informatico.

Il caso emblematico è la possibilità giuridica di intercettare le comunicazioni inoltrate mediante la posta elettronica ma non la tradizionale corrispondenza cartacea con l'assurda conseguenza di poter legittimamente monitorare ingenti flussi di dati via web, magari protetti da complesse cifrature, ma non la veicolazione dei c.d. *pizzini*[6] o la corrispondenza dei detenuti non sottoposta a preventiva censura.

In tale quadro, a volte confuso anche per il ricorso a sistemi spesso di non immediata intellegibilità, si colloca la problematica afferente il c.d. captatore informatico, tipologia di *software* capace di raccogliere clandestinamente informazioni concernenti l'attività di un utente, da ultimo oggetto di intervento delle Sezioni Unite con la sentenza nr.26889/16[7]. Al fine di comprendere al meglio i termini della questione occorre però fare riferimento alla sentenza nr.16556/09[8] della Suprema Corte, prima pronuncia in tema di *spyware,* installato dalla polizia giudiziaria in esecuzione di un decreto di acquisizione documentale emesso dal pubblico ministero ai sensi dell'art. 234 c.p.p.. Il provvedimento, ritenuto legittimo dalla Cassazione, consentiva infatti l'impiego di un virus per il prelievo in copia di quanto memorizzato all'interno di un *personal computer* in uso all'indagato ed ubicato presso un ufficio pubblico. Poiché l'estrapolazione aveva riguardato, non un flusso di comunicazioni tra entità diverse, ma dati già formati e contenuti nell'*hard disk* ovvero che in futuro sarebbero stati memorizzati[9], l'attività era stata qualificata come prova atipica e, come tale, sottratta alla disciplina prevista per le intercettazioni telematiche.

Benché innovativa (i fatti risalgono al 2004), la sentenza già all'epoca ha posto alcuni limiti inerenti l'ubicazione del personal computer in luogo aperto al pubblico e la non modificabilità del sistema informatico nel quale sarebbe stato effettuato l'accesso.

L'interpretazione illustrata è divenuta però incompatibile con la novella legislativa del 2008 che ha introdotto espressamente la perquisizione di un sistema informatico o telematico, definendo di fatto il concetto di domicilio informatico e prevedendo comunque l'adozione di "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

Nella prassi, tuttavia, non sono mancati tentativi di continuare a distinguere l'atipicità dell'intrusione infor-

[6] Strumento arcaico ma sempre attuale di emanazione e/o richiesta di disposizioni in uso tra gli appartenenti a *Cosa Nostra*.
[7] Cass. Sez. Un., 1 luglio 2016 (c.c. 28 aprile 2016), nr.26889, Scurato.
[8] Cass. Sez. V, 29 aprile 2010 (c.c. 14 ottobre 2009), n.16556 Virruso, 246.954.
[9] Nello specifico si trattava di un testo predisposto per essere stampato su supporto cartaceo e poi inoltrato al destinatario latitante attraverso un rodato circuito di intermediari.

matica a distanza e silente, finalizzata alla copia di tutto o parte dell'archivio della macchina, dagli istituti dell'ispezione, della perquisizione e del sequestro. L'acquisizione *insciente domino* e da remoto rappresenterebbe una procedura sì occulta ma non tesa al conseguimento di un vincolo ablativo sul bene captato. Tale assunto si baserebbe sulla considerazione che, a mente dell'art. 189 c.p.p., il mezzo in argomento non arrecherebbe pregiudizio alla libertà di autodeterminazione dell'interessato che rimarrebbe estranea all'operazione di raccolta dati. La fase delle indagini preliminari, peraltro, sarebbe caratterizzata da una sorta di dissenso presunto da parte del destinatario delle iniziative investigative che non sarebbe assimilabile alla facoltà protetta dalla menzionata disposizione. In caso contrario, ogni innovazione investigativa frutto dello sviluppo tecnologico, in quanto incidente sui diritti fondamentali, potrebbe trovare applicazione solo dopo la sua codifica normativa. Il procedimento di acquisizione incontrerebbe così il solo limite di dover essere autorizzato con provvedimento motivato, ossia "*diretto a dimostrare la sussistenza in concreto di esigenze istruttorie volte al fine, costituzionalmente protetto, della prevenzione e della repressione dei reati*"[10], emesso dall'autorità giudiziaria, anche requirente[11].

Il captatore è diventato nuovamente protagonista con la diffusione massiva degli *smartphone* e dei *tablet* ma con la funzione, non di acquisire le copie elettroniche della documentazione "staticamente" allocata sui dispositivi, ma di consentire il monitoraggio "dinamico" dei nuovi canali telematici (messaggerie istantanee, *chatroom*, *social network* etc.), l'agevolazione della tradizionale intercettazione di flussi di dati nonché la captazione audio nei pressi dell'apparato indipendentemente dal luogo ove si trovi l'utilizzatore.

Proprio tale aspetto è alla base della pronuncia n. 27100/15[12] che, rilevando la genericità dell'indicazione dei siti ove sarebbe avvenuta l'intercettazione, ha ritenuto inutilizzabili gli esiti dell'attività realizzata con l'inoculazione del cd. *trojan horse*.

Sia le corti territoriali[13], che successivamente la giurisprudenza di legittimità[14], hanno invece ritenuto non necessaria l'indicazione del luogo soggetto a captazione limitatamente però ai soli delitti di criminalità organizzata e terrorismo. Con riferimento a queste ultime fattispecie infatti, applicandosi l'art. 13 D.L. nr.152/91 conv. nella L. n. 203/91, non opera il limite motivazionale di cui al co. 2 dell'art. 266 c.p.p.

Potendo però lo *spyware* consentire non solo le captazioni audio ma anche altre forme di intrusione nei dispositivi e nella *privacy* dell'utilizzatore la problematica appare tutt'altro che risolta. Un'analisi attenta, tuttavia, suggerisce possibili soluzioni peraltro già sperimentate nelle attività investigative. Il dato di partenza è l'individuazione del risultato cui si mira, valutato alla luce del quadro normativo vigente; se l'ispezione e la perquisizione informatica, a seguito della novella del 2008, hanno una precisa disciplina che non consente l'accesso occulto ai sistemi elettronici, non altrettanto risulta per l'intercettazione di comunicazioni tra presenti o telematiche, tipizzate rispettivamente agli art. 266 e 266 *bis* c.p.p., o e per la captazione di immagini, priva di regolamentazione normativa. La natura stessa delle intercettazioni, definita dai caratteri enucleati dalla giurisprudenza di legittimità[15] (terzietà del captante, clandestinità dell'attività e riservatezza della comunicazione), le rende compatibili con l'impiego del *software* che, da mezzo di ricerca della prova in se stesso, diviene mera modalità esecutiva attraverso la quale il mezzo di ricerca della prova può operare. In altri termini il virus rappresenta sotto il profilo elettronico ciò che sotto l'aspetto fisico è l'apparato di intercettazione

[10] Corte Cost. nr.34/73.
[11] Corte Cost. nr.81/93 e nr.281/98.
[12] Cass. Sez. VI, 26 giugno 2015 (c.c. 26 maggio 2015), n. 27100 Musumeci, 265.654.
[13] Ordinanza del Tribunale di Palermo in funzione di giudice riesame datata 11.01.16.
[14] Oltre alla già citata pronuncia delle Sez. Un., cfr. Cass. Sez. VI, 04 luglio 2016 (c.c. 03 maggio 2016), n. 27404, Marino.
[15] Cass., Sez. Un., 24 settembre 2003 (c.c. 28 maggio 2003), n. 36747, Torcasio.

veicolare. Analogamente, nelle intercettazioni tra presenti c.d. tradizionali non rileva la strumentazione utilizzata, o i modi attraverso i quali si realizza l'accesso ad un fabbricato utilizzato per le riunioni dagli indagati (collaborazione di un terzo, intrusione clandestina, etc.), ma la legittimità dell'attività.

Con riferimento alla registrazione di immagini il discorso è solo lievemente differente non sussistendo limiti alla captazione in ambiente pubblico ma solo nei luoghi di privata dimora e comunque con esclusione delle condotte comunicative[16]. Anche in questa circostanza, la possibilità di sfruttare il dispositivo dell'interessato per la realizzazione stessa del servizio di captazione non ne inficia il risultato.

Nella prassi operativa, peraltro, proprio al fine di evitare che la dichiarazione di inutilizzabilità possa travolgere tutte le attività si suole distinguere nettamente le operazioni, se non addirittura richiedere provvedimenti distinti per l'intercettazione audio e la captazione video. Al fine di non travalicare i limiti di quanto autorizzato la capacità di accesso e verifica all'interno della memoria del dispositivo può essere peraltro inibita agli operatori, scongiurando in tal senso il rischio di acquisizioni dati non consentite.

Tra i dati acquisibili grazie al *trojan horse* vi sono senz'altro quelli afferenti la localizzazione dell'apparato mobile sul quale il virus è installato indipendentemente dal soggetto che detenga stabilmente ovvero occasionalmente lo stesso dispositivo. La situazione è analoga al tracciamento gps inviato dal sistema occultato su un veicolo, utilizzato dall'indagato o da terzi estranei. L'eventuale assimilabilità di tale mezzo alle intercettazioni ovvero l'ipotizzato *vulnus* alla *privacy* sono state da tempo pacificamente risolte dalla giurisprudenza di legittimità[17] che ha sostanzialmente riconosciuto nella rilevazione satellitare, effettuata anche attraverso gli apparati di telefonia mobili[18], una forma tecnologicamente avanzata di pedinamento. Tra l'altro i dati gps indicano asetticamente il percorso dinamico compiuto senza fornire ulteriori elementi circa i luoghi precisamente frequentati, le persone incontrate dal conducente ovvero le attività compiute che, invece, sono documentabili attraverso la forma tradizionale di osservazione a distanza.

La portabilità dei dispositivi mobili e la possibilità di operare le captazioni nelle sue vicinanze ha sollevato l'obiezione secondo cui una simile intercettazione itinerante, oltre a rendere impossibile la preventiva individuazione dei luoghi, si scontrerebbe con altri divieti, ad esempio, in tema di garanzie difensive o di guarentigie parlamentari. Il problema è reale e analogo a ciò che si verifica con le intercettazioni casuali o a c.d. cornetta aperta; in tal senso e considerando che raramente gli operatori hanno contezza preventiva o immediata dell'identità degli interlocutori occasionali cui l'attività non è diretta, l'utilizzabilità della singola captazione andrà valutata in relazione alla specifica disposizione eventualmente violata. Impedire a priori la possibilità di effettuare le intercettazioni in luoghi di per sè frequentati anche da soggetti non indagati equivarrebbe a precludere quasi sempre il ricorso a tale mezzo di ricerca della prova.

Quanto alla diffusione dell'uso del captatore informatico da parte delle Forze di polizia occorre osservare quanto esso, sia per i costi allo stato piuttosto sostenuti, che per le difficoltà tecniche legate all'inoculazione da remoto il cui esito positivo non è affatto scontato, risulti adottato ancora in ambiti investigativi circoscritti e sempre limitato ai soli delitti di criminalità organizzata e terrorismo. Si tratta, infatti, di un rimedio tutt'altro

[16] C. Cost., 24 aprile 2002 (c.c. 11 aprile 2002), n. 135; Cass. Sez. I, 10 aprile 2004 (c.c. 29 gennaio 2003), n. 16965, Augugliaro, 224.240; Cass. Sez. IV, 22 marzo 2005 (c.c. 19 gennaio 2005), n. 11181, Besnik, 231.047; Cass. Sez. Un., 28 luglio 2006 (c.c. 28 marzo 2006) n. 26795, A.P., 234.267.

