CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

DENTRO LE NOSTRE VITE: IL CAPTATORE INFORMATICO TROJAN HORSE COME ARCHETIPO DELL´0NNISCIENZA INVESTIGATIVA

Le vicende giudiziarie relative all´impiego dei moderni sistemi di captazione informatica mostrano come lo strumento tecnologico in questione si presti facilmente a degenerare in fenomeni di abuso, poco inclini al rispetto del delicato equilibrio tra le esigenze di tutela delle libertà fondamentali e le necessarie pratiche di contrasto ad attività di tipo criminale. Categorie criminologiche dal particolare allarme sociale hanno suscitato l´intervento del legislatore teso a disciplinare lo strumento senza contemperare le contrapposte esigenze in gioco , mediante contrappesi di tipo garantistico indispensabili in uno stato democratico.

di **Nicola Scerbo**
IUS/17 - DIRITTO PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Giovedì 3 Agosto 2023

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

The judical procedings relating to the use of modern IT systems show how the technological instruments in question lends itself easily to degenerate into phenomena of abuse, little inclined to respect the delicate belance between the need to protect fundamental frerdoms and necessary contractual practices to criminal phenomena. Criminological categories of particolar social alarm have aroused the intervention of the legistalor aimed at regulating the instrument without riconciling the opposing needs at skate, throught counterweights of a guarantee type indispensable in a democrate state.

Sommario: 1. Uno strumento costoso e poco controllato; 2. Il contesto normativo; 3. Il Trojan (captatore) come intrusione sproporzionata; 4. Un prima fase di assestamento normativo; 5. Il caso “Palamara” e la sua importanza mediatica; 6. Una breve ricognizione giurisprudenziale (Sezioni unite Scurato come architrave garantista); 7. Gli elementi di apertura (la criminilità organizzata come consolidato espediente giustificativo di massima); 8. lo stato dell'arte e le criticità per il futuro; 9. Conclusioni.

1. Uno strumento costoso e poco controllato Il tema delle intercettazioni ha rappresentato, fin dall'insorgenza della moderna tecnologia investigativa, un'annosa questione su cui dottrina, giurisprudenza ed addetti ai lavori tutti hanno posto la loro attenzione. Fiumi di letteratura sono rinvenibili in ogni rivista specializzata, ma, il punto di fondo di ciascun intervento, ha come chiave di volta la considerazione dei potenziali pericoli legati ad un uso improprio dello strumento, oggetto non solo di apprensione in merito alle capacità tecniche di accesso ad aspetti estremamente riservati della vita privata di ciascun individuo, ma, piuttosto, alle caratteristiche di estrema malleabilità e vulnerabilità ad agenti esterni od eterointegrazioni personalistiche.

In una recente esposizione, il Copasir, dopo aver analizzato la relazione della sezione centrale per il controllo sui contratti secretati della Corte dei conti, ha evidenziato come esista una «zona grigia di atti che le amministrazioni degli enti non inviano alla sezione in nessuna fase del controllo. I contratti senza visto e registrazione della sezione non sono efficaci, ma la sezione stessa non dispone di poteri che possano far emergere ciò che non viene a sua conoscenza».

Nel 2020 risultano registrati alla Corte dei conti quattro contratti di noleggio per sistemi di intercettazione. Come indicato anche dal Copasir, si tratta di un dato in contrasto con «la poderosa attività delle procure in merito all'impiego di sistemi di intercettazione, che vede l'ordinamento italiano tra i maggiori utilizzatori di tali strumenti».

CamminoDiritto.it
ISSN 2421-7123

Come stabilito dalla recente riforma orlando dedicata al tema delle intercettazioni, è prevista una disciplina tariffaria sui servizi erogati dai fornitori privati dei sistemi di intercettazione, mediante lo strumento normativo dei decreti ministeriali. Il decreto legislativo del 2018 ha, ulteriormente, definito la questione relativa all'inserimento delle spese di intercettazioni tra le spese generali di giustizia, adeguandosi alla disciplina contenuta nel teso unico del 2002.

A conti fatti, il conferimento di incarico diretto da parte del P.M. in modo diretto ad un soggetto privato, nell'ambito di un procedimento specifico, rientra tra le spese di giustizia [1]. L'approfondimento del Copasir si è posto come obiettivo fondamentale quello di «individuare gli strumenti normativi più idonei alla tutela informativa del paese». Secondo il Copasir, infatti, serve «una valorizzazione di apposite linee guida tra le aziende coinvolte e gli uffici giudiziari competenti, sull'esempio di alcune Procure italiane, per il corretto impiego delle strumentazioni volte ad attività di intercettazione e captazione»[2].

Il caso Exodus[3], un software di captazione impiegato da varie procure, il cui discutibile uso è stato oggetto di indagine da parte della procura di Napoli, ha spinto il comitato ad occuparsi delle criticità sul tema. Le scarse garanzie di sicurezza emerse nel corso delle indagini in merito a gestione e conservazione dei dati da parte del sistema in questione, hanno manifestato la sua inidoneità a garantire adeguati parametri di segretezza ed integrità[4].

Exodus non era altro che un malware di captazione introdotto nei sistemi di comunicazione dei soggetti sottoposti alle indagini, mediante un espediente tecnico in due steps. In pratica, dopo aver effettuato una operazione di download di applicazioni commerciali standard per ottenimento di agevolazioni sui piani tariffari delle utenze telefoniche, l'utente introduceva il virus nei suoi sistemi informatici[5].

L'evento in questione ha generato la risposta di opinione pubblica e politica, tanto da generare l'emanazione del decreto-legge 30 dicembre 2019 n. 161**,** recante “modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni”, c.d. “decreto Bonafede”.

2. Il contesto normativo

Il provvedimento ha introdotto importanti modifiche alle norme previste dal codice di procedura penale, già novellate ai tempi della riforma orlando, riguardanti soprattutto modalità di esecuzione e conservazione delle intercettazioni, introducendo la possibilità di

CamminoDiritto.it
ISSN 2421-7123

impiego del "captatore informatico"(trojan horse) anche per reati contro la pubblica amministrazione da parte di pubblici ufficiali ed incaricati di pubblico servizio, legittimando e normando l'impiego di uno strumento fino all'epoca incerto nelle modalità e nei confidi tanto da essere ritenuto, in passato, uno strumento atipico di ricerca della prova.

Nel nuovo art. 267 del c.p.p, comma 2 bis. si può leggere che «il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater[6] e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni...».

Dunque, una vera e propria estensione dei margini di applicabilità dello strumento a categorie di soggetti non rientranti, formalmente, nelle maglie dell'attività della criminalità organizzata, caratterizzata, pertanto, da un gradiente di offensività nettamente superiore. L'uso del trojan si traduce concretamente nell'inserimento di un virus all'interno del dispositivo del soggetto sottoposto alle indagini, i cui requisiti tecnici sono stabiliti con decreto ministeriale.

Nel verbale delle operazioni di indagini dovrebbe essere indicata anche la tipologia di software (programma specifico) impiegato. Come disposto al comma 3 dell'art. 267 «Il decreto del pubblico ministero che dispone l'intercettazione indica le modalità e la durata delle operazioni. Tale durata non può superare i quindici giorni, ma può essere prorogata dal giudice con decreto motivato per periodi successivi di quindici giorni, qualora permangano i presupposti indicati nel comma 1».

A differenza dei presupposti necessari per procedere alla richiesta di acquisizione dei tabulati telefonici, o anche detti dati esterni al traffico telefonico, nel caso di impiego del captatore, così come avviene nel caso delle intercettazioni previste dall'art. 266 c.p.p., il presupposto richiesto, oltre ai requisiti qualitativi e quantitativi sul tipo di reato[7], è l'esistenza di gravi indizi di reato, nonché, l'indispensabilità dello strumento ai fini della prosecuzione delle indagini.

Il decreto che dispone l'impiego dello strumento« indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonché, se si procede per delitti diversi da quelli di cui all'articolo 51 commi 3-bis e 3-quater, e dai delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4, i luoghi e il tempo, anche indirettamente determinati, in relazione ai

CamminoDiritto.it
ISSN 2421-7123

quali è consentita l'attivazione del microfono»[8].

Anche in questo caso è prevista la possibilità di una disposizione di urgenza, con decreto motivato da parte del P.M. nei casi che comportino grave pregiudizio alle indagini. Il decreto necessita comunque di convalida del G.I.P. Nelle successive 24 ore. Le comunicazioni intercettate finiscono nel c.d. "Archivio digitale", in cui deve essere assicurata l'integrità di quanto intercettato, registrato e trasmesso.

Nel caso in cui non sia possibile un trasferimento contestuale di tali contenuti all'interno dell'archivio, le ragioni di tale impedimento devono essere riportate nel verbale delle operazioni compiute dalla polizia giudiziaria, al termine delle quali, il captatore deve essere disattivato con modalità di esecuzione adeguate a renderlo inidoneo per ulteriori utilizzi. Inoltre, il P.M. «Il pubblico ministero dà indicazioni e vigila affinché nei verbali non siano riportate espressioni lesive della reputazione delle persone o quelle che riguardano dati personali definiti sensibili dalla legge, salvo che risultino rilevanti ai fini delle indagini»[9].

Per garantire l'immediatezza, i verbali vengono «trasmessi al pubblico ministero per la conservazione nell'archivio di cui all'articolo 269, comma 1. Entro cinque giorni dalla conclusione delle operazioni, essi sono depositati presso l'archivio di cui all'articolo 269 comma 1, insieme ai decreti che hanno disposto, autorizzato, convalidato o prorogato l'intercettazione, rimanendovi per il tempo fissato dal pubblico ministero, salvo che il giudice non riconosca necessaria una proroga»[10].

Ai difensori è dato avviso che, entro il termine fissato dal Pm, per via telematica, hanno facoltà di esaminare gli atti e ascoltare le registrazioni o di prendere cognizione dei flussi di comunicazioni informatiche o telematiche presenti nell'archivio digitale. «Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione e di quelli che riguardano categorie particolari di dati personali, sempre che non ne sia dimostrata la rilevanza. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima»[11].

I difensori possono estrarre anche delle copie delle trascrizioni effettuate o fare eseguire la trasposizione della registrazione su supporto idoneo. In caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono richiedere copia dei flussi intercettati, ovvero copia della stampa[12].

