UNIVERSITÀ DEGLI STUDI DI CATANIA

Scuola di Specializzazione per le Professioni Legali "A. Galati"

IL *TROJAN HORSE*

Luci ed ombre di un poliedrico strumento di controllo "orwelliano" nelle mani degli inquirenti.

RELATORE

Dott.ssa Agata Consoli

CORSISTA

Dott. Claudio Nigrelli

730001321

Anno accademico 2019/2020

INDICE

Premessa.

Il progresso tecnologico ha indubbiamente migliorato - ed allo stesso tempo condizionato - la vita di ogni consociato. È innegabile che ormai l'uso dei dispositivi telematici, siano essi *smartphone, tablet, personal computers*, etc., è diventato parte del nostro quotidiano. Che sia per svago, per lavoro o per comodità non possiamo fare a meno di utilizzare questi strumenti nelle operazioni giornaliere e gli stessi finiscono con l'essere al nostro fianco in ogni momento ed in qualsiasi posto ci troviamo.

Certamente il progredire della tecnologia e le agevolazioni che ad esso conseguono sono qualcosa di positivo, che migliora la vita dell'uomo, cambiandone in certi casi anche i rapporti sociali.

Tuttavia, se da un lato la tecnologia offre un importante contributo all' uomo, dall'altro quest'ultimo spesso se ne serve per compiere dei delitti, adoperando le moderne modalità di comunicazione[1] per rendere meno agevole agli inquirenti l'eventuale intercettazione di conversazioni che potrebbero rivelarsi incriminanti.

D'altro canto, anche le Procure cercano di dotarsi di strumenti investigativi per riuscire a perseguire i delitti posti in essere mediante queste nuove modalità, risultando spesso inappropriati o poco efficaci i mezzi di ricerca della prova tipici previsti dal codice di rito.

È proprio in questo contesto che si inserisce il captatore informatico. Un *malwere*[2], spesso di tipo *Trojan*, ma ne esistono di vario genere, iniettato dagli inquirenti nel dispositivo

[1] Si pensi, ad esempio, ai sistemi di messaggistica istantanea come *Whatsapp*, *Instagram* o *Messenger* che hanno finito col soppiantare i tradizionali SMS, garantendo una maggiore tutela della *privacy* degli utenti servendosi della cifratura "*end-to-end"*, ossia fra i due dispositivi coinvolti nella conversazione e non sui server; ovvero ai programmi di videochiamata digitale come *Skype* che si servono della rete *VoIP - Voice over Internet Protocol* – gestiti da *internet service providers* internazionali. O ancora, ai servizi di messaggistica che utilizzano i c.d. *cloud* – spazi virtuali messi a disposizione dell'utente da parte dei *providers* al fine di immagazzinarvi dati – difficilmente accessibili da parte degli inquirenti se non con la collaborazione delle multinazionali che li gestiscono. Per una panoramica più dettagliata si veda *L. GIORDANO, Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont*., fasc. 3/2017, p. 3 ss.

[2]Secondo la definizione fornita da *Treccani – Enciclopedia on line* un *Malware* è un "Software che, una volta eseguito, danneggia il funzionamento e la sicurezza del sistema operativo; il termine deriva dalla contrazione di *malicious* e *software* e significa letteralmente "programma malvagio". Sempre più diffusi, i m. si trasmettono via internet; spesso tramite la posta elettronica, ma anche attraverso la semplice navigazione. Tra le categorie di m. più diffuse si ricordano virus, *trojan horse*, *keylogger*, *worm* e *backdoor*. Esistono poi i m. poliformici (che cambiano continuamente forma, pur mantenendo inalterata la

bersaglio al fine di aggirare le difese predisposte dai sistemi di sicurezza di cui è dotato e carpire informazioni e dati in esso contenuti, fino ad arrivare a controllare da remoto (servendosi della c.d. funzione *client*) l'intero dispositivo.

Le invasività dirompente e la poliedricità che caratterizzano un simile strumento hanno suscitato opinioni contrastanti, sia tra gli operatori del diritto che nell'opinione pubblica, sull'utilizzo che gli inquirenti, ma anche i privati[3], dovrebbero (e potrebbero) fare di tali *softwares*.

Emerge plasticamente, pertanto, come uno strumento del genere sia in grado di minacciare diritti fondamentali dell'individuo come la riservatezza, la segretezza della corrispondenza e l'inviolabilità del domicilio allorché il suo impiego non venga ponderatamente disciplinato dal Legislatore, garantendo ad ogni consociato le garanzie e le tutele previste dagli artt. 2, 14 e 15 della Costituzione e dalle norme sovranazionali in materia (art. 8 CEDU).