[17] Cass. Sez. II, 21 maggio 2013 (c.c. 13 febbraio 2013), n. 21644, Bellino, 221,918; Cass. Sez. V, 10 marzo 2010 (c.c. 15 gennaio 2010), n. 9667, Z.B.; Cass. Sez. VI, 11 aprile 2008 (c.c. 11 dicembre 2007), n. 15396, Sitzia, 239.638; Cass. Sez. IV, 21 gennaio 2008 (28 novembre 2007), n. 3017, Besin, 238.679; Cass. Sez. IV, 1 marzo 2007 (c.c. 29 gennaio 2007), n. 8871, Navarro Mongfort, 236112; Cass. Sez. V, 2 maggio 2002 (27 febbraio 2002), n. 16130, Bresciani, 221.918; Cass. Sez. V, 31 maggio 2004 (c.c. 7 maggio 2004), n. 24715, Massa, 228.731.

[18] Cass. Sez. I, 28 maggio 2008 (c.c. 13 maggio 2008), n. 21366, Stefanini, 240.092.

che ordinario nella disponibilità concreta di organismi selezionati per competenza e professionalità.

Già adesso, comunque, sotto il profilo strettamente operativo si percepiscono taluni vantaggi rispetto alle tradizionali attività propedeutiche alle intercettazioni di comunicazioni tra presenti; infatti, non solo la fase di studio delle abitudini dell'indagato – indispensabile per la collocazione degli apparati di captazione – potrebbe in prospettiva ridursi in maniera significativa, ma l'esposizione del personale operante, nonché le imprevedibili *discovery* legate alla casualità e allo stesso intervento umano potrebbero essere addirittura eliminate.

La recente pronuncia delle Sezioni Unite lascia impregiudicata la possibilità di un impiego dello *spyware*, oltre che per i delitti elencati nell'art. 51 co. 3 *bis* e 3 *quarter*, anche per quelli comunque commessi da un'associazione per delinquere. Tuttavia, nell'ottica di disciplinare il futuro utilizzo dello strumento, più che impedirne *tout court* l'uso in queste ultime ipotesi, sarebbe opportuno restringerne il campo d'azione in funzione della gravità del reato fine. In altri termini, pur potendosi condividere il timore di un ricorso abnorme alla tecnologia in argomento anche in presenza di associazioni finalizzate alla commissione di reati punibili a querela o di minore allarme sociale, non appare giustificato ridurre la capacità di indagine nell'ipotesi di gravissime manifestazioni delittuose (es. omicidio e rapina) solo perché riconducibili a forme di delinquenza organizzata non mafiosa né terroristica.

Infine, se da un lato, la sentenza ha consentito di superare il precedente orientamento eccessivamente punitivo nei riguardi delle attività investigative tecnologicamente avanzate, dall'altro ha evidenziato la necessità di una puntuale regolamentazione da parte del Legislatore. Potrebbe, peraltro, essere l'occasione per introdurre nel codice di rito nuovi mezzi di ricerca della prova, ad oggi definiti dalla sola giurisprudenza, quali la videosorveglianza domiciliare (c.d. *home watching* elettronico), il monitoraggio della corrispondenza di detenuti ed il controllo satellitare a distanza (gps).

Trojan horse, strumenti investigativi e diritti fondamentali: alla ricerca di un difficile equilibrio

di Luigi Gino Velani
(Avvocato del Foro di Lucca – Docente a contr. di diritto processuale penale nell'Università di Pisa)

1. *"Timeo Danaos et dona ferentes..."* ma i Troiani non dettero ascolto al grido di allarme di Lacoonte e portarono il cavallo all'interno delle mura, convinti dei buoni propositi dei greci e che quel dono fosse il segno tangibile della fine delle ostilità (come narra Publio Virgilio Marone nel libro II dell'Eneide).

E così, è noto a tutti, il destino della città di Ilio trovò il suo tragico epilogo.

L'astuto Ulisse aveva ideato e portato a compimento il piano che, poi nei secoli, è diventato la metafora entrata nel linguaggio comune per definire qualsiasi stratagemma atto a penetrare le difese, il paradigma per antonomasia dell'intrusione occulta che porta ad ottenere il risultato avuto di mira[19].

[19] Va detto che seppure Ulisse sia considerato un eroe coraggioso e intelligente, allo stesso tempo gli è rimproverato (anche da autori antichi) di essere stato perfido, infame e traditore.

Non a caso, è proprio nella vicenda del Cavallo di Troia che troviamo l'etimologia della parola "*Trojan horse*", termine con il quale nella sicurezza informatica si definisce un software c.d *malware* (cioè dannoso)[20], che ha la caratteristica di nascondere il suo funzionamento all'interno di un altro programma apparentemente utile o innocuo, oppure che è inserito in allegato ad una e-mail, ed è inviato alla sua destinazione "da remoto"; nel momento in cui esegue la finta applicazione o il presunto aggiornamento o legge il messaggio di posta elettronica, l'utente attiva anche il *virus*, che – come i guerrieri achei guidati da Ulisse – si autoinstalla nell'apparecchio o nel sistema e lo "conquista", comunicando il contenuto (a seconda del caso, di vario genere) a un recettore.

Il *malware* attacca indifferentemente *tablet*, *pc*, *smartphone* ed agisce, a differenza del dilagare dei guerrieri greci dentro le mura di Troia, in modo del tutto occulto, ma con la stessa capacità che ebbero le armi degli achei.

Fuori dalla metafora, se queste sono le caratteristiche dei *virus trojan*, non stupisce per niente che un simile strumento sia stato ritenuto utile a livello investigativo, viste le informazioni (elementi di prova) che, tramite il suo utilizzo, è teoricamente possibile apprendere al fascicolo delle indagini: conversazioni, fotografie, video, messaggi di posta elettronica, dati contenuti nell'hard disk, persino in presa diretta nel momento in cui il soggetto digita lettere e numeri sulla tastiera dello strumento sottoposto alla captazione.

Una mole d'informazioni di indubbio valore, ragionando nell'ottica del controllo di legalità, fondamentale all'interno di uno Stato.

Tuttavia, le problematiche sollevate dall'uso di tale strumento privo di regolamentazione positiva a oggi, non sono di poco momento, perché attingono – e sembrano entrare in frizione – con le esigenze di tutela delle libertà costituzionali e dei valori fondamentali protetti a livello internazionale (rispetto alla materia in esame rilevano, in particolare, l'art. 8 della Carta Europea dei diritti dell'Uomo, l'art. 7 della Carta di Nizza e l'art. 16 del TFUE).

Va detto che un vero e proprio dibattito sul tema si è sviluppato – nel nostro paese, ma anche in altre nazioni (Stati Uniti e Germania ad esempio) – solo di recente; effettivamente, complice una certà omertà delle istituzioni, l'utilizzo di questi programmi-spia da parte di Stati e forze dell'ordine non è stato certamente pubblicizzato e, anzi, raramente a livello processuale ne è emerso l'utilizzo ai fini d'indagine, fino a che nelle aule di giustizia non si è dovuto, per forza di cose, cominciare a fare i conti con le implicazioni dovute all'uso sempre più frequente degli strumenti informatici di questo genere.

D'altro canto, l'utilizzo di strumenti informatici e il *web* sono diventati una parte fondamentale della vita delle persone ed è naturale che gli inquirenti rivolgano attenzione investigativa anche alle regioni immateriali di cui l'uomo è ormai un abituale frequentatore (dai contenuti di un hard disk ai social network).

Il tema è piuttosto complesso e coinvolge vari profili che non è possibile affrontare compiutamente in questa sede.

Ed è di quelli che fa "tremare i polsi", viste le pregnanti ricadute sui diritti fondamentali dell'individuo e, di conseguenza, sul rispetto delle garanzie riconosciute al soggetto sottoposto alla vicenda penale.

2. Le riflessioni che seguono prendono le mosse dall'intervento delle sezioni unite "Scurato" che hanno risolto il contrasto, sollevato con ordinanza del 10 marzo 2016 dalla VI sezione penale, nei termini già riassunti nei precedenti scritti di questo "Focus" a cui si rimanda.

[20] Il termine indica un qualsiasi software usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

I giudici di legittimità hanno dato per pacifico che nel caso concreto l'uso del *trojan* fosse riconducibile alla disciplina delle intercettazioni telefoniche e da qui, hanno tirato le somme, come se il tradizionale mezzo di ricerca della prova fosse perfettamente assimilabile al *virus* in questione, distinguendo i casi in cui non è necessario il rispetto del presupposto di cui al comma 2 dell'art. 266 c.p.p., che sono quelli appena riassunti.

Leggendo la pronuncia non è possibile esimersi dal notare, intanto, come i giudici di legittimità abbiano affrontato la questione tralasciando di analizzare la natura, le caratteristiche dello strumento e le implicazioni immediate che discendono dal suo utilizzo, quale l'esigenza di garantire il corretto utilizzo del software *trojan* nel rispetto dei principi fondamentali, vista la particolare forza intrusiva, amplificata dalla circostanza che l'operazione avviene in maniera del tutto occulta, e la capacità di apprendere una quantità di dati così imponente da fagocitare la "vita" del soggetto captato e anche dei terzi che, per caso, vengano in contatto con il dispositivo sottoposto alla captazione.

Il *software malware*, difatti, è in grado di permettere al captante di apprendere le eventuali conversazioni effettuate dall'individuo tanto compiendo una "ordinaria" intercettazione di conversazioni, quanto agendo da microfono o microspia, di acquisire la corrispondenza e-mail, i filmati, i messaggi di qualsiasi genere presenti sull'apparecchio, di monitorarne i movimenti tramite il gps e di accedere ad attività quali la navigazione web e Skype.

Non solo.

Il programma permette al captante di utilizzare l'apparecchio "da remoto", ad esempio facendo inviare messaggi di posta elettronica, oppure inserendovi file o eseguendo riprese video o fotografiche.

Insomma, il *trojan*, da un lato, permette all'intruso di controllare le varie funzioni dello strumento "infettato" e di modificarne il contenuto e, dall'altro lato, assomma le capacità acquisitive proprie di singoli mezzi investigativi, così da diventare, perlomeno a parere di chi scrive, un formidabile veicolo di compressione di varie libertà costituzionali e, comunque, più in generale, di quel bene che possiamo definire "riservatezza" dell'individuo (tra cui rientrano, ad esempio, lo stile di vita, le tendenze culturali, i luoghi frequentati, l'orientamento politico e quello sessuale)[21].

Il primo dei valori che subisce una compressione nei casi in questione è l'inviolabilità del domicilio, ex art. 14 Cost.

Effettivamente, l'esistenza di un domicilio informatico è pacifica nella giurisprudenza della Corte di Cassazione, tanto che il codice penale prevede il reato d'introduzione e trattenimento abusivi nel sistema, ex art. 615 *ter* c.p., e il "possessore" è considerato nella posizione di vantare una pretesa di riservatezza sul bene, meritevole di protezione costituzionale[22].

---

[21] V. per l'individuazione dei fondamenti del diritto alla riservatezza nella giurisprudenza e nella dottrina italiana, A. Cerri, Riservatezza (diritto alla, III - Diritto costituzionale), voce in Enc.Giur., Milano, 1991, XXVII, p. 2 ss. Il problema della salvaguardia del diritto alla riservatezza è precipuo degli Stati moderni e nasce nell'Inghilterra del 1800, per poi affermarsi negli altri Paesi retti da una struttura democratica: v., per l'analisi dello sviluppo delle normative internazionali in merito alla privacy, ancora A. Cerri, Riservatezza (diritto alla, II - Diritto comparato e straniero), voce in Enc.Giur., cit., p. 1 ss. Risalgono ai primi anni del 1970 le pronunce della giurisprudenza costituzionale in merito al diritto alla riservatezza, v. C. Cost. 9.7.1970, n. 122 in Giust. civ., 1970, III, p. 245 e C.Cost., 27.3.1974, n. 86 in FI, 1974, I, p. 1283. Anche la Corte di Cassazione, che inizialmente negava l'esistenza di un diritto alla privacy, cfr. Sez. civ., 22.12.1956, in Giust. civ., 1956, I, p. 5, è poi giunta ad un pieno riconoscimento del diritto alla riservatezza, v., ad esempio, Sez. civ., 07.12.1960, in FI, 1961, I, p. 42.E' noto il recente intervento della corte costituzionale tedesca sul tema, che pur ammettendo, previa autorizzazione, le misure di sorveglianza occulte, quali il trojan, ha dichiarato l'illegittimità di alcune norme previste dall'ordinamento tedesco per il mancato rispetto del principio di proporzionalità tra mezzo utilizzato e bene violato, rispetto alla materia oggetto del procedimento penale. Cfr., per maggiori riferimenti, la nota di L. Giordano - A. Venegoni, La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici, in www.dirittopenalecontemporaneo.it.