L'attività del G.I.P. si traduce nel disporre la «trascrizione integrale delle registrazioni

CamminoDiritto.it
ISSN 2421-7123

ovvero la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento. Il giudice, con il consenso delle parti, può disporre l'utilizzazione delle trascrizioni delle registrazioni ovvero delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche effettuate dalla polizia giudiziaria nel corso delle indagini»[13].

Come anticipato, il vecchio archivio del pubblico ministero, con la novella contenuta nella disciplina del decreto Bonafede, è sostituito da un archivio digitale sottoposto a controllo e direzione dell'ufficio del procuratore della repubblica.

La gestione deve avvenire garantendo il requisito specifico della segretezza della documentazione in esso contenuto, afferente sia al materiale diretto sulle attività di intercettazione, quanto a contenuti ritenuti irrilevanti o di cui è vietata l'utilizzazione[14] o, a maggior ragione, riguardanti particolari categorie di dati sensibili. I soggetti autorizzati ad accedere all'archivio sono il giudice procedente ed eventualmente i suoi ausiliari, il P.M. ed i suoi ausiliari, inclusi gli ufficiali di polizia giudiziaria delegati all'attività materiale di ascolto, nonché difensori, assistiti e, eventualmente, interpreti.

Le registrazioni effettuate possono essere conservate fino a sentenza non soggetta a impugnazione, ma gli interessati, quando la documentazione non è più necessaria per il procedimento, possono chiederne la distruzione, a tutela della riservatezza, al giudice che ha autorizzato o convalidato l'intercettazione[15].

Come indicato dall'art. 271 al comma 1-bis «non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo».

3. Il trojan (captatore) come intrusione sproporzionata

In un recente articolo apparso sul quotidiano “il Dubbio”, in cui viene riportata l'intervista del costituzionalista Marini all'agenzia Adn kronos, lo stesso sostiene che si debba limitare l'uso del trojan horse ai casi «assolutamente eccezionali»[16].

Secondo il Professore di Diritto pubblico all’Università di Roma Tor Vergata, il captatore informatico «incide in modo troppo invasivo sulla vita privata di tutti i cittadini, ledendo la riservatezza delle comunicazioni personali sancita dall’articolo 15 della Carta

CamminoDiritto.it
ISSN 2421-7123

costituzionale. È assolutamente necessario trovare un nuovo e più equilibrato bilanciamento tra i valori costituzionali che vengono in rilievo, potenziando i limiti giuridici all'uso del trojan; il suo utilizzo deve essere assolutamente eccezionale. Oggi la segretezza delle comunicazioni rischia di essere gravemente compromessa e nessuno, pur non avendo commesso illeciti, può escludere di non essere intercettato. Gli stessi giustizialisti sono i primi ad esserne consapevoli e ne subiscono le conseguenze».

Uno dei principali vulnus dell'impianto normativo attuale, secondo Marini, risiede nella cornice dei reati per i quali è possibile procedere all'uso del trojan, senza distinzione tra quelli di terrorismo e mafia e quelli contro la pubblica amministrazione compiuti da pubblici ufficiali o incaricati di pubblico servizio. Altre criticità individuate dal costituzionalista riguardano l'uso indiscriminato dello strumento e la necessità di ampliare le garanzie processuali, «prevedendo il coinvolgimento di un organo collegiale».

Il principale errore degli addetti ai lavori ricorrerebbe nell'impiego dello strumento non come elemento di conferma ad elementi indiziari già acquisiti durante le indagini, ma come strumento di ricerca dei reati ex novo.

Nel caso in cui il magistrato dovesse autorizzare un uso improprio del captatore, «sarebbe necessario un approccio più garantista dato che si incide sui diritti fondamentali della persona. Tra l'altro, andrebbero risarciti effettivamente i soggetti oggetto di intercettazioni e che poi vengono assolti. Mentre l'ordinamento oggi non garantisce un risarcimento adeguato, che dovrebbe consistere non solo in un totale ristoro delle spese di giustizia, ma anche di tutti gli effetti dannosi all'immagine e personali che l'uso del trojan ha prodotto».

D'altro canto, da almeno un decennio, le intercettazioni sono il mezzo di ricerca della prova per eccellenza, esplicandosi nell'acquisizione occulta del materiale di comunicazione o conversazione tra soggetti, anche di tipo informatico o telematico. In pratica, le operazioni consistono nell'invasione della sfera privata del cittadino in deroga a quanto sancito dall'art. 15 della costituzione[17].

L'ordinamento processual-penalistico italiano prevede una suddivisione a due delle categorie di intercettazioni: da un lato, le intercettazioni di conversazioni o comunicazioni telefoniche, informatiche o telematiche[18], dall'altro le c.d. "intercettazioni ambientali" [19].

Nel primo caso, emerge la possibilità per gli inquirenti di captare, anche con software appositi, le comunicazioni e le conversazioni effettuate mediante telefono, fisso o mobile ed i flussi di comunicazioni e dati trasmessi per via telematica e informatica. Per le seconde, invece, bisogna distinguere le comunicazioni tra presenti da quelle aventi ad

CamminoDiritto.it
ISSN 2421-7123

oggetto conversazioni, sempre tra presenti, le quali, però, si svolgono nei luoghi di privata dimora[20].

In tal caso, alla riserva di legge e di giurisdizione, l'esistenza dei gravi indizi di reato e dell'assoluta indispensabilità alla prosecuzione delle indagini, si aggiunge l'ulteriore requisito del fondato motivo di ritenere che nel luogo di privata dimora si stia svolgendo l'attività criminosa. (c.d. "captazione domiciliare").

Come noto, la fase delle indagini preliminari ha subito il condizionamento dell'evoluzione tecnologica e digitale, in cui, il captatore, ha giocato un ruolo determinante nelle procedure di acquisizione di dati a distanza mediante comandi di archiviazione nei server collegati.

Diversamente da altre tipologie di strumenti di ricerca della prova, il trojan consente agli inquirenti un notevole ventaglio di opzioni intrusive come l'accesso ai dati ed eventualmente una copia degli stessi, memorizzati nel dispositivo del soggetto sottoposto alle indagini.E', inoltre, possibile avviare la registrazione del traffico dati in arrivo o in partenza, la registrazione di telefonate e videochiamate, nonché, sempre a distanza, l'attivazione delle funzioni di microfono e/o telecamera indipendentemente dalla volontà dell'utente coinvolto.

Di fatto, quello che avviene è una replicazione dell'apparato strumentale nelle mani degli operatori investigativi, in cui, attraverso il meccanismo della registrazione di tutto ciò che avviene entro un certo raggio di azione, è possibile sfruttare le tendenziali abitudini del soggetto di avere sempre con sé l'apparato digitale in questione.

La caratteristica dinamica del trojan, nonché la sua principale criticità di impiego, risiede nella generale tendenza ad una acquisizione massiva ed indeterminata di dati personali e sensibili, di cui, anche se significativa, solo una parte diverrà materiale probatorio utile alle indagini o nella successiva fase dibattimentale. Si evince come gli interessi in gioco siano molteplici, generando un conflitto tra l'esigenza di tutela della riservatezza nella sfera privata del cittadino e la necessità di contrasto ad attività criminose di particolare interesse.

La suprema Corte[21], chiamata ad esprimersi sui limiti e presupposti dell'utilizzo del captatore, ha ritenuto di escluderne l'impiego ai fenomeni di criminalità ordinaria, riservandola solo per azione di criminalità organizzata. Sempre secondo la Corte, l'impiego di captatori, per i quali sia tecnicamente impossibile predeterminare gli ambienti dove le registrazioni avranno luogo, deve ritenersi legittimo solo per fattispecie previste dalla legge speciale D.L. 13 maggio 1991, n. 152, contenente "provvedimenti

CamminoDiritto.it
ISSN 2421-7123

urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa"[22].

La Corte ha, però, tralasciato di esprimersi su aspetti rilevanti legati all'uso di videocamera, all' analisi dell'hard disk e al key-logger[23].

Si tratta, infatti, di una serie di attività potenzialmente idonee ad incidere in maniera significativa sul diritto alla riservatezza del soggetto sottoposto ad indagine, o di colui che, anche del tutto estraneo ai fatti, potrebbe utilizzare lo strumento informatico sottoposto ad attività investigativa per finalità meramente personali.

4. Una prima fase di assestamento normativo

La legge di conversione L. 25 giugno 2020, n. 70 del decreto Bonafede, ha introdotto una serie di criteri temporali per la successione delle leggi nel tempo, necessari a disciplinare l'impiego del captatore a seconda del momento in cui si è provveduto all'iscrizione nel registro delle notizie di reato.

Così, gli esiti del software di captazione potranno essere utilizzati per i procedimenti riguardanti attività della criminalità organizzata iscritti prima dell'1 settembre 2020, mentre per i procedimenti iscritti successivamente dovrà porsi la distinzione tra reati previsti dall'art. 51, cc. 3-bis[24] e 3-quater del c.p.p., i reati con pena massima non inferiore a cinque anni commessi da pubblici ufficiali o incaricati di pubblico servizio ed i reati comuni.

Ai reati di mafia continuerà ad applicarsi l'art. 13 del D.L. 13 maggio 1991, n. 152[25]. Nel caso in cui si stia procedendo contro uno dei delitti commessi da pubblici ufficiali od incaricati di pubblico servizio, la nuova disciplina prevede la possibilità di impiegare il captatore informatico nei luoghi previsti dall'art. 614 c.p. [26].

Nel caso dei reati comuni, invece, la condizione esclusiva di impiego al di fuori delle private dimore, riconosce la deroga di un fondato motivo che evidenzi lo svolgimento dell'attività criminosa al loro interno, ritenendo sufficiente elemento di tutela la possibilità predeterminata che il malware introdotto nel sistema possa essere disattivato a distanza in tali circostanze.

Come elemento ulteriore, ma non di poco conto, la nuova disciplina prevede la possibilità di utilizzare i risultati delle attività di captazione anche per il perseguimento di reati diversi da quello per cui si è proceduto, contraddicendo, così, il principio stabilito dalle

CamminoDiritto.it
ISSN 2421-7123

sezioni unite Cavallo[27].

5. Il caso "Palamara" e la sua importanza mediatica

Uno degli esempi più significati legati all'uso del captatore informatico ed alle sue criticità, riguarda il caso Palamara.

Il fatto di cronaca giudiziaria, nonostante la portata delle conseguenze sui vertici della magistratura e i suoi risvolti politici nella discussione inerente le dinamiche relative alle nomine del Consiglio superiore, ha avuto, comunque, il merito di rendere fruibile all'opinione pubblica il dibattito, un tempo riservato ad una ristretta cerchia di addetti ai lavori, sui potenziali abusi e deviazioni degli strumenti di indagine di nuova concezione tecnologica.