In merito, pur non facendo espresso riferimento ai captatori informatici, la Convenzione del Consiglio d'Europa siglata il 23 novembre 2001 a Budapest aveva previsto all'art. 15 una serie di principi minimi processuali ai quali le legislazioni degli Stati aderenti avrebbero dovuto adeguarsi: *i.* riserva di legge; *ii.* tutela della dignità della persona; *iii.* riserva di giurisdizione (o comunque di un organo indipendente) ed infine *iv.* principio di proporzionalità, secondo il quale "*il sacrificio imposto alla libertà personale di un soggetto deve essere proporzionato ed adeguato al reato che si vuole perseguire*".[4]

Quale corollario dei sopra enunciati principi, nella sezione dedicata alla disciplina procedurale, la Convenzione dettava alcune disposizioni relative a modalità di ricerca e

funzionalità) e quelli metamorfici (che alterano completamente il loro codice), entrambi particolarmente difficili da individuare."

[3] Trattasi di *softwares* rinvenibili nel libero mercato da chiunque e che addirittura vengono forniti alle stesse Procure da aziende private che si occupano proprio di questo genere di servizi.

[4] *O. CALAVITA, L'odissea del* trojan horse, in *Dir. pen. cont.*, fasc. 11/2018, p. 5 ss.

acquisizione della prova[5], alle quali il Legislatore ha cercato di allinearsi con la L. 18 marzo 2008, n. 48[6].

Tuttavia, con tale intervento, non era stato introdotto alcun nuovo mezzo di ricerca della prova all'interno del codice, limitandosi il Legislatore ad un mero adattamento delle previgenti discipline all'incalzante avanzare del progresso tecnologico.

Ciò posto, senza alcuna pretesa di sgomberare definitivamente il campo dagli innumerevoli dubbi (applicativi e non) suscitati da uno strumento così efficace e dirompente qual è il captatore informatico, nel presente elaborato si cercherà di comprendere: quali sono le effettive potenzialità del *Trojan*; se vi sono nuovi diritti fondamentali che potrebbero essere lesi dalle sue capacità intrusive, ovvero se quelli già previsti dalla Carta costituzionale possano dirsi sufficienti, nonché valutare se le operazioni tecnico-informatiche del captatore siano ascrivibili a fattispecie tipiche investigative e/o se è possibile ricondurle nell'alveo delle indagini atipiche ai sensi dell'art. 189 Cost.

Si cercherà, infine, di dare atto delle più recenti modifiche introdotte sul punto dalle riforme "*Orlando*", "*Buonafede*" e dalla legge n. 3 del 2019, focalizzando principalmente l'attenzione sugli interventi che hanno interessato il c.d. *virus* di Stato.

[5] «Conservazione rapida di dati informatici immagazzinati (art. 16), «conservazione e divulgazione rapide di dati relativi al traffico (art. 17), «ingiunzione di produrre» (art. 18), «perquisizione e sequestro di dati informatici immagazzinati» (art. 19), «raccolta in tempo reale di dati sul traffico» (art. 20), «intercettazioni di dati relativi al contenuto» (art. 21). (Sez. II, Convenzione di Budapest).

[6] Le principali garanzie perseguite dalla legge in parola possono così riassumersi: *a)* conservare inalterato il dato informatico originale nella sua genuinità; *b)* impedirne l'alterazione successiva; *c)* formare una copia che assicuri la conformità del dato informatico acquisito rispetto a quello originale; *d)* assicurare la non modificabilità della copia del documento informatico ed infine *e)* la garanzia dell'istallazione di sigilli informatici (ad. es. *algoritmo di hash*) sui documenti acquisiti. Sul punto si veda *amplius P.TONINI, Manuale di procedura penale, diciassettesima edizione,* Giuffrè Editore, 2016, p. 384 ss.

Capitolo I

SOMMARIO: 1. Il quadro normativo di riferimento. – 1.1 I principali interventi in materia di captatori informatici.

1. Il quadro normativo di riferimento.

La possibilità di inoculare un *virus* informatico in un dispositivo elettronico portatile per effettuare delle intercettazioni di comunicazioni ha reso evidente il rischio di una possibile captazione di informazioni riservate nei luoghi di privata dimora, anche quando non sussista il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa. Una simile eventualità soggiace a precisi limiti legislativi, disciplinati dall'articolo 266 c.p.p., dai quali gli inquirenti non possono prescindere, pena l'inutilizzabilità del materiale così ottenuto.