[22] Cfr. Cass. pen., sez. VI, 4.10.1999 n. 3067.

Ci pare corretto, allora, trovare nell'art. 14 Cost. una delle disposizioni di riferimento della situazione cui dà origine l'impiego del *malware*.

Dunque, ogni limitazione dovrebbe avvenire nel rispetto dei limiti stabiliti dalla legge processuale di attuazione delle previsioni costituzionali che disciplina le eccezioni, cioè il comma 2, dove sono richiamate le ispezioni, le perquisizioni ed i sequestri, seppure una conclusione del genere sembri messa in discussione dalla giurisprudenza costituzionale in tema[23].

Ma il disposto in questione non pare sufficiente ad esaurire il campo in cui il programma informatico tende ad immettersi in questi casi.

In effetti, nel momento in cui il *virus* capta i dati contenuti nel "bersaglio", l'inquirente viene in contatto con moltissimi aspetti della vita dell'individuo che, non crediamo di dire una banalità, costituiscono qualcosa di più del "domicilio".

Allora i riferimenti costituzionali, per così dire, aumentano, coinvolgendo anche gli artt. 13 e 15 Cost.

A nostro modo di vedere, poi, entrano in gioco anche gli artt. 2 e 3 Cost., l'uno perché è la disposizione, per così dire, "di apertura" agli interessi divenuti esigenze inviolabili della personalità degli individui in base all'evoluzione dei costumi sociali – e la "riservatezza", a modesto avviso di chi scrive, forma ormai parte integrante del catalogo delle libertà fondamentali – [24], l'altro perché l'utilizzo di strumenti così invasivi della sfera intima, quali i programmi *trojan*, deve avvenire con ragionevolezza e proporzione e, quindi, deve essere riservato agli illeciti che più turbano l'ordine e la sicurezza pubblica.

Dunque, l'omologazione del *malware* alla disciplina delle intercettazioni di conversazioni operata dalle sezioni unite, sconta aspetti di criticità rispetto a tali vincoli, poiché le operazioni che si possono compiere per mezzo di tali programmi da un canto sono tra le più invasive che uno Stato mette in campo e, d'altro canto, sono prive di regolamentazione specifica quantomai necessaria in virtù di tale forza intrusiva.

---

[23] Il diritto vivente sembra autorizzare limitazioni al di fuori dei casi del comma 2 dell'art. 14 Cost, cfr. C. cost., 24.4.2002 n. 135, anche se la possibilità di comprimere beni di rango costituzionale, al di fuori delle ipotesi eccezionali previste dalle disposizioni fondamentali appare un' operazione di dubbia correttezza, come sostenuto da recente dottrina, perché, di fatto, rende vano il precetto di cui al comma 1 dell'art. 14 Cost., v. M. Trogu, in AA.VV. *Le indagini atipiche (a cura di A. Scalfati)*, Torino, 2016, 437.

[24] Punti di partenza al fine di riscontrare tale conclusione sono il bisogno della comunità di strumenti idonei a fornire tutela al diritto alla riservatezza e l'esistenza di un interesse dei consociati a che le notizie riguardanti le proprie condizioni personali (concernenti, ad esempio, la salute o l'orientamento sessuale) e le persone od i luoghi frequentati, non trovino diffusione, ma restino, per l'appunto, "riservate". Il bisogno di tutela delle informazioni attinenti la sfera personale dei soggetti è, in effetti, divenuto sempre più crescente a seguito della rilevante importanza che hanno assunto i sistemi informatici e la tecnologia in genere all'interno della società moderna, con conseguente maggiore facilità tanto di effettuare indebite "intrusioni" nella vita privata degli individui, quanto di trattamento, anche illecito, dei c.d. dati sensibili inerenti ai singoli. Sebbene il diritto alla riservatezza non venga espressamente menzionato da alcuna disposizione costituzionale, è ormai acclarato che esso sia contemplato dalla nostra carta fondamentale, emergendo dall'analisi complessiva degli articoli inerenti la tutela delle libertà fondamentali e, comunque, lo si considera recepito dall'art. 2 Cost., che costituisce una disposizione, per così dire, "di apertura" agli interessi divenuti esigenze inviolabili della personalità degli individui in base all'evoluzione dei costumi sociali.Nessun dubbio, quindi, sull'esistenza di un diritto soggettivo alla riservatezza, meritevole di tutela da parte dell'ordinamento, che, a nostro modo di vedere, copre anche aspetti della vita privata quali i luoghi frequentati o la circolazione dei singoli sul territorio. "La fruizione di periodi di isolamento, materiale e psicologico, è un'esigenza addirittura biologica dell'uomo, sicchè può ben dirsi che l'aspirazione a spazi di libertà sottratti ad ingerenze altrui è eterna, quale che sia il contesto socio economico in cui l'individuo opera." così A. Cautadella, Riservatezza (diritto alla, I - Diritto civile), voce in Enc. Giur, cit., p. 1. Da questa originaria formulazione, esaltante l'aspetto individualistico del diritto alla riservatezza, l'attenzione, anche del legislatore, si è inoltre spostata sugli aspetti relativi alla gestione e la diffusione dei dati personali, v. S. Fiore, Riservatezza (diritto alla, IV – Diritto penale), voce in Enc. Giur., cit., p. 2. Rispetto ai profili più strettamente attinenti alla gestione elettronica dei dati personali, cfr. S. Fiore, Riservatezza, voce in Enc. Giur., cit., p. 1; G. Mirabelli, In tema di tutela dei dati personali, in Dir. Inf., 1993, p. 622 ss; Id., Le posizioni soggettive nell'elaborazione elettronica dei dati personali, in Dir. inf., 1993, p. 313 ss; S. Rodotà, Progresso tecnico e problemi istituzionali nella gestione delle informazioni, in AA.VV., Privacy e banche dei dati, Bologna, 1981, p. 30; G. Giacobbe, Riservatezza (diritto alla), voce in Enc. Dir., Milano, XL, 1989, p. 1244.

Ma c'è di più.

3. Le problematiche in questione non rappresentano certamente una novità, dato che le medesime perplessità critiche rivolte all'utilizzo dei programmi *trojan* sono state riservate ad altri apparati e sistemi utilizzati dagli inquirenti per acquisire elementi di prova grazie a tecnologie sempre più sofisticate ed avanzate, che il legislatore del 1988 non poteva certamente immaginare quando ha "disegnato" all'interno del codice di rito i mezzi di ricerca della prova.

Esempio di questo tipo è il monitoraggio dei movimenti dell'individuo o di un veicolo attraverso il sistema GPS, che la giurisprudenza italiana tende a qualificare quale mero pedinamento[25], sganciando, così, il suo utilizzo dal rispetto della c.d. doppia garanzia (autorizzazione all'uso con provvedimento del giudice nei casi e modi previsti dalla legge), al contrario da quanto, viceversa, dovrebbe essere, a nostro parere[26].

Effettivamente, i punti nodali delle questioni sollevate dall'utilizzo di detti strumenti sono sempre gli stessi: (a) la particolare capacità intrusiva che li caratterizza, tale da impattare violentemente sulle libertà costituzionali e sui principi convenzionali e (b) la mancanza di una normativa che li regolamenti compiutamente nel rispetto dei valori fondamentali e del principio di bilanciamento.

Rispetto all'utilizzo dei programmi *trojan*, le perplessità sono, inoltre, amplificate in virtù di altri fattori.

Anzitutto, il fatto che non esiste una "certificazione" dell'affidabilità dello strumento. Le aziende che forniscono tali programmi non sono molte e i programmi – da ditta a ditta – non sono certamente identici, ma non esiste un "disciplinare" che specifichi quali debbano essere i contenuti del *virus* e quali controlli debba subire ai fini dell'eventuale verifica di conformità prima del suo utilizzo (*softwares* che, immaginiamo, siano anche tutelati dalle leggi sulla proprietà intellettuale, con quanto ne consegue rispetto alla ritrosia delle imprese a rendere note le loro caratteristiche).

L'utilizzo del *malware* non è semplice, tanto che la polizia giudiziaria deve ricorrere all'operatività delle aziende stesse; quindi, l'operazione non è "gestita" dagli inquirenti (a tale proposito, ricordiamo che, per note motivazioni, in tema di intercettazioni di comunicazioni la giurisprudenza pretende che gli apparati siano – o, quantomeno, l'acquisizione del flusso dei dati, avvenga nei sistemi – installati presso i competenti uffici di Procura ad opera della p.g., a pena di inutilizzabilità dei risultati *ex* art. 271 c.p.p.).

Non esiste, allo stato, una disciplina della "catena" delle operazioni, che regoli, tra l'altro, le modalità di utilizzo, la verbalizzazione delle operazioni, i limiti da osservare nelle singole ipotesi. Per analogia, pensiamo al percorso che ha portato ai vari interventi normativi in tema di prelievi di campioni biologici finalizzati agli accertamenti DNA, all'utilizzo di tali risultati e alla loro conservazione. Francamente non pare che le implicazioni date dall'utilizzo dei *trojan* ai fini processuali siano meno "delicate" di quelle che si è voluto compiuta-

[25] Cfr., tra le altre, Cass. pen. sez. V, 10.3.2010 in *Dir. Pen. Proc.*, 2010, 1464 e Cass. Pen. Sez. I, 28.5.2008 *Ced Cass. rv 240092*.

[26] Negli Stati Uniti il sistema gps è stato oggetto di una nota pronuncia della suprema corte che ha stabilito che nessun mezzo limitativo dei "beni" di un individuo possa essere effettuato in mancanza di un "mandato" emesso da un giudice laddove esistano le condizioni atte a giustificarlo, cfr. Corte Suprema USA, 23.1.2012, *U.S. vs Jones*. Da notare che nella *cuncurring opinion* redatta dal *Justice* Sotomayor, è stato sottolineato, in buona sostanza, che occorre ripensare l'affermazione per cui nessuno può avere una ragionevole aspettativa di riservatezza riguardo ai dati volontariamente divulgati al pubblico, poiché ciò non comporta un automatico consenso a qualsiasi utilizzo di tali informazioni, generalmente estesa e in ogni contesto, compresa l'indagine penale. Da parte sua la Corte europea dei diritti dell'uomo, v. CEDU, sez. V, 2.9.2010, *Utza c. Germania,* ha considerato il gps strumento utilizzabile ai fini delle indagini in procedimenti di contrasto alla criminalità, valorizzando le circostanze che in Germania esiste una regolamentazione del suo uso, i fatti oggetto del procedimento erano di grave allarme sociale (reati di terrorismo) e che in precedenza strumenti meno invasivi non avevano ottenuto alcu risultato. Sul tema v., volendo, le riflessioni effettuate prima di tali pronunce da L.G. Velani, Nuove tecnologie e prova penale: il sistema d'individuazione satellitare g.p.s., in Giur. It., 2003, 2372 ss e più di recente, L. Filippi, Il gps è una prova incostituzionale. Domanda provocatoria ma non troppo dopo la sentenza Jones della Corte Suprema USA, in Arch. Pen., 2012, 309.

mente disciplinare in tema di DNA e appare, quindi, ragionevole attendere un intervento regolatore da parte del legislatore anche in tema di utilizzo investigativo di *virus* informatici, prima di ricorrere al loro utilizzo.