L'ampio utilizzo del trojan horse nelle vicende riguardanti il noto magistrato, ha condotto buona parte degli agenti interessati alla vicenda ad interrogarsi sulla pervasività di simili programmi informatici. Professionisti ed esperti del settore, un tempo, nelle loro argomentazioni critiche, considerati individui quasi mitologici relegati ai margini degli eventi, hanno improvvisamente visto emergere un consistente interesse su argomenti di notevole importanza per gli aspetti più sensibili della vita di ciascun individuo.

Tramite l'espediente amplificatore della comunicazione mediatica su un fatto di cronaca, l'attenzione dello spettatore si è concentrata non più sul motivo primario delle attività di indagini, ovvero la ricerca della prova di un malaffare generale nei vertici del potere, quanto sullo strumento impiegato nell'attività svolta dagli investigatori. Fin da subito è risultato evidente come l'uso del trojan horse abbia rappresentato il principale mezzo di acquisizione della prova, da cui ne è derivato l'intero impianto accusatorio.

Senza entrare nel merito della vicenda, di cui in questa sede interessa relativamente poco, è indispensabile indirizzare il ragionamento sugli elementi afferenti alle criticità sorte nelle procedure di acquisizione dei dati oggetto di indagine mediante captatore, nonché alla loro gestione in capo agli uffici delle procure coinvolte, laddove sono emerse evidenti incongruenze e rischi di interferenza illecita sulla genuinità e qualità degli elementi probatori acquisiti.

Lo stesso Antonello Soro, in qualità di presidente dell'Autorità Garante nella prefazione alla "Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico" non manca di indicare le sue perplessità sull'uso dei captatori, alla luce delle notizie di cronaca relativi al già citato caso exodus.

CamminoDiritto.it
ISSN 2421-7123

Come egli scrive, i «Recenti avvenimenti, descritti anche dagli organi di informazione, hanno infatti dimostrato i rischi suscettibili di derivare dal ricorso, a fini investigativi, da parte delle società incaricate, a determinati software le cui peculiari caratteristiche meriterebbero, a nostro avviso, una disciplina specifica. Ci si riferisce, in particolare, a programmi informatici connessi ad app, non direttamente inoculati, quindi, nel solo dispositivo dell'indagato, ma posti su piattaforme (come Google play store) accessibili a tutti. Ove rese disponibili sul mercato, anche solo per errore in assenza dei filtri necessari a limitarne l'acquisizione da parte dei terzi - come parrebbe avvenuto nei casi noti alle cronache - queste app-spia rischierebbero di trasformarsi in pericolosi strumenti di sorveglianza massiva. Appare, dunque, opportuna una riflessione in ordine ai limiti di utilizzo di questi software a fini intercettativi, valutando anche la possibilità di un divieto o, in subordine, dell'adozione di ulteriori, specifiche cautele. L'esame di tale questione è utile, anche, per una più ampia riflessione su alcuni possibili miglioramenti della disciplina delle intercettazioni, che sottoponiamo all'attenzione del Governo e del Parlamento»[28].

In realtà, gli appelli del garante, come si può evincere anche dal testo completo della segnalazione, alla luce dei fatti avvenuti nel caso Palamara, non hanno generato gli effetti di tutela sperati, anzi, per una qualche eterogenesi dei fini, si è realizzato potenzialmente l'effetto distorsivo di cui si temevano le ripercussioni sulle tutele processuali dello stato di diritto.

Come emerso dalle cronache giudiziarie, la difesa del magistrato, nel corso delle fasi processuali, ha sollevato l'ipotesi molto verosimile che i dati captati sul cellulare del soggetto indagato mediante il software spia siano, in realtà, transitati da un server "occulto", la cui collocazione è stata individuata a Napoli, prima di terminare il loro viaggio digitale su quello installato presso la procura di Roma, messo a disposizione della Guardia di finanza cui erano state affidate le attività di indagini, ufficialmente unico autorizzato a ricevere i dati derivanti dall'attività investigativa.

Il fatto, nei suoi contorni essenziali, è stato in un primo momento ammesso anche dall'ingegnere della società Rcs, fornitrice del software di captazione e, successivamente, confermato dall'ispezione disposta dalle procure di Firenze e di Napoli, in seguito alla quale è emerso come la società si servisse, inizialmente, di «un sistema fondato su un unico server centrale che faceva transitare i dati su quelli periferici attraverso internet, salvo poi optare, tra agosto e settembre 2019, per un sistema decentralizzato, con server nelle singole procure, attraverso un sistema di cifratura rinforzato.

Il tutto dopo un misterioso trasferimento dei server da un palazzo all'altro del centro direzionale, fin dentro la procura di Napoli, all'oscuro di qualsiasi manovra»[29].

CamminoDiritto.it
ISSN 2421-7123

Secondo la testimonianza dell'ispettore di polizia postale F.S. non era da escludere «la possibilità che le attività siano continuate» oltre il termine previsto dal decreto che disponeva l'impiego del captatore. Il difensore del magistrato ha inoltre evidenziato che «Potrebbe esserci stata un'indicazione di registrazione, ovvero che il trojan comunicava di essere ancora vivo e presente all'interno del telefono del dottor Palamara».

Il procuratore della repubblica di Perugia, competente sul caso in questione, ha sottolineato come per gli inquirenti l'uso del software sia ritenuto «legittimo, rituale, rispettando i criteri», in quanto, anche se digitalmente la registrazione è transitata da un server sconosciuto, è comunque avvenuta su di un hardware posizionato in una procura della Repubblica.

Dall'ispezione effettuata ad opera del Cnaipic (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche[30]) è emerso, però, come vi sia stata una modifica improvvisa dell'architettura del sistema, tra agosto e settembre 2019, su decisione del management aziendale. Prima della data in questione il sistema di captazione aveva delle caratteristiche centralizzate con server unico di Css ed Hdm installato a Napoli, al servizio dell'intero territorio nazionale, più alcuni server di Ivs decentrati presso le singole procure dislocate sul territorio.

Dopo, invece, è avvenuto il cambiamento con passaggio a più server Css, uno per ogni procura, senza che si rendesse più necessaria la procedura di smistamento dei dati verso gli Ivs per il tramite del server Hdm centralizzato. E in mezzo a questi cambiamenti si è registrato il trasferimento dei server oggetto della contestazione della difesa di Palamara.

La differenza tecnica dei due sistemi di acquisizione dei dati e di gestione della procedura di captazione sta nella circostanza per cui nel primo caso, il server Css "istruisce" il trojan che poi "restituisce" i dati al server attraverso un canale cifrato. Dall'ispezione, è emerso, però, come tale procedura non garantisca «univocamente che un determinato dato non possa esser stato modificato».

Dunque, i dati oggetto di acquisizione vengono in un primo momento inviati in modo frazionato, salvo essere riconvertiti successivamente in formato unico dal server Css e trasferiti mediante ip privato al server Hdm. Al termine della complessa procedura eseguita dal sistema, i dati subiscono la cancellazione automatica ad opera del software. Il secondo sistema, molto più immediato, prevede il trasferimento dei dati direttamente al server terminale, installato negli uffici delle singole procure, con la copertura delle cartelle cifrate[31].

CamminoDiritto.it
ISSN 2421-7123

Nella pratica, tutto ciò si traduce nella circostanza per cui i dati derivanti dalle attività di intercettazione mediante captatore, non sarebbero transitati direttamente dal luogo di collocazione del device sottoposto alle operazioni di indagini al server della Procura competente ad indagare, nel caso in oggetto, quella di Roma, ma gli stessi, invece, sarebbero transitati prima di tale decisivo passaggio presso dei server collocati a Napoli, verosimilmente presso la Procura della Repubblica. Lì, sarebbero rimasti a disposizione degli amministratori di sistema della società Rcs, fornitrice del sistema informatico.

Aspetto ancora più rilevante della vicenda, sembrerebbe che dai server collocati a Napoli siano transitati i dati delle intercettazioni delle Procure in tutta Italia che avevano dato affidamento di gestione ad Rcs. Come evidenziato anche dall'avvocato Massimo Borgobello su "agenda digitale", «sotto il profilo strettamente giuridico, la presenza di un server occulto può determinare l'inutilizzabilità in giudizio delle conversazioni captate in sede di indagine.

Questo vale per tutte le indagini in cui l'incarico è stato affidato ad Rcs, da qualunque parte d'Italia: sotto questo profilo molte inchieste sono a rischio, con i relativi processi. Il problema è che saranno necessarie perizie di parte, verosimilmente costosissime, per effettuare una verifica seria di quanto accaduto. Dalla vicenda emerge una evidente violazione della Direttiva UE 16/680 e delle norme di recepimento inserite nel Decreto legislativo 51 del 2018»[32].

Sempre secondo Borgobello, «non è accettabile che in un Paese in cui si richiedono standard elevati in materia di protezione dei dati alle aziende, sia possibile intercettare e gestire i relativi dati con il modello ante GDPR, improntato ad una sostanziale conservazione dei risultati delle indagini anche in violazione di alcune normative. La violazione di non tutte le norme, infatti, determina l'inutilizzabilità dei risultati delle intercettazioni: la Cassazione ha spesso forzato il testo del Codice per "salvare" indagini effettuate in modo irrituale. le intercettazioni e la giustizia penale, in generale, sono un elemento da cui si misura il grado di maturità di una democrazia e del suo ordinamento giuridico: i retaggi dello stato di polizia e del processo inquisitorio sono ancora molti forti in Italia».

6. Una breve ricognizione giurisprudenziale (Sezioni unite Scurato come architrave garantista)

Un risposta emblematica sulla natura intrusiva dello strumento in questione è rinvenibile nella Sezione unite Scurato, laddove gli ermellini avevano già rilevato la natura intrusiva del captatore sottolineando per l'appunto come "Uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente: a) di captare tutto il traffico dati

CamminoDiritto.it
ISSN 2421-7123

in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia web mail, che outlook); b) di attivare il microfono e, dunque, di apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi; c) di mettere in funzione la web camera, permettendo di carpire le immagini; d) di perquisire l'hard disk e di fare copia, totale o parziale, delle unità di memoria del sistema informatica preso di mira; e) di decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (keylogger) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (screenshot); f) di sfuggire agli antivirus in commercio. I dati raccolti sono trasmessi, per mezzo della rete internet, in tempo reale o ad intervalli prestabiliti ad altro sistema informatico in uso agli investigatori." [33].