Invero, la giurisprudenza ha dovuto confrontarsi nel corso degli anni con le multiformi potenzialità dei captatori e, nello specifico, la nota sentenza a Sezioni Unite n. 26889 del 28 aprile 2016 "*Scurato"* ha posto alcuni importanti principi in ordine alla possibilità di effettuare intercettazioni tra presenti mediante l'uso del captatore informatico in luoghi di privata dimora.

Va da subito precisato che tale pronuncia si è occupata solamente di una delle tante funzionalità che caratterizzano il *Trojan*; in ogni caso, questo arresto assume rilevanza perché ha dato la stura al processo di riforma che ha interessato la disciplina delle intercettazioni di cui agli artt. 266 e ss. c.p.p.

La questione giuridica sottoposta alla Corte consisteva nello stabilire: "*Se - anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa, sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispositivi elettronici portatili*".

In estrema sintesi, la tesi prospettata dal ricorrente si rifaceva ad un orientamento secondo il quale l'indicazione, nel decreto autorizzativo, del luogo in cui doveva eseguirsi l'intercettazione doveva ritenersi un requisito necessario ai sensi dell'art. 266, co. 2, c.p.p., dal momento che solo in questo modo si sarebbe potuta garantire la compatibilità della disciplina con i principi costituzionali di cui all'art. 15 Cost., evitando, inoltre, il rischio di autorizzazioni "al buio" da parte del Giudice. [7]

Nel caso di specie, le intercettazioni erano state effettuate in un procedimento per delitti di criminalità organizzata e la Procura aveva proceduto a norma dell'art. 13 del D.L. n. 152/1991, convertito con modificazioni dalla L. n. 203 del 1991, il quale, derogando ai presupposti fissati dall'art. 266, comma 2, c.p.p., permette la captazione anche nei luoghi di privata dimora, senza che sia necessario che tali luoghi siano sedi di attività criminosa in atto.

Secondo la Corte, l'esigenza perseguita dal Legislatore con l'art. 13 D.L. 152/1991, ossia adottare modalità più incisive per contrastare il crimine organizzato derogando alla disciplina applicabile ai delitti "comuni" *ex* art. 266 c.p.p., sarebbe pienamente compatibile con i principi costituzionali e sovranazionali in materia, nonché conciliabile con il principio di proporzionalità della misura adottata.

Ne deriva, secondo il principio di diritto espresso nella sentenza, che "*Limitatamente ai procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (ad es., personal computer, tablet,*

[7] *"Dalle considerazioni appena svolte deriva che il decreto autorizzativo deve individuare, con precisione, i luoghi nei quali dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, non essendo ammissibile un'indicazione indeterminata o addirittura l'assenza di ogni indicazione, al riguardo. È dunque necessario verificare, nel caso in disamina, che i decreti autorizzativi contenessero una precisa individuazione dei luoghi in cui procedere ad intercettazione ambientale e che non siano state effettuate captazioni in luoghi diversi da quelli ai quali si riferiva l'autorizzazione*" (Cass. Sez. 6, n. 27100 del 26/05/2015, *Musumeci*).

smartphone, ecc.) - anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa" (Cass. Sezioni Unite n. 26889 del 28 aprile 2016, *Scurato*).

Pertanto, il captatore informatico è utilizzabile per realizzare intercettazioni "tra presenti" nei soli procedimenti per delitti di criminalità organizzata in forza della disciplina derogatoria di cui all'art. 13 D.L. 152/1991, anche quando nei luoghi di privata dimora non sia in atto l'attività criminosa. Al contrario, l'utilizzo del nuovo mezzo tecnologico - nei luoghi di privata dimora quando non sussiste il fondato motivo che ivi si stia svolgendo l'attività criminosa - era stato escluso per i reati "comuni" perché, non potendosi prevedere, nel momento dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto, non sarebbe possibile verificare il rispetto della condizione di legittimità richiesta dall'art. 266, comma 2, c.p.p.

La stessa sentenza ha precisato inoltre che, ai fini dell'applicazione della disciplina prevista dall'art. 13 del D.L. n. 152 del 1991, per procedimenti relativi a delitti di criminalità organizzata devono intendersi quelli elencati nell'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., nonché quelli comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.

Dunque, le Sezioni Unite non solo non hanno escluso la legittimità dell'uso di tale strumento captativo per le intercettazioni tra presenti nei luoghi di privata dimora dove si stia svolgendo l'attività criminosa, ma soprattutto, non l'hanno esclusa per le ulteriori forme di intercettazione, tra cui quelle telematiche *ex* art. 266 *bis*, c.p.p.