L'impiego del *software* altera il contenuto del sistema in cui è stato introdotto, redendo, così, palesemente irripetibili le operazioni compiute. Tuttavia, non è prevista alcuna forma di controllo (da riservare al giudice e alle parti) sulla conformità del materiale acquisito rispetto all'originale e, ancora prima, sui modi concreti di acquisizione e conservazione del materiale medesimo. Materiale, non è fantasioso immaginarlo, che in momenti successivi all'acquisizione occulta, l'interessato può cancellare dalla memoria del proprio strumento per qualsiasi motivo, così rendendo impossibile verificare, magari a mezzo di un banale sequestro dell'apparecchio, se effettivamente qual dato fosse stato contenuto o meno nel sistema attaccato dal *virus*.

A complicare il quadro, infine, è l'approccio al problema manifestato dalla giurisprudenza, che tende a riportare i "nuovi" mezzi investigativi ai mezzi di ricerca della prova o alle attività di p.g. tradizionali (pedinamento, ispezione, perquisizione, intercettazione telefonica, ecc.) oppure qualificandoli ex art. 189 c.p.p., lungi dall'interrogarsi compiutamente sulle caratteristiche proprie di tali mezzi, nei termini che abbiamo già accennato sopra, e sulla necessità di sottoporli ad una regolamentazione specifica, rispettosa dei principi che abbiamo citato sopra.

In altre parole, la giurisprudenza ragiona attraverso i tipici paradigmi posti a disposizione dal codice del 1988, sforzandosi di collocare nel loro alveo strumenti che, però, da un lato sono destinati a operare nel mondo immateriale, sensibilmente diverso da quello "reale" che costituiva il punto di riferimento del legislatore all'epoca, e dall'altro lato, possiedono solo una vaga somiglianza e sono piuttosto lontani da rivestire i caratteri propri dei mezzi di ricerca della prova previsti dal codice di rito, soprattutto in ragione della forza di penetrazione che li caratterizza, a sua volta amplificata dall'utilizzo subdolo e occulto cui si prestano in virtù dei caratteri che li contraddistinguono.

Ciò avviene soprattutto, a nostro sommesso avviso, al fine di conservare al procedimento i risultati acquisiti, atteso che una diversa interpretazione renderebbe inutilizzabile il materiale probatorio così ottenuto.

Tuttavia, a parere di chi scrive, per le motivazioni che abbiamo espresso sopra l'uso del *trojan* travalica i limiti di tutela imposti dalla normativa costituzionale e sovranazionale.

Da qui, l'inammissibilità del mezzo e l'inutilizzabilità, *ex* art. 191 c.p.p., dei risultati eventualmente acquisiti con tale sistema.

Infine, dobbiamo notare che, anche se volessimo condividere la soluzione raggiunta dalle S.U. e riportare l'accertamento alla disciplina ex art. 266 ss. c.p.p. nel caso concreto deciso dalla pronuncia "Scurato" (da notare che la Procura Generale nell'articolata memoria depositata in Corte di Cassazione ha sottolineato che il trojan era stato utilizzato esclusivamente per captare conversazioni, ma non per acquisire altri elementi e il gip aveva espressamente vietato il suo utilizzo per riprese video), la conclusione resa non pare in ogni modo corretta.

Se, infatti, il limite ex art. 266 comma 2 c.p.p. non è espressamente indicato nei casi *ex* art. 13, ciò non significa che si possa prescindere dall'individuare il luogo dove deve avvenire la captazione anche in tali ipotesi.

La differenza contenutisca tra le due disposizioni si riflette sulla motivazione del provvedimento che autorizza le intercettazioni, perché nel caso dei reati comuni il giudice dovrà giustificare il presupposto di cui al comma 2 dell'art. 266 c.p.p.

Tuttavia, pure nelle ipotesi di cui all'art. 13 il "luogo" assume rilevanza poichè nessun giudice, prima dell'avvento dei trojan, avrebbe autorizzato l'indiscriminata collocazione di microspie in ogni sito frequentato dal presunto mafioso, perchè deve comunque esistere un nesso tra captazione della conversazione, utilità della medesima e luogo dove avviene l'intercettazione ambientale.

In altri termini, l'art. 13 esonera il giudice dallo specificare i motivi per cui ritiene che nei luoghi *ex* art.

614 c.p. si stia svolgendo l'attività criminosa, ma non lo esime da motivare in merito alla necessità di eseguire l'accertamento in questione in determinati luoghi specificatamente individuati, perché la chiave di volta della normativa, perlomeno a nostro parere, è il presupposto dato dalla "necessità" di disporre l'intercettazione per lo "svolgimento delle indagini" (mentre l'art. 267 c.p.p. parla di assoluta indispensabilità).

Dunque, deve specificare i motivi per cui "è necessario" (cioè utile) disporre l'intercettazione in quel determinato luogo ai fini di acquisire elementi alle indagini.

Un atto che si limitasse ad autorizzare l'intercettazione ubiqua (luoghi privati, aperti al pubblico, pubblici) dovrebbe considerarsi nullo per difetto di motivazione, poichè il giudice non avrebbe giustificato l'esistenza di tale vincolo pertinenziale[27].

Pertanto, anche da questo punto di vista l'epilogo reso con la pronuncia "Scurato" non sembra condivisibile.

L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi, ma sbagliano la terapia*

di Leonardo Filippi
(Avvocato del Foro di Cagliari – Professore Ordinario di procedura penale)

Le Sezioni unite Scurato in tema di captatore informatico hanno azzeccato la diagnosi, ma hanno sbagliato la terapia.

Infatti esse hanno riconosciuto che il nuovo mezzo di ricerca della prova, basato sull'invio "da remoto" e surrettiziamente (ad esempio, con l'invio di allegati a messaggi di posta elettronica o di aggiornamenti di programmi o di applicazioni) su qualsiasi apparecchio (*smartphone*, *tablet*, *p.c.*) di *virus* autoinstallanti (si tratta di un *malware* noto come *trojan horse*), i quali, senza rivelare all'utente la propria presenza, comunicano attraverso la rete, in modalità nascosta e protetta, con il captante che si trova in un centro remoto di comando e controllo e che gestisce il sistema di captazione, attivandolo o spegnendolo all'occorrenza. Tali *virus* sono in grado di intercettare non soltanto il suono captato dal microfono ma anche le immagini carpite dalla *webcam* o filmate con la videocamera, oltre a tutto ciò che viene digitato sulla tastiera o visualizzato sullo schermo. A questi occulti poteri di ispezione e di intercettazione si aggiungono quelli, sempre occulti, di perquisizione e di sequestro in quanto il *virus* può cercare e acquisire i *files* presenti sul dispositivo intercettato e sugli altri connessi in rete locale, inviando dati, comunicazioni o immagini al captante e conseguendo così i risultati tipici di ispezioni, perquisizioni e sequestri di dati informatici (atti eseguiti *on line*, ma da considerare pur sempre compiuti nel domicilio "informatico", tutelato anche penalmente dall'art. 615-ter c.p. contro i "delitti contro la inviolabilità del domicilio"), intercettazioni e riprese fotografiche ed audiovisive. Infine il captatore

[27] Cfr. le lucide osservazioni di A. Cisterna, Spazio ed intercettazioni, una liaison tormentata. Note ipogarantisticche a margin della sentenza Scurato delle sezioni unite, in Arch. Pen., 2016, n. 2.

* Il presente contributo è stato già pubblicato in www.ilpenalista.it

informatico consente pure la geo-localizzazione del dispositivo controllato, attuando anche un "pedinamento elettronico" di chiunque lo detenga.

Il nuovo congegno investigativo non può perciò essere inquadrato soltanto nella disciplina legislativa dell'intercettazione, come riduttivamente hanno fatto le Sezioni Unite, anche in considerazione della privazione che esso comporta dei diritti difensivi riconosciuti dalla legge per le ispezioni, perquisizioni e sequestri.

A tale inedita potenza invasiva e captativa, priva di alcuna garanzia, si aggiunge il particolare, non secondario, che il nuovo strumento di indagine è ospitato nel dispositivo mobile intercettato e quindi si sposta con esso, per cui risulta impossibile individuare previamente i luoghi e quindi i domicili in cui autorizzare tale imprevedibile captazione. Proprio per tale ragione la Suprema Corte l'ha bandito dall'ordinario strumentario investigativo.

Ma è stato trascurato che tale "bulimico" congegno ignora tutti i divieti probatori posti in generale dalla legge (ad es. in tema di diritto di difesa - art.103 c.p.p., di segreto professionale, d'ufficio, di Stato o di polizia - artt. 200, 201, 202 e 203 c.p.p.), sia specificamente in materia di ispezioni e perquisizioni corporali (artt. 245, comma 2, e 249, comma 2, c.p.p.), perquisizioni domiciliari (art. 251, comma 1, c.p.p.), sequestri (artt.254, comma 2, 254-bis, 255, 256 e 256-bis c.p.p.) e intercettazioni (artt.271 c.p.p.).

Perciò, se è parzialmente corretta la premessa, meno corretta è però la conclusione raggiunta dalle Sezioni Unite, perché la Corte ammette tale invasivo strumento nelle indagini per i delitti di criminalità organizzata, per il fatto che per essi il luogo dell'intercettazione è normativamente indifferente (in forza dell'art. 13 d.l. n. 152/1991, conv. dalla l. n. 203/1991): ma la circostanza che la legge non richieda, per alcuni gravi reati, un requisito ulteriore per intercettare nel domicilio, non consente al giudice di autorizzare l'intercettazione in "ogni" imprevedibile domicilio in cui sarà portato il dispositivo.

A ben vedere, proprio dalla premessa da cui muovono le Sezioni Unite, secondo cui il giudice non può previamente conoscere il domicilio intercettato, deriva l'ovvia conclusione per cui la ispe-perqui-intercettazione "itinerante", al pari delle riprese visive, non è prevista dalla legge, né è sottoponibile al previo controllo giurisdizionale quanto agli ignoti domicili che potranno essere violati, sottraendosi così alla "doppia riserva" di legge e di giurisdizione, imposta dagli artt. 14 e 15 Cost., oltre che dall'art. 8 C.E.D.U. Si tratta perciò di un mezzo di ricerca della prova contrastante con la Costituzione e con la summenzionata Convenzione Europea e quindi inammissibile. D'altra parte, ciò è confermato anche dalle iniziative parlamentari, proposte anche dal Governo, tese proprio all'approvazione di modifiche legislative che prevedano specificamente l'impiego della nuova tecnologia investigativa imperniata sul captatore informatico. Né, essendo un atto "a sorpresa", può essere confuso con una prova atipica, per la cui assunzione il giudice deve previamente sentire le parti sulle modalità di assunzione, procedura impossibile per il *trojan horse*.

Trattandosi di un mezzo di ricerca della prova non previsto dalla legge, la violazione del principio di legalità processuale rende questa tecnologia investigativa non una prova atipica, ma una prova "incostituzionale" e "inconvenzionale", perché darebbe luogo ad un'inammissibile autorizzazione ad una ispe-perqui-intercettazione "in bianco", cioè "in qualsiasi domicilio" (nel domicilio del soggetto intercettato, ma anche di terzi estranei ai fatti per cui si procede) si trovi il dispositivo portatile intercettato, nelle mani di "chiunque" lo detenga (anche terzi estranei) e con "qualunque" persona comunichi (anche se immune dall'intercettazione, come ad esempio il difensore o il Presidente della Repubblica) su "qualsiasi" argomento (pure se coperto da segreto) o "qualunque" cosa faccia: in altre parole, la sua ammissibilità segnerebbe la fine della *privacy*, l'annientamento degli artt. 2, 13, 14 e 15 Cost. e la violazione del principio europeo della proporzionalità di questa inedita e formidabile ingerenza nella sfera della *privacy*, in rapporto ai principi fondamentali di una società democratica, come la Corte Costituzionale tedesca ha di recente affermato, con sentenza 20 aprile 2016, proprio in riferimento alla tecnologia dei *virus trojan*. Secondo la *Bundesverfassungsgericht* la legge deve effettuare un bilanciamento tra i contrapposti valori costituzionali, in forza del principio di proporzio-

nalità, per effetto del quale "i poteri investigativi che incidono in maniera profonda sulla vita privata vanno limitati dalla legge alla tutela di interessi sufficientemente rilevanti nei casi in cui sia prevedibile un pericolo sufficientemente specifico a detti interessi". E dal principio di proporzionalità la *BVerfG* fa derivare diverse conseguenze, sottolineando soprattutto che la raccolta segreta di dati personali può estendersi dall'individuo oggetto dell'indagine a soggetti terzi soltanto in condizioni particolari e che occorre tutelare in maniera rigorosa il "nucleo della vita privata", adottando disposizioni di legge che elevino il livello di garanzia.