Nella sentenza della cassazione Sez. IV, n. 32428 del 24.9.2020, la Corte, invece si distingue per una scarsa sensibilità al tema del rispetto delle libertà fondamentali, quali la libertà del domicilio e la riservatezza delle comunicazioni, allineandosi all'indirizzo giurisprudenziale per cui il captatore è considerato una modalità differente di intercettazione.

Nonostante la pronuncia si occupi di molti aspetti legati all'uso del sistema, la stessa riconduce la risoluzione degli aspetti critici alla salvaguardia dei risultati raccolti mediante l'indagine. Più nello specifico, per quanto attiene al difetto di motivazione dei decreti autorizzativi, nel caso di specie, trattandosi di fatti di criminalità organizzata, non doveva essere motivata una "assoluta indispensabilità per la prosecuzione delle indagini" ma una semplice "necessità per lo svolgimento".

Dalla sentenza emerge, inoltre, la legittimità della sovrapposizione di operazioni investigative mediante l'uso del trojan ad altre già in corso, mediante strumenti tradizionali di intercettazione delle conversazioni telefoniche e tra presenti, sulla base del fatto che "la disposizione di un diverso decreto di intercettazione sul medesimo bersaglio/dispositivo elettronico colpito dalle investigazioni, motivata dalla necessità di far ricorso, per ragioni investigative, allo strumento di captazione informatica sviluppato tramite virus trojan, configura, un nuovo ed autonomo mezzo di ricerca della prova, perfettamente legittimo in presenza del rispetto dei presupposti di legge per la sua autorizzazione, che non presenta interferenze con le intercettazioni telefoniche e/o ambientali già disposte con i mezzi ordinari, pur se l'oggetto sul quale sono stati installati i captatori informatici coincide con quello su cui sono state disposte altre intercettazioni" [34].

Le conclusioni della sentenza riportano all'assunto per cui la legittima sostituzione con intercettazioni mediante captatore informatico a quelle tramite strumenti ordinari, anche sovrapposte nei tempi e termini di autorizzazione, discende dalla loro differente natura. Il

CamminoDiritto.it
ISSN 2421-7123

trojan sarebbe più pervasivo, avendo, infatti, ad oggetto flussi informativi complessi riguardanti un determinato target oggetto di indagini, avendo come finalità il raggiungimento dell'acquisizione e registrazione di conversazioni, messaggi e qualsiasi altra informazione differente rispetto a quelle captate tramite gli strumenti di intercettazione ordinari.

Un tema affrontato nella sentenza in questione, seppur per un caso diverso, riguarda anche la Società privata Rcs, fornitrice dei sistemi di intercettazione.

Sulla base delle censure mosse dalla difesa, circa la mancata precisione dei decreti autorizzativi contenenti le indicazioni sull'assistenza del personale fornito dalla società alle attività di inserimento del trojan svolte dalla polizia giudiziaria, nonché, l'incertezza, generata dall'assenza di una puntuale e precisa documentazione di verbalizzazione delle operazioni di indagine effettuate, senza indicazione delle concrete modalità attuative dell'operazione di intercettazione con il captatore realizzate materialmente dal personale privato delegato.

La corte, nel rispondere a tali eccezioni, seguendo le linee delle Sezioni unite Scurato, conclude per una omogeneità od assimilazione delle intercettazioni standard a quelle svolte mediante uso del captatore e che da tale considerazione ne deriverebbe l'assunto per cui le operazioni prodromiche di installazione del software nel dispositivo del soggetto sottoposto ad indagine debbano considerarsi autorizzate insieme al provvedimento che dispone l'attività di intercettazione[35].

Se ne ricava il principio per cui, essendo lo strumento delle intercettazioni un mezzo di ricerca della prova necessario all'accertamento di gravi forme di criminalità, i diritti di inviolabilità del domicilio e segretezza della corrispondenza tutelati rispettivamente dagli art. 14 e 15 Cost., debbano coordinarsi con il più generico interesse collettivo alla pubblica sicurezza ricompreso nell' obbligatorietà dell'azione penale ex art. 112 Cost., subendone, inevitabilmente, la compressione, seppur temporanea[36].

Ulteriore precisazione attiene alle operazioni di installazione o disinstallazione del software spia operate dalla polizia giudiziaria; la pronuncia in questione, infatti, aggiunge si tratta di "atti materiali rimessi alla contingente valutazione della polizia giudiziaria, non essendo compito del pubblico ministero indicare le modalità dell'intrusione negli ambiti e luoghi privati ove verrà svolta l'intercettazione" e che "l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali"[37].

Dalla sentenza se ne ricava che l'atto di autorizzazione delle operazioni "rende superflua

CamminoDiritto.it
ISSN 2421-7123

l'indicazione delle modalità da seguire nell'espletamento dell'attività materiale e tecnica da parte della polizia giudiziaria, mentre la prova delle operazioni compiute nel luogo e nei tempi indicati dal giudice stesso e dal pubblico ministero è offerta dalla registrazione delle conversazioni intercettate"[38].

Nel suo saggio sulla rivista Penale, diritto e procedura, Leonardo Filippi riassume molto bene i principi stabiliti dalla Corte: «a) le questioni relative all'installazione degli strumenti tecnici per l'intercettazione, come il virus trojan, in relazione all'obiettivo da intercettare, non attengono alla fase autorizzativa dell'attività investigativa demandata al giudice per le indagini preliminari, né alla verifica dei presupposti di legittimità delle intercettazioni, bensì alla fase esecutiva, già coperta dall'autorizzazione a disporre le stesse intercettazioni; b) la fase esecutiva è consegnata alle prerogative del pubblico ministero che può delegare la polizia giudiziaria alle operazioni materiali di installazione tecnica degli strumenti (software, hardware, trojan) idonee a dar vita, in concreto, alle intercettazioni e addirittura ci si spinge ad affermare che eventuali modifiche degli strumenti già indicati nel decreto autorizzativo del G.I.P. come quelli da utilizzare per eseguire le captazioni possono essere disposte dallo stesso pubblico ministero; c) le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni, anche tramite virus trojan, costituiscono atti materiali rimessi alla contingente valutazione della polizia giudiziaria e l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali»[39].

In buona sostanza, come specificato dallo stesso Filippi, le modalità di installazione del trojan non interessano al giudice, in quanto fase esecutiva demandata al pubblico ministero che può (nella maggior parte dei casi è così) delegare le attività materiali di intercettazioni alla polizia giudiziaria, la quale, avendo una sorta di licenza generale nelle modalità gestionali di tali operazioni, discostandosi anche dal contenuto del provvedimento di autorizzazione del giudice, potrebbe anche omettere qualsiasi verbalizzazione delle operazioni, in virtù dell'irrilevanza processuale di simili omissioni.

Da ciò ne deriverebbe come libertà domiciliare e segretezza delle comunicazioni siano banalmente affidate alla discrezionalità della polizia giudiziaria, la quale, in tal modo, avrebbe riservato un "pieno e incontrollabile" potere di impiegare qualsivoglia modalità operativa di intercettazione senza che giudice e il P.M. sappiano, volutamente o meno, se si è proceduto in modo legittimo.

Qui ritorna in soccorso il noto caso Palamara. Infatti, come emerso anche dalle notizie di cronaca, nei primi falliti tentativi di installazione del software spia sul device del soggetto, dovuti al rifiuto dell'indagato stesso di ricevere mail o messaggi da cui, inevitabilmente,

CamminoDiritto.it
ISSN 2421-7123

sarebbe derivata la creazione della backdoor di accesso per gli inquirenti, all'insaputa del G.I.P., che aveva autorizzato col suo provvedimento le operazioni di intercettazione col captatore, però, il pubblico ministero ordinò alla polizia giudiziaria incaricata delle operazioni materiali di bloccare le telefonate in uscita dal cellulare, costringendo, così, lo stesso Palamara, dopo diversi tentativi di risoluzione di quello che poteva apparire come un semplice guasto del device, al reset del sistema per superare l'inconveniente e conseguentemente ad accettare a sua insaputa l'accesso del trojan horse nel suo dispositivo.

Dall'analisi della vicenda ne deriva il ragionamento per cui, oltre alla pericolosità implicita dello strumento di indagine, dovuta alla sua struttura tecnica, si aggiunge l'elemento di notevole incertezza nelle modalità di gestione delle procedure di inserimento, captazione e disinstallazione del software spia, nella maggior parte dei casi, in mano all'arbitrio della polizia giudiziaria e, perciò, sconosciute agli organi giudiziari di direzione e controllo delle indagini, nonché, delle riserve difensive.

Inutile ribadire quanto ciò contrasti con i principi democratici dello stato di diritto nell'ottica di una tutela delle principali garanzie difensive nel processo penale. Come emerso anche nella recente "Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico" del Garante per la protezione dei dati personali: «l'utilizzo a fini intercettativi in sede giudiziaria, dei captatori informatici è una misura indubbiamente utile alla luce dell'evoluzione delle tecnologie disponibili.

Esso consente, infatti, di prescindere dall'installazione fisica dei dispositivi di captazione per realizzare intercettazioni di comunicazioni e conversazioni tra presenti, inoculando direttamente nel dispositivo-ospite il software-spia.

Tuttavia, le caratteristiche innovative proprie di questi software e, più in generale, dell'attività intercettativa telematica su terminali mobili di tipo smartphone o su dispositivi informatici assimilabili, sono tali da determinare un sostanziale, rilevantissimo, mutamento negli effetti e nelle potenzialità di un mezzo di ricerca della prova, quale quello intercettativo, pensato e normato con riferimento a ben altre realtà.

Alcuni agenti intrusori sarebbero, infatti, in grado non solo di "concentrare", in un unico atto, una pluralità di strumenti investigativi (perquisizioni del contenuto del pc, pedinamenti con il sistema satellitare, intercettazioni di ogni tipo, acquisizioni di tabulati) ma anche, in talune ipotesi, di eliminare le tracce delle operazioni effettuate, a volte anche alterando i dati acquisiti.

Le garanzie stabilite dal codice di rito penale, a tutela dell'indagato (dal riscontro effettivo

CamminoDiritto.it
ISSN 2421-7123

del giudice sugli atti compiuti dagli inquirenti e sul rispetto delle condizioni stabilite dalla legge per ciascun atto, al contraddittorio sulla prova) risulterebbero, così, fortemente depotenziate dal ricorso, non adeguatamente circoscritto, a tali metodologie di indagine, in ragione delle peculiari caratteristiche che le rendono difficilmente inquadrabili nelle categorie gius-processuali tradizionali.

Questa difficoltà di qualificazione dogmatica è, del resto, alla base del contrasto interpretativo composto, nell'aprile 2016, dalle Sezioni unite della Corte di Cassazione, che hanno precisato le condizioni di utilizzo dei captatori informatici per realizzare intercettazioni di conversazioni e comunicazioni tra presenti, anche in ambito domiciliare.

Le particolari caratteristiche di queste metodologie di indagine rendono, infatti, l'intercettazione ambientale "itinerante" in quanto disposta su un dispositivo mobile e, per ciò solo, ontologicamente incompatibile con l'indicazione del luogo e le particolari tutele accordate alla riservatezza delle conversazioni svolte in ambito domiciliare.

Cogliendo molte delle indicazioni delle Sezioni unite, il legislatore ha recentemente disciplinato il ricorso ai captatori informatici, ammettendolo in particolare per le sole intercettazioni tra presenti e demandando a un successivo decreto ministeriale la definizione dei requisiti tecnici dei programmi informatici funzionali all'esecuzione di tali operazioni investigative.

In sede di parere sia sullo schema di decreto legislativo di riforma della disciplina delle intercettazioni, sia sullo schema di decreto ministeriale attuativo, il Garante ha fornito al Governo alcune proposte di integrazione del testo, utili a circondare di maggiori garanzie l'utilizzo dei captatori informatici a fini investigativi. In sede di parere sullo schema di decreto legislativo, in particolare, si invitava a valutare l'opportunità di includere nel decreto autorizzativo, anche per i delitti di competenza delle Procure distrettuali, l'indicazione dei luoghi e del tempo della captazione al fine di rafforzare, anche in questo ambito, le garanzie connesse ad un più incisivo controllo del giudice sull'attività investigativa.

Si rappresentava, peraltro, come tale modifica avrebbe contribuito a sviluppare in tutta la sua portata il criterio di delega di cui all'articolo 1, comma 84, lett. e), della legge 103 del 2017, laddove prescrive di scindere la fase dell'inserimento del captatore da quella della effettiva attivazione del microfono, al fine di circoscrivere per quanto possibile l'invasività di tale mezzo di ricerca della prova e di garantire la dovuta corrispondenza delle operazioni intercettative all'oggetto del decreto autorizzativo.

Inoltre, il Garante invitava il Governo a precisare alcune parti del decreto legislativo che

CamminoDiritto.it
ISSN 2421-7123

rischiavano di legittimare, in via interpretativa, l'acquisizione (sia pur senza possibilità di utilizzazione in giudizio) di dati personali anche al di fuori dei limiti temporali e spaziali stabiliti dal decreto autorizzativo del GIP.

Infine, si ravvisava l'opportunità di introdurre un espresso divieto (con la relativa sanzione in caso di inosservanza) di conoscibilità, divulgabilità e pubblicabilità di intercettazioni realizzate mediante captatori, inerenti soggetti estranei ai fatti per cui si proceda, peraltro in conformità ai criteri di delega.

In sede di parere sullo schema di decreto ministeriale, invece, il Garante aveva sottolineato l'esigenza di specificare con maggiore dettaglio i moduli software suscettibili di utilizzo, tra quelli che, comunemente, compongono un sistema di intercettazione mediante captatore informatico (es. il software che, installato sui dispositivi target, opera l'acquisizione delle informazioni; il sistema di inoculazione; il sistema di gestione; ecc.).

Si rilevava, inoltre, la necessità di indicare in modo puntuale le misure tecniche da adottare al fine di garantire la riservatezza dei dati sui sistemi funzionali all'esecuzione delle intercettazioni mediante captatore informatico, specificando ad esempio le modalità di accesso ai sistemi da parte degli operatori autorizzati, le funzionalità di registrazione delle operazioni ivi svolte, le modalità di trasmissione dei dati acquisiti mediante captatore.

Infine, si suggeriva di escludere il ricorso a captatori il cui funzionamento abbassasse il livello di sicurezza del dispositivo-ospite per impedirne la compromissione da parte di terzi, con eventuali riflessi negativi sulla protezione dei dati personali ivi contenuti, nonché sulla stessa riservatezza dell'attività investigativa.

La maggior parte di tali indicazioni non sono state recepite dai testi definitivamente approvati. In essi manca, soprattutto, la previsione di garanzie adeguate per impedire che, in ragione delle loro straordinarie potenzialità intrusive, questi strumenti investigativi, da preziosi ausiliari degli organi inquirenti, degenerino invece in mezzi di sorveglianza massiva o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, rendendolo estremamente permeabile se allocato in server non sicuri o, peggio, delocalizzati anche al di fuori dei confini nazionali.

La necessità di tali garanzie sembra, peraltro, asseverata dalle notizie diffuse dagli organi di stampa, in relazione alle particolari modalità di realizzazione delle captazioni mediante malware, da parte delle società incaricate ex art. 348, comma quarto, c.p.p. Le indagini giudiziarie in corso, di cui ha dato notizia la stampa, hanno infatti dimostrato i rischi connessi all'utilizzo di captatori informatici in assenza delle necessarie garanzie e,

CamminoDiritto.it
ISSN 2421-7123

soprattutto, con il ricorso, da parte delle società incaricate, a tecniche particolari, meritevoli di cautele ulteriori, in ragione delle loro peculiari caratteristiche e specifiche potenzialità.

Ci si riferisce, in particolare, all'utilizzo, ai fini intercettativi, di software connessi ad app, che quindi non sono direttamente inoculati nel solo dispositivo dell'indagato, ma posti su piattaforme (come Google play store) accessibili a tutti.

Ove rese disponibili sul mercato, anche solo per errore in assenza dei filtri necessari a limitarne l'acquisizione da parte dei terzi, come parrebbe avvenuto nei casi noti alle cronache, queste app-spia rischierebbero, infatti, di trasformarsi in pericolosi strumenti di sorveglianza massiva. Inoltre, estremamente pericoloso è l'utilizzo che, pure, parrebbe essere stato fatto nei casi all'esame degli inquirenti, di sistemi cloud per l'archiviazione, addirittura in Stati extraeuropei, dei dati captati.

La delocalizzazione dei server in territori non soggetti alla giurisdizione nazionale costituisce, infatti, un evidente vulnus non soltanto per la tutela dei diritti degli interessati, ma anche per la stessa efficacia e segretezza dell'azione investigativa

. Il ricorso a tali due tipologie di sistemi (app o comunque software che non siano inoculati direttamente sul dispositivo-ospite ma scaricati da piattaforme liberamente accessibili a tutti e, per altro verso, archiviazione mediante sistemi cloud in server posti fuori dal territorio nazionale) dovrebbe, dunque, essere oggetto di un apposito divieto.

A tal fine, si potrebbe ricorrere all'integrazione del decreto ministeriale del 20 aprile 2018, ovvero si potrebbe novellare il decreto legislativo n. 216 del 2017, la cui efficacia in parte qua è comunque differita ai provvedimenti autorizzativi emessi dopo il 31 luglio prossimo.

In subordine, ove non si ritenesse di sancire un divieto espresso di ricorso a tali tecniche, si potrebbe prevedere, anche in tal caso, preferibilmente con norma primaria, che l'effettiva installazione nel dispositivo elettronico portatile e le conseguenti funzionalità acquisitive del captatore informatico possano compiutamente realizzarsi solo dopo aver verificato l'univoca associazione tra il dispositivo interessato dal software e quello considerato nel provvedimento giudiziale autorizzativo.

In ogni caso, anche in ragione della rapida evoluzione delle caratteristiche e delle funzionalità dei software disponibili a fini intercettativi, sarebbe opportuno introdurre, in sede legislativa o anche soltanto novellando il citato decreto ministeriale, un espresso

CamminoDiritto.it
ISSN 2421-7123

divieto di ricorso a captatori idonei a cancellare le tracce delle operazioni svolte sul dispositivo ospite.

Ai fini della corretta ricostruzione probatoria e della completezza e veridicità del materiale investigativo raccolto è, infatti, indispensabile disporre di software idonei a ricostruire nel dettaglio ogni attività svolta sul sistema ospite e sui dati ivi presenti, senza alterarne il contenuto. Si potrebbe esplicitare, in questo senso, il requisito della "integrità, sicurezza e autenticità dei dati captati" che, ai sensi dell'art.4, comma 1, del decreto ministeriale, i software utilizzati devono assicurare, garantendo così effettivamente la completezza della "catena di custodia della prova informatica".

Più in generale, sul piano applicativo, se non attraverso una specifica integrazione del decreto ministeriale stesso, si potrebbe anche prevedere l'adozione di un unico protocollo di trasmissione e gestione dei dati destinati a confluire sui server installati nelle sale intercettazioni delle Procure della Repubblica per la loro conservazione, evitando possibili disomogeneità nei livelli di sicurezza.

Si potrebbe inoltre valutare l'opportunità di rendere disponibili software gestionali idonei a consentire l'analisi dei dati inerenti le caratteristiche dell'accesso ai server utilizzati per l'attività intercettativa da parte dei fornitori privati, per la realizzazione delle attività di manutenzione.

Si eviterebbe, in tal modo, di rendere accessibili, alle aziende stesse, i sistemi di conservazione dei log di accesso alla strumentazione mediante cui è svolta l'attività captativa, rafforzando le garanzie di segretezza della documentazione investigativa.

Sarebbe, peraltro, opportuno definire i criteri di gestione, da parte di ciascun Procuratore della Repubblica, delle intercettazioni eseguite da altri uffici giudiziari e relative a procedimenti i cui atti siano stati successivamente trasmessi per competenza ovvero comunque acquisiti per l'utilizzazione in procedimenti diversi ex art. 270, c.3, c.p.p.

Tanto si segnala ai sensi degli articoli 37 del decreto legislativo 18 maggio 2018, n. 51 e 23, comma 1, lettera a) del decreto legislativo 10 agosto 2018, n. 101, ai fini dell'adozione dei provvedimenti ritenuti opportuni, confermando la piena disponibilità dell'Autorità per la collaborazione che dovesse essere ritenuta utile»[40].