Si tratta perciò di un mezzo di ricerca della prova inammissibile che la nuova tecnologia non può imporre in spregio ai fondamentali diritti della persona.

Il regime della captazione dei dati informatici nel diritto francese

di Paul Le Fèvre
(Avvocato del foro di Parigi)

La possibilità di utilizzare nel contesto di un'indagine penale il "captatore informatico" è stata introdotta dalla legge n 2011-267 del 14 marzo 2011.

Successivamente due leggi hanno ampliato la portata di questa disciplina (Legge n 2014-1353 del 13 novembre 2014 e legge n 2016-731 del 3 giugno 2016).

È difficile comprendere il regime giuridico applicabile a questo nuovo strumento investigativo senza avere a mente la specificità della procedura penale francese (ancora sistema inquisitorio) rispetto al sistema processuale penale italiano: la figura del giudice istruttore, che è stata abolita alla fine degli anni '80 in Italia, esiste ancora in Francia.

Il giudice istruttore è un magistrato indipendente incaricato di indagare sui fatti gravi e complessi (cioè essenzialmente i crimini e i reati economico-finanziari[28]).

Egli è dotato di poteri molto ampi, come ad esempio quello di disporre le intercettazioni.

Per gli altri reati, è presente il Procuratore della Repubblica – magistrato che dipende dal Ministro della Giustizia – che dirige l'inchiesta penale.

Contrariamente al Giudice Istruttore, il Procuratore della Repubblica non può eseguire atti che comprimano le libertà senza l'autorizzazione di una terza figura dell'ordinamento penale francese: il giudice della libertà e della detenzione (di seguito "JL").

Questo giudice è, come il giudice istruttore, un giudice indipendente. Tuttavia, a differenza del giudice, non indaga i fatti. Ha un ruolo di arbitro molto limitato.

[28] In Francia, le infrazioni sono divise in tre categorie che sono, in ordine di gravità crescente:
- Le contravvenzioni (fatti minori puniti con la sola ammenda)
- I delitti (atti come la violenza o il furto punibili con la reclusione fino a 10 anni);
- I crimini (la maggior parte dei reati gravi, come l'omicidio o stupro - la pena può andare fino all'ergastolo).

Così abbiamo in Francia due possibili tipologie di indagini penali condotte da ciascuno dei magistrati (Giudice Istruttore o Procuratore della Repubblica), con discipline molto diverse.

Fatte queste premesse di carattere comparatistico, l'acquisizione dei dati informatici è regolata dagli articoli 706-102-1 e seguenti del codice di procedura penale (di seguito "CPP").

Questi articoli sono contenuti nel titolo 25 del CPP dedicato alla criminalità e alla delinquenza organizzata.

Vi è infatti in Francia, a partire dalla legge n 2004-204 del 9 marzo 2004, una disciplina penale speciale prevista dagli articoli 706-73 e seguenti del CPP riservata ad alcuni crimini e delitti, commessi da bande organizzate, la cui lista diviene ogni anno più lunga.

Per questi reati, i poteri di indagine del Giudice o del Procuratore (a seconda dei casi) sono notevolmente rafforzati.

È solo ed unicamente nel quadro di questa procedura eccezionale e solamente per le infrazioni che a questa sono sottoposte che gli inquirenti, che agiscono agli ordini del Giudice Istruttore o del Procuratore della Repubblica, possono utilizzare un nuovo strumento di indagine che è definito come:

«Un dispositivo tecnico il cui scopo, senza il consenso degli interessati, è quello di accedere ovunque ai dati informatici, salvarli, conservarli e trasmetterli, così come sono memorizzati in un sistema informatico, come vengono visualizzati su uno schermo dall'utente di un sistema automatizzato di elaborazione dati, così come sono inseriti attraverso i caratteri o come sono ricevuti e trasmessi dai dispositivi audiovisivi. » (articoli 706-102-1 e 706-102-2 del CPP).

Se l'indagine è condotta da un Giudice Istruttore, egli può ordinare l'acquisizione dei dati informatici dopo aver chiesto il parere del Procuratore della Repubblica (la durata dell'operazione non può superare i quattro mesi rinnovabili entro il limite massimo di due anni).

Se, invece, l'indagine è condotta dal procuratore, egli deve richiedere l'autorizzazione preventiva da parte del JLD per eseguire un tale atto di indagine (la durata dell'operazione non può essere superiore a un mese, rinnovabile una sola volta).

Nella decisione di acquisire dati informatici deve essere specificato il reato che giustifica il ricorso a tale metodo, la posizione precisa o la descrizione dettagliata dei sistemi coinvolti e la durata dell'operazione.

Anche se si deve individuare il reato originale che giustifica l'installazione di questo sistema, l'articolo 706-102-4 del codice di procedura penale prevede che "il fatto che queste operazioni rivelino reati diversi da quelli indicati in queste decisioni non costituisce motivo di nullità del procedimento incidentale ".

Questo dispositivo può essere installato dagli inquirenti in due modi:

Sul posto: il Procuratore della Repubblica, autorizzato dal JLD (o il Giudice Istruttore) può entrare nelle case o veicoli per collocare – senza che la persona interessata ne venga a conoscenza – lo strumento tecnico che consente l'acquisizione dei dati informatici.

A distanza: il dispositivo sarà installato in questo caso attraverso una rete di comunicazione elettronica.

Una volta installato, questo dispositivo tecnico permette agli inquirenti non solo di accedere ai dati informatici elencati sul sistema, ma ancor più di «registrarli» e di «conservarli» che corrisponde a procedere a una perquisizione e a un sequestro a distanza, senza che la persona interessata ne venga a conoscenza, senza essere soggetto alle stesse garanzie previste in materia di perquisizioni e di sequestri tradizionali.

La legge stabilisce tuttavia:

-È vietato collocare questo dispositivo negli uffici di avvocati e medici, in studi di notai e ufficiali giudiziari, negli uffici di giornalisti, giudici e parlamentari (articolo 706-102-5 comma 4, del CPP).

-"Ogni elemento relativo alla vita privata estraneo alle infrazioni indicate nella decisione del provvedimento che autorizza la misura non può essere mantenuto nel fascicolo del processo" (articolo 706-102-8 del CPP).

Il regime giuridico di questo nuovo dispositivo è sostanzialmente lo stesso previsto per le intercettazioni telefoniche tradizionali, con una differenza: le intercettazioni telefoniche possono essere effettuate per qual-

siasi reato punibile con almeno due anni di reclusione, mentre l'acquisizione di dati informatici può essere realizzata nel contesto del reato commesso da una banda organizzata ed esclusivamente per i reati elencati agli articoli 706-73 e 706-73-1 del CPP.

L'utilizzo del captatore informatico "Trojan Horse" nella procedura penale portoghese

Di Paulo de Sá e Cunha Leonor Chastre
(Partners, Cuatrecasas, Gonçalves Pereira, RL)

Come premessa a questa breve analisi circa l'ammissibilità dell'utilizzo del *Trojan horse*, come captatore informatico, all'interno della serie degli strumenti di indagine a disposizione di colui che dirige la fase delle indagini, il Pubblico Ministero (*Ministério Público*), dobbiamo marcatamente evidenziare l'inammissibilità di alcuni strumenti nell'Ordinamento giuridico portoghese.

La procedura penale portoghese prescrive la legalità della prova, ossia, l'ammissibilità della prova che non sia proibita dalla legge (Art. 125 del Codice di Procedura Penale portoghese). Pertanto, in aderenza a questo principio di legge, ogni prova ottenuta attraverso la tortura, la coercizione o la violenza all'integrità personale fisica e morale, l'intromissione nella sfera privata di un soggetto, nel domicilio, nella corrispondenza o nelle comunicazioni telefoniche, va considerata nulla ed inutilizzabile, in linea con i principi costituzionali portoghesi (Art. 126).

L'utilizzo del *Trojan horse* può sollevare alcune questioni circa la sua legalità e costituzionalità, poiché non corrisponde ad alcuno strumento di acquisizione della prova previsto dal Codice di Procedura Penale portoghese (ad esempio, registrazioni telefoniche, intercettazioni ambientali o sequestro della corrispondenza) e può essere considerato una intromissione nella vita privata, nella corrispondenza o nelle comunicazioni telefoniche.

Diversi altri diritti costituzionali potrebbero essere fortemente lesi se l'utilizzo del *Trojan* fosse permesso nelle fase delle indagini. Vale a dire: la sicurezza nei procedimenti penali; la libertà di espressione ed informazione; il diritto all'immagine; il diritto alla riservatezza (privacy); il diritto all'inviolabilità del domicilio e della corrispondenza; il diritto di autodeterminazione ed alla comunicazione.

La Costituzione portoghese prevede espressamente (Art. 26, n. 1 e n. 2) che ad ognuno è riconosciuto il diritto all'identità personale, allo sviluppo della personalità, alle capacità civili, alla cittadinanza, al nome ed alla reputazione, all'immagine, alla libera espressione, alla protezione della riservatezza della vita propria e della propria famiglia ed alla protezione contro ogni forma di discriminazione. La legge deve stabilire effettive garanzie avverso l'acquisizione e l'utilizzo impropri di informazioni attinenti a persone e famiglie, nonché avverso la loro acquisizione o il loro utilizzo contrario alla dignità umana.

Una delle regole essenziali per l'interpretazione delle norme di rango primario è l'interpretazione costituzionalmente orientata, vale a dire, tra le varie opzioni ermeneutiche possibili bisogna prediligere l'interpretazione che sia maggiormente compatibile con i diritti fondamentali.

In caso di conflitto con i ben noti "diritti di libertà", questo metodo equivale al principio *in dubio pro libertate*.

Ciò significa che, in caso di dubbio, deve prevalere l'interpretazione che consenta la minor compressione possibile dei diritti fondamentali.

Le restrizioni dei diritti fondamentali sono giustificate e possono essere legittimate unicamente a causa della necessità di salvaguardare altri diritti o interessi costituzionalmente protetti, e non possono eccedere da ciò che è necessario a questo scopo (Art. 18, n. 2 della Costituzione portoghese, che prescrive: "La legge può restringere diritti, libertà e garanzie unicamente nei casi espressamente previsti nella Costituzione, e queste restrizioni devono essere limitate ai casi necessari di salvaguardia di altri diritti o interessi costituzionalmente protetti.").

I diritti fondamentali possono essere limitati unicamente quando è indispensabile e nella misura minore possibile, al fine di salvaguardare gli altri diritti ed interessi protetti dalla Costituzione.

Le peculiarità ed il potenziale dei captatori informatici, come nel caso del *Trojan horse* ed il suo utilizzo come strumento giudiziario per raccogliere elementi di prova da riversare nei procedimenti penali, lederebbe in maniera inaccettabile svariati diritti, libertà e garanzie, non solo della persona che commette il crimine ma anche di indagati innocenti, di terzi, o di altri.