7. Gli elementi di apertura (la criminilità organizzata come consolidato espediente giustificativo di massima)

CamminoDiritto.it
ISSN 2421-7123

Le osservazioni della dottrina[41] rilevano come l'assenza di una dettagliata regolamentazione in materia non pregiudichi la possibilità di ritenere le attività investigative utilizzabili in giudizio.

Nonostante l'art. 191 del c.p.p., infatti, preveda che «le prove acquisite in violazione dei divieti stabiliti dalla legge non possono essere utilizzate» e che «l'inutilizzabilità è rilevabile anche d'ufficio in ogni stato e grado del procedimento» ciò sarebbe la conseguenza del fatto che alcune delle attività in questione, sono semplicemente riconducibili a strumenti di ricerca della prova già disciplinati da altre disposizioni normative.

A titolo di esempio, nella nota Sentenza Prisco, la possibilità di attivare la videocamera del device in cui è inoculato il virus spia, è riconducibile alla videoripresa, consentita nei limiti stabiliti dalla sentenza[42], mentre, le comunicazioni avvenute mediante le applicazioni di messaggistica online è invece riconducibile alla intercettazione telematica ex art. 266-bis c.p.p.)[43].

Inoltre, considerata l'assenza del principio di tassatività della prova nel nostro ordinamento, sulla base dell'art. 189 c.p.p. il giudice è autorizzato ad ammettere anche prove non espressamente disciplinate dalla legge[44].

Nella sentenza della Cassazione ss., Sez. V, 30 settembre 2020, (dep. 11 novembre 2020), n. 31604, infatti, la Corte, specifica «il trojan horse non esercita alcuna pressione sulla libertà fisica e morale della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità» escludendone anche la riconducibilità dello strumento di indagine a metodi e tecniche idonee ad influire sulla libertà di determinazione del soggetto ex art. 188 c.p.p.[45].

Secondo tale impostazione, dunque, in tal caso, sarebbe proprio la natura «subdola» dello strumento di captazione, in quanto segreto nel suo dinamismo operativo, la principale garanzia dell'integrità del processo di autodeterminazione del soggetto sottoposto ad indagini, in quanto, all'oscuro del controllo esercitato sul suo dispositivo, tenderà ad assumere un atteggiamento naturale non soggetto ad agenti di influenza esterni.

Secondo Signorato, invece, l'attività di inoculazione del captatore operata grazie alla inconsapevole agevolazione del destinatario concretizzatesi con le operazioni di download esca, violerebbe, invece, il principio del nemo tenetur se detegere, da intendersi non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni autoincriminanti, a detrimento della libertà morale dell'individuo

CamminoDiritto.it
ISSN 2421-7123

coinvolto[46].

Secondo la Corte, nel caso in cui con il trojan si arrivasse ad effettuare intercettazioni invalidate dall'inutilizzabilità come quelle intercorrenti tra l'imputato ed il suo difensore oppure si arrivasse ad attività lesive della dignità umana, ciò non inciderebbe sulla legittimità del decreto autorizzativo, in quanto comporterebbe nell'onere motivazionale del giudice un requisito non previsto dalla legge.

Inoltre, sempre secondo la Corte, simili situazioni patologiche rinvengono una adeguata e puntale protezione nell'art. 271 c.p.p., in base al quale non sarebbero utilizzabili le risultanze di specifiche intercettazioni «qualora le stesse siano state eseguite fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dagli articoli 267 e 268 commi 1 e 3».

Allo stesso tempo, non sono utilizzabili «i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo». Non possono essere utilizzati, inoltre, «le intercettazioni relative a conversazioni o comunicazioni delle persone indicate nell'articolo 200 comma 1, quando hanno a oggetto fatti conosciuti per ragione del loro ministero, ufficio o professione, salvo che le stesse persone abbiano deposto sugli stessi fatti o li abbiano in altro modo divulgati»[47].

Sempre secondo la Corte, «la necessità dell'indicazione di uno specifico luogo, quale condizione di legittimità dell'intercettazione, non risulta imposta né dall'art. 266 c.p.p., comma 2 (in cui, con riferimento all'intercettazione di comunicazioni tra presenti, vi è solo la previsione di una specifica condizione per la legittimità dell'intercettazione se effettuata in un luogo di privata dimora), né dalla giurisprudenza della Corte EDU».

Di conseguenza, «devono ritenersi legittime le intercettazioni "tra presenti" eseguite a mezzo di captatore informatico installato su un dispositivo portatile, nell'ambito dell'attività investigativa svolta in relazione a procedimenti di criminalità organizzata e ciò prescindendo dalla preventiva individuazione ed indicazione dei luoghi in cui la captazione deve essere espletata»[48].

Per concludere usando le parole d Muratori «nell'ambito dei procedimenti aventi ad oggetto i c.d. "reati comuni" sono proprio le considerazioni sulla struttura del mezzo probatorio a fare emergere un profilo di incompatibilità fra l'utilizzo dello strumento tecnico del captatore informatico e l'applicazione della disciplina sulle intercettazioni, atteso che nell'ambito di tali procedimenti non si riuscirebbe a dare attuazione alla clausola prevista dall'art. 266, comma 2, c.p.p. a tutela del domicilio e posto che, se anche

CamminoDiritto.it
ISSN 2421-7123

fosse tecnicamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione ove quest'ultimo facesse ingresso in luogo di privata dimora, ne risulterebbe comunque impedito il controllo dell'organo giudicante al momento dell'autorizzazione.

Lo scenario, tuttavia, cambia decisamente in relazione ai delitti di criminalità organizzata. Per tali più gravi delitti, infatti, è certamente ragionevole pensare che il legislatore, in considerazione dell'eccezionale gravità e pericolosità delle minacce derivanti alla società e ai singoli dalle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di ingenti risorse finanziare, abbia voluto operare uno specifico bilanciamento di interessi, optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio»[49].

Al riguardo, appare interessante richiamare anche la decisione della Cass., Sez. I, Sent. 4 novembre 2020 (dep. 22 dicembre 2020), n. 37039, con la quale la Suprema Corte si è pronunciata in tema di "intercettazioni disposte dal pubblico ministero nei casi di urgenza", confermando un orientamento giurisprudenziale considerato dalla Corte «sostanzialmente uniforme» in basa a cui «l'inutilizzabilità degli esiti delle intercettazioni è prevista dall'art. 267 c.p.p. solo nel caso di mancata convalida».

Nella vicenda processuale in questione, la difesa ha proposto ricorso in cassazione avverso il provvedimento del tribunale delle libertà che confermava la misura cautelare della custodia in carcere per reati di mafia ex. 416 bis c.p. Nei fatti relativi alle operazioni di intercettazioni la polizia giudiziari aveva chiesto al P.M. un decreto autorizzativo ad eseguire intercettazione in via d'urgenza con l'uso del captatore informatico sulla base della sussistenza di gravi elementi indiziari a carico dell'indagato nonché il pericolo di commissione dei fatti per i quali si procedeva[50].

Il Pubblico Ministero ha riconosciuto tali necessità con decreto poi convalidato dal G.I.P. Dal canto suo, la difesa ha sollevato due eccezioni per vizio di motivazione nel provvedimento di convalida del tribunale delle libertà, una per difetto del requisito dell'urgenza e l'altro sulle tempistiche del potere dispositivo del P.M.

Sulla base di quanto eccepito dalla difesa, il requisito del periculum in mora, indispensabile ai fini della configurazione di una esigenza di urgenza, sarebbe compromesso dall'inattività del pubblico ministero oltre il termine di quarantotto ore. Il ricorso, non ha poi ricevuto accoglimento da parte della Corte in quanto la presenza dei gravi indizi di reato riguarda la presenza di un illecito penale e non la colpevolezza di un determinato soggetto.

CamminoDiritto.it
ISSN 2421-7123

Da ciò ne consegue che tali indizi possano poi riguardare anche un soggetto diverso dalla persona per la quale verranno disposte le intercettazioni con captatore. Sul requisito dell'urgenza, invece, la Corte, come accennato in precedenza, ha aderito all'orientamento uniforme secondo cui «l'inutilizzabilità degli esiti di tali intercettazioni è prevista dall'art. 267 c.p.p. solo nel caso di mancata convalida e che, pertanto, una volta che la stessa intervenga assorbendo integralmente il provvedimento originario, resta preclusa ogni discussione sulla sussistenza del requisito dell'urgenza, rimessa, peraltro, alla valutazione dell'organo procedente».

Infine, sempre secondo la Corte, il ritardo nell'attivazione materiale delle operazioni di intercettazione col virus spia, «non può di per sé influire sulla validità ed utilizzabilità dei risultati delle operazioni, essendo tale ritardo inidoneo a dimostrare ex post il difetto del requisito dell'urgenza». Secondo i giudici di legittimità sulla base dell'art. 267, comma 3, c.p.p. È il P.M. che decide «le modalità e la durata delle operazioni», sicché, qualora decidesse di procrastinare l'inizio delle operazioni rispetto alla data del decreto, non sarebbe tenuto ad alcuna motivazione»[51].

8. Lo stato dell'arte e le criticità per il futuro

Dunque, riassumendo, il d.lgs 29 dicembre 2017, n. 216 c.d. "Orlando", ha disciplinato per la prima volta l'utilizzo del captatore informatico (trojan horse), come strumento di ricerca della prova solo per il perseguimento dei gravi reati di criminalità organizzata e terrorismo.

Il decreto del 2017 conteneva, secondo la giurisprudenza, già in sé la possibilità di un impiego del software spia nelle operazioni di indagine per reati contro la pubblica amministrazione, laddove, però, ne veniva riservato l'impiego nei contesti domiciliari solo nell'ipotesi in cui si sospettasse la concreta commissione dell'attività criminale in tale luogo.

La l. n. 3/2019 c.d. "Spazzacorrotti", ha, invece, esteso la generale utilizzabilità del software anche alle operazioni di indagine riguardanti i reati contro la pubblica amministrazione, commessi sia da pubblici ufficiali che incaricati di pubblico servizio e puniti con la reclusione non inferiore nel massimo a cinque anni. Ciò anche nei luoghi indicati dall'art. 614 c.p. come private abitazioni o altri luoghi di privata dimora e anche nelle circostanze in cui non è presente il requisito aggiuntivo previsto dall'art. 266, comma 2, c.p.p.[52].

Per quanto attiene ai reati comuni, invece, è stato escluso l'impiego del virus spia in quanto, nell'impossibilità di elaborare preventivamente una lista dettagliata di tutti i

CamminoDiritto.it
ISSN 2421-7123

potenziali luoghi di privata dimora in cui il software potrebbe essere impiegato, diverrebbe impossibile rispettare le condizioni di legittimità previste dall'impianto del codice di rito.

Dal Ministero di grazia e giustizia, saranno via via stabiliti, con decreto ministeriale, i requisiti tecnici che i vari trojan horse sviluppati per le operazioni di intercettazione delle procure dovranno rispettare in merito ad "affidabilità, sicurezza ed efficacia".

Prima della riforma Orlando le Sezioni unite, con la sentenza 28 aprile 2016, n. 26889 (Scurato), hanno legittimato l'utilizzo del nuovo strumento di indagine per il compimento di attività investigati mediante intercettazioni "tra presenti", ma solo nei casi di procedimenti contro la criminalità organizzata.

I dubbi circa la possibilità di una deviazione elastica dei margini di utilizzabilità oltre i criteri stabiliti dal caso Scurato, erano già presenti nelle note della Corte, la quale non aveva esitato di specificare che, considerata la "forza intrusiva" dello strumento «la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso».

Nel rispetto del bilanciamento tra esigenze di tutela della sicurezza collettiva (da preservare) ed il rispetto delle libertà fondamentali (violate) è il sempre il provvedimento di autorizzazione gel giudice che riveste «una fondamentale funzione di garanzia, spiegando le ragioni dell'assoluta indispensabilità dell'atto investigativo e indicando con precisione quale sia il criterio di collegamento tra l'indagine in corso e la persona da intercettare».

Il successivo intervento delle sezioni unite con la Sentenza n. 51 del 2 gennaio 2020 (Cavallo) , riguardante il tema della possibilità di impiego delle intercettazioni in "procedimenti diversi" da quelli per cui erano state autorizzate, ha ulteriormente introdotto il principio per cui le varie intercettazioni effettuate in un procedimento diverso da quello per cui sono state autorizzate sono comunque utilizzabili a condizione che si tratti, però, di reati per i quali è previsto l'arresto obbligatorio in flagranza[53].

Come sottolineato da Enrico Cassaro «nel corso degli anni, vi è stato un uso prudente del captatore informatico nelle indagini. Non solo perché anche dagli stessi magistrati delle Procure della Repubblica è percepito come uno strumento invasivo. Ma anche per i costi elevati che il captatore informatico presenta, a maggior ragione in questo periodo di frequente richiamo al contenimento delle spese per le intercettazioni.

CamminoDiritto.it
ISSN 2421-7123

Dai dati del Tribunale di Milano, se la spesa per intercettazioni telefoniche (tradizionale) è pari a €4 al giorno e quella per intercettazioni ambientali pari a €60 al giorno, quella, invece, per le intercettazioni telematiche, di cui stiamo trattando, è di ben €150 al giorno. Infine, vi sono anche dei problemi pratici da superare: per esempio, l'eccessivo uso delle batterie dei dispositivi portatili, la necessità di sfuggire agli antivirus e ai firewall»[54].

E ancora prosegue affermando che «il problema più grande è, e rimane, la mancanza di una disciplina completa e precisa. Il trojan è normato, ma mancano i decreti ministeriali che indichino quali debbano essere le caratteristiche tecniche dell'intrusore informatico. C'è infatti il problema dell'inoculazione, ma vi è anche il problema della disattivazione. Altro aspetto importante riguarda la perquisizione, poiché si acquistano tutti i dati nella memoria del dispositivo. Tutto questo non è normato. Mancano delle norme certe che evitino la manipolazione dei dati; e ciò, nel mondo di oggi dove questi ultimi sono pagati a peso d'oro, è ancora più grave. Tutto ciò è aggravato anche dal fatto che, secondo diverse inchieste giornalistiche, sembra che i dati non viaggiano direttamente dal dispositivo al server della Procura, ma passano prima per un altro server, di terzi soggetti. È, ad esempio, il caso dei dati raccolti con il malware Exodus, i quali finivano su server negli Stati Uniti, accessibili da qualsiasi dispositivo e browser, in una sorta di caveau da cui chi aveva le chiavi avrebbe potuto ottenere informazioni sensibili per attività di dossieraggio. Lo Stato si affida, per l'installazione e la cura dei captatori informatici, a società private. Ciò rende, infatti, assai più permeabile la filiera su cui si snoda l'attività di indagine, coinvolgendovi una pluralità di soggetti, spesso privi dei requisiti professionali, organizzativi e persino dell'affidabilità, necessari per svolgere un'attività così delicata quale quella intercettativa»[55].

9. Conclusioni

In conclusione, il progresso e le opportunità messe a disposizione dall'impiego delle nuove tecnologie deve essere oggetto di costante attenzione e monitoraggio da parte del decisore, in virtù dell'enorme potenzialità intrusiva e lesiva dei diritti fondamentali delle persone. Software in linea teorica molto utili per l'attività di contrasto alla mafia, al terrorismo ed alla corruzione, corrono il rischio di divenire, in assenza di un adeguato controllo esterno, strumenti di sorveglianza di massa.

Lo stesso Garante dei dati personali, nella sua segnalazione ha chiesto la risoluzione delle criticità per le garanzie processuali dell'indagato.

A tal riguardo, la richiesta è di stabilire limiti nelle operazioni d'intercettazioni telematiche, su modo e luogo in cui avvengono, così come sulla modalità di trasmissione e conservazione dei dati. Il trojan horse, molto più intrusivo dei normali apparati di

CamminoDiritto.it
ISSN 2421-7123

intercettazione telefoniche o ambientali, spia le attività dell'indagato, ma anche di soggetti terzi estrai, rendendo possibile l'accesso ad un insieme di dati sensibili contenuti nel dispositivo infettato quali foto, video, mail, messaggi e password di ogni genere.

Il legislatore ha risposto ancora una volta con la nuova legge sulle intercettazioni, c.d. “Bonafede”, estendendo la possibilità di impiego di uno strumento così invasivo anche per reati comuni commessi contro la pubblica amministrazione da parte di pubblici ufficiali od incaricati di pubblico servizio.

L' assoggettamento delle categorie summenzionate alla medesima disciplina prevista per reati di particolare allarme sociale, quali terrorismo o criminalità organizzata, in virtù del profondo ventaglio conoscitivo posto a disposizione degli investigatori in caso di indagini per reati di corruzione, concussione ecc., anche nelle ipotesi di estrema delicatezza contemplate dall'art. 664 c.p.p., ha reso evidente la necessità di riflettere sull' adeguatezza e proporzione di un simile strumento in tali contesti.

I recenti interventi pubblici del guardasigilli Nordio hanno avvalorato le ragione critiche degli ultimi anni, anche in virtù dei rilevanti fatti di cronaca accorsi nelle prime pagine di quotidiani e reti nazionali, inducendo ad immaginare un prossimo intervento regolatorio del legislatore, nell' ottica in un profondo ridimensionamento dello strumento, eccetto per le ipotesi di criminalità organizzata e terrorismo, quest' ultime soggette tendenzialmente ad un regime di deroga a maglie larghe e poco incline ad un equilibrio tra le esigenze di tutela delle sicurezza ed il contestuale rispetto delle libertà fondamentali.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Il Ministro Cartabia ha rilevato come da tale impostazione deriverebbe la conseguenza per cui il provvedimento di affidamento dell'incarico debba sottostare all'obbligo di controllo della Corte dei conti. Tale impostazione risulterebbe, però, essere in contrasto con le norme europee. La commissione ha messo in mora l'Italia perché inottemperante «agli obblighi basati sull'assimilazione dei contratti per le intercettazioni a transazioni commerciali». Si veda intercettazioni, contratti secretati. Il Copasir ora chiede chiarezza, di G. M. JACOBAZZI, su il Dubbio, quotidiano online, del 23 ottobre 2021.

[2] Così la Relazione sulla disciplina per l'utilizzo di contratti secretati del Copasir del 21ottobre 2021.

[3] Il nome Exodus fa riferimento ad un software di captazione informatica sviluppato dall'azienda calabrese sSurv, specializzata in sistemi di sicurezza con sede a Catanzaro.

[4] Per approfondimenti sul tema si veda Exodus, eSurv: storia di uno spyware italiano di C. GHIDOTTI su punto-informatico, sito online del 20/03/2019.

[5] Come emergerebbe dai documenti sui pagamenti della polizia di stato, rilasciato sulla base della normativa sulla "trasparenza nell'uso delle risorse pubbliche, art. 4 D.lgs. n.33 del 2013-art. 5 D.lgs n.97 2016, eSurv, ha ricevuto in data 6 novembre 2017 un versamento pari a 307.439,90 euro. La spesa è inserita alla voce "Acquisto di beni e servizi" di "Sistema di intercettazione attiva e passiva". Si veda pag. 11 del documento rinvenibile sul sito della polizia di Stato.

[6] Si tratta per l'appunto di reati associativi e/o di terrorismo.

[7] Il comma 2 bis dell'art.266 così recita: «L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo».

[8] Seconda parte comma 1, art. 267 c.p.p.

[9] Così al comma 2-bis art. 268 c.p.p.

[10] Così al comma 4 art. 268 c.p.p.

[11] Così al comma 6 art. 268 c.p.p.

[12] Così al comma 8 art. 268 c.p.p.

[13] Così al comma 7 art. 268 c.p.p.

[14] Si pensi ad eventuali e non rare intercettazioni di conversazioni tra difensore ed imputato, il cui contenuto, nell'ambito delle attività di indagini spesso e volentieri è oggetto di annotazione da parte della polizia giudiziaria contravvenendo alle disposizioni contenute all'art. 271 c.p.p in cui è previsto che «non possono essere utilizzate le intercettazioni relative a conversazioni o comunicazioni delle persone indicate nell'articolo 200 comma 1, quando hanno a oggetto fatti conosciuti per ragione del loro ministero, ufficio o professione, salvo che le stesse persone abbiano deposto sugli stessi fatti o li abbiano in altro modo divulgati».

[15] Art. 269 comma 2 del c.p.p.

[16] Si veda l'uso selvaggio dei trojan lede i diritti: lo sanno pure i giustizialisti di F.S.MARINI su il Dubbio, quotidiano online del 21 febbraio 2022.

[17] «La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge».

CamminoDiritto.it
ISSN 2421-7123

[18] Ex artt. 266, c.1, e 266--bis c.p.p

[19] di cui all'art. 266, c. 2, c.p.p.