Inoltre, alcuni strumenti, considerando l'imprecisato raggio di azione, che può derivare dal loro utilizzo, non soddisfano il requisito implicito del principio di legalità, impresso per garantire la riserva di legge nella procedura penale, in modo tale che gli indagati non siano sottoposti ad ingiustizie arbitrarie.

Come conseguenza delle considerazioni svolte, deve essere chiaro che ogni istituto della procedura penale presuppone la propria conformità costituzionale che contribuisce alla definizione dei beni giuridici, dei diritti soggettivi e delle regole di comportamento. La subordinazione della legge penale rispetto alla Costituzione non è limitata ai principi costituzionali in materia penale o ai principi di politica criminale.

L'uso di simili strumenti potrebbe anche entrare fortemente in conflitto con la necessaria proporzionalità delle restrizioni dei diritti fondamentali (come già accennato).

Gli strumenti di acquisizione della prova (si può anche ragionare se il *Trojan horse* non ecceda questa definizione e se non sia più corretto qualificarlo come strumento generale di sorveglianza) comprimono i diritti fondamentali e, come tali, sono soggetti alla riserva di legge ed all'autorizzazione da parte del Giudice (per garantire un controllo preventivo da parte di un soggetto indipendente e neutrale, che tiene anche in considerazione in concreto gli interessi del titolare del diritto fondamentale che verrebbe limitato dalla misura).

Conformemente ai principi relativi ai diritti fondamentali racchiusi nella Costituzione, l'autorizzazione di una misura lesiva di diritti è necessariamente soggetta ai limiti imposti dalla necessità, dall'adeguatezza e dalla proporzionalità, ed il principio della proporzionalità richiede che la costrizione di un diritto fondamentale per la tutela del pubblico interesse sia quanto più possibile limitata.

La decisione inerente la proporzionalità di una misura che restringa diritti fondamentali non può essere assunta unicamente in pregiudizio del soggetto titolare di quel diritto. Ciò significa che è l'autorizzazione della misura restrittiva che richiede radicate motivazioni a conferma della congruità, della necessità e della proporzionalità della misura.

L'utilizzo di captatori informatici – come il *Trojan horse* – potrebbe non essere conforme alla legge, all'adeguatezza, alla necessità ed alla proporzionalità, danneggiando così diversi diritti e principi costituzionali, che dovrebbero prevalere nel momento in cui una comparazione venisse fatta al fine di ottenere la minor limitazione possibile dovuta nel caso concreto.

Dobbiamo giungere alla medesima conclusione già ipotizzata nel corso dell'introduzione di questa breve analisi: l'inammissibilità dell'utilizzo del captatore informatico *Trojan horse* come un mezzo di ricerca della prova nell'Ordinamento giuridico portoghese.

La prospettiva *de iure condendo*

Come accennato nelle premesse, il tema del captatore informatico è stato affrontato dal legislatore con un

emendamento al DDL S2067 "*Modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena*", approvato il 2 agosto 2016 dalla Commissione Giustizia del Senato e presentato all'aula per la discussione.

L'emendamento modifica l'art. 35, recante in rubrica la dicitura "*Princìpi e criteri direttivi per la riforma del processo penale in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione*", che prevede una delega in materia di intercettazioni.

In particolare è stata aggiunta la lettera e), che di seguito si riporta:

"*e) disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili, prevedendo che:*

1) l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice;

2) la registrazione audio venga avviata dalla polizia giudiziaria o dal personale incaricato ai sensi dell'articolo 348, comma 4, del codice di procedura penale, su indicazione della polizia giudiziaria operante tenuta a indicare l'ora di inizio e fine della registrazione, secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui all'articolo 268 del medesimo codice;

3) l'attivazione del dispositivo sia sempre ammessa nel caso in cui si proceda per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, del codice di procedura penale e, fuori da tali casi, nei luoghi di cui all'articolo 614 del codice penale soltanto qualora ivi si stia svolgendo l'attività criminosa, nel rispetto dei requisiti di cui all'articolo 266, comma 1, del codice di procedura penale; in ogni caso il decreto autorizzativo del giudice deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini;

4) il trasferimento delle registrazioni sia effettuato soltanto verso il server della Procura così da garantire originalità ed integrità delle registrazioni; al termine della registrazione il captatore informatico venga disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante;

5) siano utilizzati soltanto programmi informatici conformi a requisiti tecnici stabiliti con decreto ministeriale da emanarsi entro 30 giorni dalla data di entrata in vigore dei decreti legislativi di cui al comma 1, che tenga costantemente conto dell'evoluzione tecnica al fine di garantire che tale programma si limiti ad effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia;

6) fermi restando i poteri del giudice nei casi ordinari, ove ricorrano concreti casi di urgenza, il pubblico ministero possa disporre le intercettazioni di cui alla presente lettera, limitatamente ai delitti di cui all'articolo 51, commi 3-bis e 3-quater del codice di procedura penale, con successiva convalida del giudice entro il termine massimo di quarantotto ore, sempre che il decreto d'urgenza dia conto delle specifiche situazioni di fatto che rendano impossibile la richiesta al giudice e delle ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini".

Una prima analisi generale sul decreto ministeriale previsto dall'emendamento Casson- Cucca

di Stefano Aterno
(Avvocato del foro di Roma)

Fabio Pietrosanti e Andrea Ghirardini
(Consulenti informatici)

L'emendamento c.d. Casson - Cucca proposto al Senato ed approvato a inizio agosto scorso contempla la possibilità di definire con decreto ministeriale disposizioni tecniche fondamentali per consentire l'utilizzo del captatore informatico come mezzo di ricerca della prova con il rispetto, nei limiti del possibile, di garanzie per la difesa e per gli organi di polizia. Entro il prossimo 8 settembre verrà depositato un emendamento modificativo dell'attuale testo in esame al Senato che si propone di correggere alcune questioni non esatte e tecnicamente errate indicate nell'emendamento Casson - Cucca.

La normativa che disciplinerà la regolamentazione dei captatori informatici deve essere accompagnata da un disciplinare tecnico che introduca garanzie tecniche e ponga dei limiti all'attività del programma informatico.

Il decreto deve fungere da riferimento tanto per i produttori di captatori informatici, per gli omologatori (la proposta di legge c.d. Quintarelli e gli emendamenti depositati parlano di omologazione) e per tutte le altri parti coinvolte (avvocati e consulenti), andando a stabilire nel dettaglio quali siano gli elementi funzionali nonchè di garanzia rivolti ad assicurare l'integrità e la validità temporale delle informazioni acquisite attraverso il programma informatico.

Per governare la complessità tecnica e tecnologia e garantire il rispetto dei requisiti previsti per legge, si rende necessario senza ogni ombra di dubbio, la disponibilità di regolamentazione tecnica di dettaglio, al pari di quanto già fatto ad esempio per la PEC (posta elettronica certificata), lo SPID (sistema di riconoscimento dell'identità con la PA) o il PCT (processo telematico).

Il disciplinare tecnico relativo al captatore in particolar modo deve regolamentare i seguenti aspetti:

- **Architettura informatica e moduli funzionali**

Definizione dei moduli funzionali di un sistema informatico per captatori quali; a) sistema di gestione, b) modulo captatore, c) sistema di comunicazione, d) sistema di inoculazione, e) sistema di registrazione, f) sistema di controllo dei log relativi all'attività del sistema informatico con il quale l'operatore di polizia controlla e utilizza il programma.

- **Requisiti di compliance rispetto a standard internazionali**

Definiti i requisiti ISO/IEC IS-15408 Common Criteria EAL2, usati comunemente per tecnologie per la sicurezza dello stato, come vincoli minimi di qualità e sicurezza dei software captatori.

- **Requisiti tecnici e vincoli operativi di omologazione**

Definiti i requisiti tecnici con cui devono essere documentate ed eseguite le procedure di omologazione, con particolare attenzione alla "ripetibilità certa" del processo tecnico di creazione di un agente software speculare a quello utilizzato in una investigazione specifica, in modo analogo a quanto già avviene per le certificazioni dei software usati nei giochi a premi.

- **Requisiti e modalità di custodia dei codici sorgenti del software**

Definizione requisiti, procedure e tempistiche di deposito dei codici sorgenti del software da parte dei produttori.

- **Realizzazione di registro captatori informatici e definizione precisa dei dati ivi raccolti**

Definizione delle tipologie di informazioni (nel dettaglio) che dovranno essere comunicate al registro captatori informatici da parte sia dei produttori che dei software installati presso i centri di controllo di AG/PG.

- **Processo e procedura di generazione, uso e verifica presso centro di controllo di PG/AG dei captatori informatici per le singole investigazioni**

Definizione delle procedure con cui è possibile "generare" un captatore da inoculare in un dispositivo bersaglio, quale le sue limitazioni funzionali relative alle autorizzazioni giuridiche concesse e quali le informazioni correlate obbligatorie.

Definizione delle procedure tramite cui le parti possono effettuare una analisi preliminare di congruità e validità delle procedure attuate presso i centri di controllo di AG/PG secondo un percorso tecno-procedurale che garantisca entrambe le parti e sia soprattutto ripetibile.

- **Modalità procedurali-contrattuali per consentire alle parti di ottenere l'accesso alla copia del captatore utilizzato nella specifica investigazione garantendone i vincoli di riservatezza industriale**

Definizione dei requisiti procedurali sia per i produttori che per le parti per poter accedere allo/agli specifici captatori informatici utilizzati in una investigazione specifica, ivi inclusi i requisiti "contrattuali" di garanzia della riservatezza a tutela dei produttori.

- **Modalità di validazione della integrità e di analisi del registro/log di operatività del captatore eseguibile dalle parti**

Definizione delle modalità con cui le parti possano verificare l'integrità dei log di operatività del captatore, delle sue capacità funzionali effettive nonchè di tutte le attività da questo eseguite autonomamente o governato da un operatore di PG/AG sino alla sua disinstallazione.

- **Verifica della validazione del captatore mediante interrogazione al registro captatori**

Definizione delle tipologie di interrogazione dei dati presenti nel registro nazionale dei captatori dalle parti con lo scopo di validazione preliminare per riscontro di eventuali anomalie (es: uso di captatori non certificato o uso di captatori con capacità tecniche maggiori a quelle definite nelle autorizzazioni e nel decreto)

- **Verifica della validità del processo di omologazione con sua ripetibilità indipendente**

Definizione di tutte le modalità con cui le parti possano richiedere e ri-eseguire il processo di omologazione, ivi inclusa l'ispezione dei codici sorgenti software (o di almeno parte del software) e la ri-costruzione della copia esatta del captatore informatico utilizzato nella specifica investigazione. Particolare attenzione deve comunque essere posta alla tutela del segreto industriale dei produttori e alla attribuzione di responsabilità giuridico-contrattuali dei periti tecnici di parte in merito ad accordi di riservatezza.

In considerazione della completa immaterialità degli strumenti definiti nonchè delle informazioni acquisite, l'assenza di un singolo requisito tecnico procedurale definito dal captatore dovrebbe poter rendere inutilizzabili le prove raccolte o comunque determinare dubbi sulla loro integrità e genuinità.

È fondamentale che il disciplinare tecnico sia soggetto a continua revisione da parte delle Autorità Competenti con rilascio periodico di aggiornamenti tecnici-funzionali-procedurali.

È di tutta evidenza infine che il decreto ministeriale dovrà essere scritto con la partecipazione di tutte le professionalità giuridiche e tecniche necessarie nonché con i produttori dei sistemi informatici in questione.

Trojan: urge la legge

di Giorgio Spangher
(Professore Ordinario di procedura penale)

Dopo aver mosso – quasi sotto traccia – i primi passi in alcune vicende processuali, sollevando l'interesse di pochi "addetti ai lavori" esperti in materia informatica, inascoltate le preoccupate "grida" dei difensori di quei processi sulla pervasività dello strumento, le problematiche legate all'uso del *trojan* (*virus* informatico, captatore elettronico) sono "esplose" con la sentenza delle Sezioni Unite Scurato che ha archiviato le aspettative "garantiste" aperte dalla sentenza Musumeci della VI Sezione (presidente Milo).