[20] Ex art. 614 c.p.

[21] Cass. pen, SS.UU, 28.04.16, n. 26889

[22] Art. 13 art. 13 D.L. 13 maggio 1991, n. 152 1. così stabilisce: «In deroga a quanto disposto dall'articolo 267 del codice di procedura penale, l'autorizzazione a disporre le operazioni previste dall'articolo 266 dello stesso codice è data, con decreto motivato, quando l'intercettazione è necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi. (Nella valutazione dei sufficienti indizi si applica l'articolo 203 del codice di procedura penale). Quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo a un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'articolo 614 del c. p., l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa. 2. Nei casi di cui al comma 1, la durata delle operazioni non può superare i quaranta giorni, ma può essere prorogata dal giudice con decreto motivato per periodi successivi di venti giorni, qualora permangano i presupposti indicati nel comma 1. Nei casi di urgenza, alla proroga provvede direttamente il pubblico ministero; in tal caso, si osservano le disposizioni del comma 2 dell'articolo 267 del codice di procedura penale. 3. Negli stessi casi di cui al comma 1 il pubblico ministero e l'ufficiale di polizia giudiziaria possono farsi coadiuvare da agenti di polizia giudiziaria».

[23] Secondo una definizione data dall'enciclopedia Wikipedia, «un keylogger, in informatica, è uno strumento hardware o software in grado di effettuare la registrazione (logging) della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente se ne accorga». Esistono due tipologie di keylogger, una di tipo hardware ed una di tipo software. La prima consiste in un «micro dispositivo elettronico a cavetto, dall'aspetto simile a una prolunga, da collegarsi tra il cavo della tastiera e il pc, che riesce a catturare e memorizzare in un file di testo tutte le password e qualsiasi altro dato, come ad esempio gli indirizzi web, digitati sulla tastiera», la seconda tipologia consiste in «un programma spia o "sniffer" (annusatore) installato sul computer e in grado di tracciare e memorizzare in un file di log, nascosto all'utente, le attività svolte con il pc, catturando ad esempio le schermate video, i messaggi di posta elettronica, i numeri della carta di credito e così via. Spesso i software tipo key logger vengono installati, all'insaputa dell'utente**,** tramite **worm o trojan** ricevuti attraverso l'Internet e che rimangono in esecuzione sul PC proprio per captare tutte le digitazioni (password, dati sensibili, numeri di carte di credito, identità ecc.) che avvengono su tastiera, registrarle e poi inviarle a un computer remoto spia, pronte per essere, in un secondo tempo, decodificate e usate». Per approfondimenti si veda il sito online di Axerta investigation consulting.

[24] «Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 416, sesto e settimo comma, 416, realizzato allo scopo di commettere taluno dei delitti di cui all'art. 12, commi 1, 3 e 3-ter, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 600, 601, 602, 416 bis, 416 ter, 452 quater e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416 bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'articolo 74 del testo unico approvato con decreto del Presidente della Repubblica 9 ottobre 1990 n. 309 (190 bis, 295, 371 bis, 406 c.p.p.), e dall'articolo 291 quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, nonché dall'art. 260 del decreto legislativo 3 aprile 2006 n. 152, le funzioni indicate nel comma 1 lettera a) sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

[25] Consente, per talune tipologie di reato, l'acquisizione di conversazioni che avvengono anche nei luoghi di privata dimora, senza la necessità che all'interno di tali luoghi vengano poste in essere le attività criminose oggetto d'indagine.

[26] "abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita ".

[27] Le Sezioni Unite, con sentenza n. 51/2020, hanno affermato il seguente principio di diritto: «il divieto di cui all'art. 270 cod. proc. pen. di utilizzazione dei risultati di intercettazioni di conversazioni in procedimenti diversi da quelli per i quali siano state autorizzate le intercettazioni – salvo che risultino indispensabili per l'accertamento di

CamminoDiritto.it
ISSN 2421-7123

delitti per i quali è obbligatorio l'arresto in flagranza – non opera con riferimento ai risultati relativi a reati che risultino connessi ex art. 12 cod. proc. pen. a quelli in relazione ai quali l'autorizzazione era stata ab origine disposta, sempreché rientrino nei limiti di ammissibilità previsti dalla legge».

[28] Si veda la Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, del 30/04/2019 sul sito online del Garante per la protezione dei dati personali.

[29] Si veda Il trojan sul telefono di Palamara continuò a lavorare oltre i termini di S. MUSCO, del 28 maggio 2021 su il Dubbio, quotidiano online.

[30] Come si può leggere sul sito governativo ufficiale, «il Cnaipic, avvalendosi di tecnologie di elevato livello e di personale altamente qualificato, è incaricato della prevenzione e del contrasto della minaccia informatica di matrice terroristica o criminale, attraverso alcune funzioni:

Sala operativa-Punto di contatto univoco, disponibile 24 ore su 24 e 7 giorni su 7, dedicato all'interscambio informativo; Intelligence -Raccolta dei dati e delle informazioni utili ai fini di prevenzione, attraverso il costante monitoraggio Internet, sia a livello nazionale che internazionale; Analisi-Comparazione dei dati e delle informazioni raccolte, predisposizione di rapporti previsionali sull'evoluzione della minaccia e delle vulnerabilità informatiche, delle tecniche e delle iniziative criminali; Investigazione-Risposta operativa al verificarsi di un evento informatico criminale, anche in collaborazione con organismi di polizia stranieri e internazionali, come Interpol, Europol, Sottogruppo G8 High Tech Crime. [31] Si veda sempre Il trojan sul telefono di Palamara continuò a lavorare oltre i termini di S. MUSCO, del 28 maggio 2021 su, il Dubbio, quotidiano online; anche Scoppia "intercettopoli": illegali i server che conservano trojan e captazioni di S. MUSCO del 15 maggio 2021 su il Dubbio, quotidiano online.

[32] Si veda Intercettazioni via trojan, nuovo scandalo: il server occulto. Urgono nuove regole di M. BORGOBELLO, del 15 Maggio 2021, su Agenda digitale, sito online.

[33] Sez. un., c.c. 28.4.2016, (dep. 1.7. 2016), Scurato, n. 26889/2016).

[34] Così la Sez. IV, n. 32428 del 24.9.2020

[35] La giurisprudenza consolidata, infatti, ritiene che l'inserimento di microspie nella privata dimora, rappresentando in concreto una delle possibili modalità attuative di tale mezzo di ricerca della prova, deve anche ritenersi implicitamente ammessa nel provvedimento di autorizzazione, senza la necessità di una specificazione. In tal senso cfr. Sez. VI, 31.1.2011, di Maggio, n. 14547, Rv. 250032; Sez. I, 9.12.2003 (dep. 2004), Rigato, n. 24539, Rv. 230097.

[36] Si veda L. FILIPPI, Il virus trojan: uno strumento nelle mani incontrollabili della polizia giudiziaria, del 30 Novembre 2020 su Penale, diritto procedura, rivista online.

[37] Si veda anche Sez. VI, del 23.6.2017, Nobile, n. 39403, Rv. 270941; Sez. VI,25.9.2012, Adamo, n. 41514 Rv. 253805.

[38] A riguardo anche Sez. II, 18.2.2013, Badagliacca, n. 21644, Rv. 255541; Sez. I, 2.10.2007, Biondo, n. 38716, Rv. 238108; Sez. IV, 28.9.2005, Cornetto, n. 47331, Rv. 232777 – anche Sez. VI, 13.6.2017, Romeo, n. 36874.

[39] Così L. FILIPPI, Il virus trojan: uno strumento nelle mani incontrollabili della polizia giudiziaria, del 30 Novembre 2020 su Penale, diritto procedura, rivista online.

[40] Così la Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, del 30/04/2019 sul sito online del Garante per la protezione dei dati personali.

[41] P. BRONZO, L'impiego del trojan horse informatico nelle indagini penali, in Rivista italiana per le Scienze Giuridiche, (8) 2017, p. 347. F.CAPRIOLI, Il "captatore informatico" come strumento di ricerca della prova in Italia, in Rev. Brasileira dir. proc. pen., 2017, p. 485 ss.

[42] Cass., S.U., 28.3.2006, PRISCO, in Riv. it. dir. e proc. pen., 2006, 1537.

[43] Cass.pen., 10 novembre 2015, Guarnera, in Arch. pen., 2016 (1), p. 212 s., con nota di A. TESTAGUZZA, Chat BlackBerry: sistema "pin-to-pin".

CamminoDiritto.it
ISSN 2421-7123

[44] «Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova». Così all'art. 189 c.p.p.

[45] L'art. 188 c.p.p. al comma 1 recita che «Non possono essere utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei a influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e di valutare i fatti».

[46] S. SIGNORATO, Le indagini digitali. Profili strutturali di una metamorfosi investigativa, Giappichelli, Torino, 2018, p. 238.

[47] Così Cass. ss., Sez. V, 30 settembre 2020, (dep. 11 novembre 2020), n. 31604.

[48] Così M.S. MURONE, Brevi note sul rapporto tra trojan horse e libertà di autodeterminazione, del 12 febbraio 2021, su Penale, diritto e procedura, rivista online.

[49] Così sempre M.S. MURONE, Brevi note sul rapporto tra trojan horse e libertà di autodeterminazione, del 12 febbraio 2021, su Penale, diritto e procedura, rivista online.

[50] Si veda nota del Commissariato di Palmi del 28.9.2017.

[51] Per approfondimenti, si veda la Cassazione sulle intercettazioni mediante trojan disposte dal pubblico ministero: la convalida preclude ogni discussione sul requisito dell'urgenza di A. DI DOMENICO del 18 Marzo 2021, su Sistema Penale, rivista online.

[52] Presupposto affinché le operazioni di intercettazione possano essere ritenute legittime è che durante le captazioni in luoghi domiciliari, sia in atto l'attività criminale.

[53] Per approfondimenti sul tema si veda D. ALBANESE, la Cassazione chiarisce la portata del principio di diritto affermato dalle Sezioni unite "Cavallo": nessun limite all'utilizzabilità dei risultati delle intercettazioni in caso di riqualificazione giuridica del fatto oggetto di autorizzazione del 10 settembre 2021 su Sistema Penale, rivista online.

[54] Così CASSANO, I trojan nel processo penale: strumento utile o eccessivamente invasivo?, del 8 maggio 2020 su Tra i leoni, Bocconi University Newspaper, sito online.

[55] Così sempre CASSANO...

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=9711