Le diffuse preoccupazioni per la lesione che l'uso dello strumento può determinare sui diritti di riservatezza delle persone, che rischiano di essere travolti ed annullati dalle "potenzialità" dello strumento, stante la diffusività – quasi generalizzata – del suo uso e l'estrema vastità delle informazioni acquisibili (comunicazioni, dati, immagini, suoni), sono confluite allo stato nei criteri della delega al Governo all'intero del d.d.l. di riforma della giustizia penale attualmente in discussione al Senato.

Al di là degli aspetti tecnici, emerge – con forte evidenza – l'eliminazione dell'ipotesi di "reato facenti capo a una associazione per delinquere *ex* art. 416 c.p. correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato" tra quelle per le quali – secondo le Sezioni Unite – invece, si potrebbe effettuare l'attività *de qua* nei luoghi di privata dimora prescindendo dal fatto che vi si stia svolgendo l'attività criminosa.

Si tratta, com'è noto, di quell'elemento – non condiviso dalla Procura Generale – che aveva da subito sollevato non poche perplessità, per il significativo allargamento del "doppio binario" che si veniva ad introdurre.

Con una recente intervista a «Il Sole 24 Ore», l'Avvocato Generale presso la Procura Generale della Cassazione, nella quale precisava il senso (formale) della esclusione della ricordata ipotesi delittuosa dal raggio di operatività della deroga alla tutela dei luoghi di cui all'art. 614 c.p., ha messo in luce come in materia gli operatori dovranno "controllare" e "controllarsi" sia nel decidere se ricorrere allo strumento investigativo, sia nel fissarne le modalità operative, sia nel gestire gli spesso sconvolgenti risultati probatori. La legge può e deve dire molto al riguardo ma inevitabilmente non potrà dire tutto, anche per l'incessante evoluzione delle tecnologie. A integrare il dettato normativo, dovrà esserci perciò il fattore umano, la responsabilità delle persone che, nella ricerca delle prove, dovranno avere come imperativo categorico il rispetto dei diritti degli indagati e ancor più dei soggetti estranei o occasionalmente coinvolti. E questo vale moltissimo anche per la pubblicità delle informazioni raccolte".

Si tratta di affermazioni sicuramente condivisibili. Non è detto – come si è visto – che siano da tutti condivise. Non ci si può, in questa materia, accontentare di un *self-restreint*. Siamo sicuri che quella soglia, per perseguire (non necessariamente raggiungere) l'obiettivo dell'accertamento, non sarà varcata? Per quanto inadeguata, come riconosciuto dall'Avvocato Generale, serve subito una legge, perché intanto si applica il *decisum* delle Sezioni Unite e si procede con una "gestione" del mezzo senza regole.

La delega fissa ad un anno dalla approvazione della legge il termine (massimo) per la sua attuazione.

Per alcune parti della riforma coperte dalla legge di delegazione (come per le impugnazioni) non solo è stata istituita una commissione ministeriale per l'elaborazione delle proposte di modifiche, ma questa ha anche ultimato i suoi lavori.

La riforma della intercettazione ed ora quella dell'uso del *trojan* non possono più attendere, non solo per il riferito "scarto" tra delega e decisione delle Sezioni Unite che – correttamente – viene applicata, ma soprattutto perché è facile sostenere che, al di là dei buoni propositi, quella "porta" viene e verrà attraversata.

"Trojan di Stato": l'intervento delle Sezioni Unite non risolve le problematiche applicative connesse alla natura del captatore informatico

di Luigi Annunziata
(Dottorando di Ricerca in Diritto e Procedura Penale, Università degli Studi di Roma – La Sapienza)

Il recentissimo intervento delle Sezioni Unite[29] ha rinfocolato il dibattito attorno all'impiego di quel peculiare mezzo di ricerca della prova che va sotto il nome di captatore informatico, da più parti ribattezzato "trojan di Stato" : si tratta, in via di estrema sintesi, di un malware (ossia di un software maligno, comunemente detto virus informatico) occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva (tra cui rientrano, dunque, tutti i moderni pc, smart-phones, tablet, ecc.), il quale consente in ogni momento all'attaccante – tra l'altro – di captare tutto il traffico dati (sia in entrata che in uscita), di attivare da remoto il microfono e la telecamera registrandone le attività, di "perquisire" gli hard disk e di fare copia integrale del loro contenuto, di intercettare (ed eventualmente decifrare) tutto quanto digitato sulla tastiera, di fotografare le immagini ed i documenti visualizzati dall'utente-obiettivo (c.d. screenshot).

Come noto, le questioni sollevate con l'ordinanza di rimessione si limitavano alla individuazione dei luoghi all'interno dei quali debba ritenersi consentita l'attività captativa eseguita attraverso il *trojan*[30]: attenendosi scrupolosamente al *petitum*, gli Ermellini – propinando una sorta di "doppio binario" tra reati comuni e reati associativi (non solo di stampo mafioso) – hanno escluso «*la possibilità di compiere intercettazioni nei luoghi indicati dall'art. 614 cod. pen., con il mezzo indicato in precedenza, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'art. 13 d.l. n. 152 del 1991, convertito in legge n. 203 del 1991, non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'art. 266, comma 2, cod. proc. pen., che in detto luogo «si stia svolgendo l'attività criminosa»*»; hanno invece aperto alla «*captazione nei luoghi di privata dimora ex art. 614 cod. pen., pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'art. 13 d.l. n. 152 del 1991*», precisando però che «*per procedimenti relativi a delitti di criminalità organizzata devono intendersi quelli elencati nell'art. 51, commi 3-bis e 3-quater, cod. proc. pen. nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato*».

Si tratta di una soluzione in linea con l'ormai consolidato orientamento giurisprudenziale in materia di inutilizzabilità e divieti probatori, teso ad assicurare la conservazione della prova e chiaramente ispirato ad un (difficile) bilanciamento tra interessi contrapposti, quello all'accertamento ed alla punizione dei reati da un lato e quello al rispetto delle garanzie costituzionali dall'altro lato.

Tuttavia, sarebbe stato lecito attendersi una maggiore incisività del Collegio esteso rispetto alle proble-

[29] Cass. pen., SS.UU., 1° luglio 2016 (ud. 28 aprile 2016), n. 26889, in *www.giurisprudenzapenale.com*.
[30] Cass. pen., Sez. VI, ord. 6 aprile 2016, n. 13884, in *www.giurisprudenzapenale.com*.

matiche "tecniche" derivanti dalla installazione del captatore informatico, rimaste invece irrisolte. Ciò che sorprende negativamente è l'approccio mostrato dalla Corte rispetto alla fondamentale disamina delle caratteristiche tecniche del *trojan*: infatti, dopo una attenta dissertazione in ordine alle funzionalità di tale strumento particolarmente invasivo, gli Ermellini affermano che «*l'installazione del captatore informatico in un dispositivo "itinerante" , con un provvedimento di autorizzazione motivato e nel rispetto delle disposizioni generali in materia di intercettazioni, costituisce una delle naturali modalità di attuazione delle intercettazioni al pari della collocazione di microspie all'interno di un luogo di privata dimora*».

É questo il passaggio argomentativo che convince meno, poiché si limita a considerare la fisiologia dello strumento di indagine, omettendo ogni riferimento alle gravi "patologie" che contraddistinguono il *trojan*, il quale non può in alcun modo essere assimilato alle microspie: tra le "controindicazioni" notoriamente proprie del *trojan*, la più rilevante attiene alla circostanza per cui – trattandosi nient'altro che di un virus informatico, una volta installato sull'apparecchio-obiettivo – il captatore è per sua natura in grado di evolversi incontrollatamente, potendo mutare irrimediabilmente lo stato del luogo virtuale oggetto di hackeraggio[31]; caratteristica, quest'ultima, evidentemente estranea alle microspie.

Si tratta dunque di individuare una soluzione in grado di assicurare la genuinità dei dati captati attraverso l'installazione del *trojan*: in attesa di un sempre più necessario intervento legislativo regolatore della materia *de qua*, la soluzione appare ricavabile dalla disciplina vigente.

Partendo infatti dal presupposto per cui l'attività captativa eseguita mediante *trojan* costituisce un accertamento tecnico non ripetibile[32], in quanto modifica il luogo virtuale nel quale il *malware* viene installato, costituirebbe garanzia necessaria (ma non ancora sufficiente) l'attivazione di un meccanismo analogo a quello offerto dall'art. 360 c.p.p.[33], se del caso sfruttando l'instaurazione di quel "confronto differito" già previsto (proprio in materia di intercettazioni) dall'art. 268 c.p.p., le cui maglie larghe andrebbero però sensibilmente ristrette da un sapiente intervento del legislatore: ciò consentirebbe almeno di addivenire ad un accertamento postumo sull'apparecchio hackerato, da effettuarsi nei momenti immediatamente successivi alla conclusione delle operazioni di captazione, volto a cristallizzare le caratteristiche tecniche sia del *malware* che dell'apparecchio, nonché a certificare la quantità e la qualità dei dati captati.

Assai più adeguata parrebbe poi l'ulteriore cautela – di ordine squisitamente tecnico – costituita dalla possibilità, per il Pubblico Ministero, di ordinare l'effettuazione – contemporaneamente alla installazione del *trojan* – di una operazione c.d. di *keylogging*, eseguita attraverso *software* in grado di registrare istantaneamente sia il contenuto dell'apparecchio-obiettivo al momento dell'hackeraggio sia le attività compiute su quell'apparecchio tanto dall'utilizzatore quanto (eventualmente) dall'attaccante[34]: si tratta cioè di una sorta di

---

[31] Ancora con riguardo alle patologie affliggenti il *trojan*, si deve rilevare - per completezza di riferimento - che il *software*, una volta installato, non può essere rimosso dall'attaccante, restando dunque giacente all'interno dell'apparecchio-obiettivo: ne deriva che l'investigatore "distratto", anche al di fuori dei limiti temporali impostigli dal provvedimento autorizzativo, potrebbe sempre riattivare la captazione da remoto. A tale ultimo proposito, occorre inoltre osservare come l'installazione del *trojan* non consenta soltanto di estrapolare fiumi di dati dall'apparecchio-obiettivo, ma permetta anche di introdurre qualsivoglia *file* o *software* all'interno dell'apparecchio hackerato, con conseguente ulteriore possibile mutamento dello stato originale del luogo virtuale.

[32] Non si è infatti in presenza di una lettura "postuma" dell'apparecchio-obiettivo, tradizionalmente ritenuta accertamento ripetibile dalla giurisprudenza di legittimità. Cfr. Cass. pen., Sez. I, 25 febbraio 2009, n. 11503; Cass. pen., Sez. I, 5 marzo 2009, n. 14511.

[33] Sulla natura irripetibile di analoghe operazioni di *forensic computing* e sulla necessità di attivare (anche *ex post*) il meccanismo di cui all'art. 360 c.p.p., si vedano già D. Curtotti, *Rilievi e accertamenti tecnici*, Padova, 2013, p. 183; M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2, 2011, p. 284; E.M. Mancuso, L'acquisizione *di contenuti* email, in *Le indagini atipiche*, a cura di A. Scalfati, Torino, 2014, p. 65.

[34] Per maggiori approfondimenti in ordine alla natura ed alle caratteristiche dei *softwares* di *keylogging*, nonché in ordine alla relativa

captazione della captazione, che garantirebbe la genuinità del dato probatorio acquisito attraverso un semplice confronto (postumo) tra il contenuto del *keylogger* e quello del *trojan* (*rectius*, del *file* remoto nel quale viene convogliato il flusso di dati intercettato dal captatore informatico).

Questioni di tal genere non sembrano ancora preoccupare la giurisprudenza interna, che pretende di risolvere i problemi posti dalla *forensic computing* facendo ricorso ad istituti e categorie "tradizionali" , spesso del tutto inapplicabili.

Appare pertanto evidente l'indifferibilità di un attento intervento legislativo *in subiecta materia*: in particolare, dovendosi individuare una soluzione in grado di contemperare sia le esigenze di accertamento penale sia quelle concernenti il rispetto dei diritti dell'indagato, sembrerebbe auspicabile muovere dalla disciplina vigente (con particolare riguardo a quella di cui agli artt. 360 e 268 c.p.p.) per adattarla alle vette raggiunte dalle moderne tecniche di investigazione; in questo senso, parrebbe irrinunciabile un riferimento normativo alle operazioni di *keylogging*.

Rilievi conclusivi rispetto alla delega in discussione al Senato

di Rinaldo Romanelli
(Componenete della Giunta U.C.P.I., avvocato del foro di Genova)

Come già sottolineato, la parte certamente di maggior impatto della norma appare l'esclusione dell'art. 416 c.p. dalle ipotesi di reato che giustificano l'attivazione del captatore informatico nei luoghi assistiti da tutela domiciliare.

Questa impostazione, che pure sembra un passo nella giusta direzione, desta però qualche perplessità e necessiterà di un adeguamento al momento del passaggio in aula a Palazzo Madama.

Ove la previsione si tramutasse in diritto positivo (a seguito di attuazione della delega), infatti, andrebbe a costituire parte integrante della discliplina delle intercettazioni di comunicazioni tra presenti attualmente delineata dall'art. 266 c.p.p. e dall'art. 13 del D.L. 152/1991, così come interpretato dalle SSUU "Scurato".

La prima disposizione, come si è già più volte visto, detta la norma generale che consente l'intercettazione tra presenti in ambito domiciliare solo ove vi sia fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa; la seconda, in deroga a tale previsione, consente, in procedimenti relativi a delitti di "criminalità organizzata", la stessa intercettazione in ambito domiciliare "anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa".

Le SSUU "Scurato" hanno chiarito che la locuzione "criminalità organizzata" deve riferirsi anche all'ipotesi delineata dall'art. 416 c.p. (condivisibile o meno, questo attualmente è il *dictum* del Supremo Collegio).

applicazione in ambito di *forensic computing*, si vedano S. Aterno - M. Mattiucci, Cloud Forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. Pen.*, 3, 2013, p. 875.

Il quadro che si andrebbe a comporre autorizzerebbe, dunque, le "tradizionali" intercettazioni "ambientali" in ambito domiciliare per il reato di cui art. 416 c.p., senza necessità che vi sia fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa, ma non l'attivazione del captatore informatico.

Per converso, il captatore informatico, attivabile nei medesimi limiti dell'intercettazione ambientale "tradizionale" solo per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*, sarebbe in via generale "installabile" e attivabile per tutti gli altri reati secondo i limiti di ammissibilità dettati dall'art. 266 c.p.p.

La soluzione pare irrazionale ed è, probabilmente, il frutto di una eccessiva timidezza e di un equivoco di fondo.

L'equivoco, che peraltro verte sul tema centrale della questione, sembra ruotare intorno alla specifica indicazione del luogo nel quale viene autorizzata l'intercettazione di comunicazioni tra presenti.

L'origine pare potersi rinvenire al punto n. 6 della motivazione della più volte menzionata sentenza "Scurato".

In esso la Corte, in modo per la verità non del tutto chiaro, pare escludere la possibilità di utilizzare il captatore informatico per intercettazioni ambientali fuori dalle ipotesi di criminalità organizzata, tra l'altro perché "*[..] b) all'atto di autorizzare una intercettazione da effettuarsi a mezzo captatore informatico installato su di un apparecchio portatile, il giudice non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico* (smartphone, tablet, computer) *verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale c) peraltro, anche ove fosse teoricamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione nel caso di ingresso in un luogo di privata dimora, sarebbe comunque impedito il controllo del giudice al momento dell'autorizzazione, che verrebbe disposta al buio […]*".

Appare però evidente un errore concettuale: il giudice non può prevedere in quali luoghi verrà introdotto il dispositivo portatile, ma la circostanza non ha alcuna rilevanza.

Ciò che il giudice dovrebbe limitarsi a valutare è in quale luogo domiciliare può essere autorizzata l'intercettazione perché ricorre il presupposto del comma secondo dell'art. 266 c.p.p., o perché, trattandosi di criminalità organizzata, vi è un interesse investigativo che, in quel luogo e solo in quello, consente la compressione della libertà domiciliare (sarà l'abitazione dell'indagato, l'ufficio, o un altro domicilio abitualmente frequentato rispetto al quale vi siano fondate ragioni di ritenere che l'attivazione dell'intercettazione possa fornire elementi utili all'indagine).

Quando il dispositivo accede al domicilio ove è autorizzata l'intercettazione questa viene attivata; se è già attiva e il dispositivo accede a un domicilio nel quale l'intercettazione non è autorizzata, viene disattivata.

Se il captatore informatico consente la geolocalizzazione satellitare, tale operazione pare possibile in accordo con le altre previsioni del DDL secondo le quali l'attivazione non deve essere permanente a seguito dell'installazione (cosa, peraltro, allo stato attuale della tecnica difficilmente ipotizzabile in un dispositivo portatile la cui batteria verrebbe molto rapidamente consumata dall'attività del Trojan), ma deve essere effettuata di volta in volta dalla polizia giudiziaria sulla base delle disposizioni impartite nel decreto autorizzativo.

Se così è, però, non si comprende con immediatezza per quale ragione escludere l'art. 416 c.p. dal novero dei delitti per i quali può utilizzarsi il Trojan in ambito domiciliare, lasciando immutata la disciplina che consente le intercettazioni "tradizionali".

Forse perché con l'ambientale "tradizionale" il giudice autorizza la captazione in un domicilio ben determinato e, dunque, valuta espressamente che rispetto a quello specifico luogo sussistono effettive e concrete ragioni investigative che legittimano la compressione delle libertà domiciliari?

Si ritiene, dunque, che solo per reati di cui all'articolo 51, commi 3-*bis* e 3-*quater*, sia accettabile un'intercettazione "itinerante" che si traduca di fatto in una molteplicità di imprevedibili intercettazioni domiciliari?

Come si è visto, però, l'ipotesi dell'intercettazione "itinerante" non è necessitata dalle caratteristiche del

Trojan e concettualmente non appare accettabile per le numerose ragioni che sono già state esposte nei vari interventi che compongono questo "Focus".

La soluzione corretta sarebbe stata allora piuttosto quella di prevedere nella delega – anziché la generica locuzione *"[...] l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice [...]"* – i criteri cui deve attenersi il giudice nel dettare tali limiti, inserendo tra questi la specifica indicazione del luogo assistito da tutela domiciliare nel quale viene autorizzata l'intercettazione e la specificazione delle ragioni che la giustificano, estendendo espressamente tali principi ad ogni tipologia di intercettazione, ivi incluse quelle tradizionali (che pure, di fatto, già sono necessariamente collegate ad un luogo predeterminato).

Se poi, come pare, il legislatore ha voluto in qualche modo cogliere le oggettive distanze che separano una qualunque associazione riconducibile alla fattispecie delineata dall'art. 416 c.p. da fenomeni di criminalità organizzata ben più pericolosi quali quelli di tipo mafioso o terroristico, in un'ottica di coerente ridefinizione del quadro normativo di riferimento, sarebbe stato meglio superare le timidezze cui si è accennato (ed è auspicabile che ciò avvenga nel corso dell'ulteriore esame cui sarà sottoposto il DDL al Senato) ed escludere del tutto l'ipotesi associativa semplice prevista dall'art. 416 c.p. dall'ambito di applicazione dell'art. 13 del D.L. 152/1991.

Come condivisibilmente affermato dal Procuratore Generale presso la Corte di Cassazione al punto n. 7 della memoria depositata nel procedimento Scurato, in rifermento alla disposizione da ultimo menzionata: "*Nella norma derogatoria è infatti prefigurato un peculiare e specifico bilanciamento di interessi nel cui ambio la segretezza delle comunicazioni e la tutela del domicilio subiscono più consistenti limitazioni in ragione della eccezionale gravità e pericolosità, per gli individui e o per l'intera collettività, dei reati dei quali si ricerca la prova*".

Il riferimento all'associazione per delinquere semplice in questa prospettiva appare del tutto improprio, ove si consideri che essa può costituirsi anche con la finalità di commettere reati di modesto allarme sociale e perfino procedibili a querela di parte.

Sempre in accordo con le ragioni espresse nella richiamata memoria del Procuratore Generale, certamente più corretto sarebbe limitare l'ambito di operatività dell'art. 13 del D.L. 152/1991 a quei reati di criminalità organizzata che effettivamente si connotano per essere di eccezionale gravità e pericolosità, quali sono le associazioni con finalità di terrorismo e di eversione dell'ordine democratico (art. 270 *bis* c.p.), le associazioni di tipo mafioso (art. 416 *bis* c.p.) e le associazioni finalizzate al traffico di sostanze stupefacenti (art. 74 D.P.R. 309/90).

Nella memoria si sosteneva, con apprezzabili argomentazioni, che tale dovesse essere, *de iure condito*, l'interpretazione da darsi alla nozione di criminalità organizzata.

L'ipotesi ermeneutica è stata, evidentemente, rigettata dalla Suprema Corte, che ha ritenuto di individuarla anche nel delitto di cui all'art. 416 c.p.; mutando però la prospettiva *de iure condendo,* poco importa quale tra le due sia l'interpretazione attualmente corretta, quanto piuttosto quale delle soluzioni si presenti come maggiormente rispettosa di quel criterio di "proporzionalità" che deve sussistere tra la "necessità democratica" di investigare che giustifica l'ingerenza dello Stato nella comunicazione privata del cittadino e la libertà che allo stesso deve essere garantita.

Appare fin troppo evidente che il regime delineato dal diritto vivente, dopo la sentenza "Scurato", non rispetti tale proporzione per due ordini di ragioni: consente l'intrusione in un numero indeterminabile di domicili che non hanno alcun collegamento con l'interesse investigativo; la consente per associazioni finalizzate alla commissione di qualunque reato, anche di modestissima gravità e pericolosità.

Nessuno dei due profili è stato adeguatamente affrontato e risolto dall'emendamento introdotto nel DDL S2027 e ciò dovrà, dunque, avvenire nel prossimo esame del testo nell'aula del Senato.

Vi è poi da attendersi che alcuni temi trattati dal DDL C3762, cui fa cenno anche la pronucia "Scurato" (punto 2.4. a cui si rimanda), possano essere recepiti attraverso un emendamento *ad hoc* nel testo del DDL "processo", estendendo l'ambito della disciplina dall'intercettazione di conversazioni tra presenti alle altre modalità acquisitive della prova che il captatatore consente (ampiamente descritte nei vari contributi che compongono questo "Focus").

Ogni asservazione a riguardo sarebbe prematura, atteso che il testo iniziale ha subìto modificazioni ed aggiustamenti e non è ancora nota la proposta nella sua ultima versione.

In ogni caso, v'è d'augurarsi che ciascun aspetto non solo venga trattato tenendo ben presenti i diversi punti di vista offerti da chi, a vario titolo, si pone a confronto con questo strumeno (così come si è cercato di fare di in questo scritto) – evitando così che il legiferare sia frutto delle ragioni di una sola "parte", o peggio di equivoci anche di natura tecnica – ma soprattutto che la linea guida sia quella di ricercare la necessaria proporzione tra interesse investigativo e libertà del cittadino, in un contesto nel quale il peso sempre crescecente della tecnologia rischia di comprimere quest'ultima fino ad annientarla.

Il rapporto Stato, tecnologia, cittadino e libertà non *è* (solo) la sfida del "Trojan horse", ma la sfida del futuro ed in questa prospettiva consapevole e responsabile va affrontata.