Ciò posto, sul punto è intervenuto il Legislatore con il D. Lvo. n. 216 del 2017, in attuazione della delega contenuta nell'art. 1, comma 84, lett. d), della legge n. 103 del 2017.

Obiettivi principali della legge delega erano: la predisposizione di una serie di misure per bloccare la conoscibilità delle risultanze delle operazioni all'esterno, anche mediante l'introduzione di sanzioni di carattere penale (tutela a valle); limitare la possibilità per gli operatori di P.G. di verbalizzare conversazioni irrilevanti ai fini dell'indagine (tutela a monte) ed, infine, che venisse assicurato un uso parsimonioso delle intercettazioni ritenute rilevanti da parte del Pubblico Ministero, e del Giudice, in caso di eventuale richiesta di applicazione di una misura cautelare.

Sulla scorta di tali premesse, dunque, il Legislatore individuava, nell'ambito della riforma, cinque momenti qualificanti:

- divieto di trascrizione, anche sommaria, di: *a*) intercettazioni irrilevanti ai fini d'indagine, sia per l'oggetto che per i soggetti coinvolti; *b*) intercettazioni parimenti non rilevanti riguardanti dati definiti sensibili dalla legge (art. 268 co. 2 bis c.p.p.); *c*) intercettazioni di conversazioni avvenute tra l'indagato ed il proprio difensore, attinenti al mandato difensivo (art. 103, co. 7, c.p.p.);
- nuova disciplina sul deposito dei verbali e delle registrazioni;
- introduzione di una nuova procedura di acquisizione al fascicolo delle indagini delle intercettazioni rilevanti;
- istituzione dell'archivio riservato delle intercettazioni;
- limiti alla riproduzione delle intercettazioni negli atti cautelari.

Pertanto, nello specifico, la riforma si articolava attraverso i seguenti punti essenziali: *i*) modalità innovativa di redazione del c.d. brogliaccio, ossia dei verbali delle operazioni di ascolto delle conversazioni e delle comunicazioni; *ii*) deposito di tali verbali e il relativo avviso ai difensori; *iii*) l'archivio per la conservazione del materiale intercettato, in attesa della cernita tra quello che doveva confluire nel fascicolo delle indagini di cui all'art.373, comma 5 c.p.p. e quello che doveva restare nell'archivio riservato; *iv*) le richieste al giudice di acquisizione al fascicolo delle indagini delle conversazioni che avrebbero costituito il materiale probatorio; *v*) il relativo provvedimento del giudice e l'eventuale udienza "stralcio"; *vi*) le modalità di trasposizione delle conversazioni nella richiesta di misura cautelare e nella successiva ordinanza cautelare del giudice e, in ultimo, *vii*) l'uso dei captatori informatici nelle operazioni di indagine.

L'art. 9, rubricato "*Disposizione transitoria*", prevedeva, infine, che le disposizioni di cui agli artt. 2, 3, 4, 5 e 7 si sarebbero applicate alle operazioni relative ai "*provvedimenti autorizzativi*" emessi dopo il 26 luglio 2018, mentre per quanto riguarda la modifica introdotta con l'art. 2 comma 1, lett. *b* del decreto, riguardante la pubblicazione dell'ordinanza cautelare, era previsto che la disposizione venisse applicata decorsi dodici mesi dall'entrata in vigore dello stesso.

Prima di occuparci degli ulteriori interventi in materia, si rende necessaria una breve precisazione in ordine alla disciplina intertemporale che ha interessato la (ancora non avvenuta) entrata in vigore della riforma in oggetto.

Come accennato, il D. Lvo. n. 216 del 2017 sarebbe dovuto entrare in vigore a pieno regime il 26 luglio 2018.

Tuttavia, nelle more, il D. L. 25 luglio 2018 n. 91, convertito con modificazioni nella legge n. 108/2018, aveva prorogato il termine al 31.3.2019. A sua volta, la legge di Bilancio 2019 (legge 30 dicembre 2018. n. 145), ne dispose altra proroga al 31.7.2019. Quindi, con il D. L. 4 giugno 2019 n.53 (recante "*Disposizioni urgenti in materia di ordine e sicurezza pubblica*" o cosiddetto decreto *sicurezza bis*), l'efficacia delle nuove disposizioni slittò a "*dopo il 31 dicembre 2019*", ossia al 1° gennaio 2020.

Ciò nonostante, con il D. L. 30 dicembre 2019 n. 161 c.d. "*controriforma Bonafede*", l'entrata in vigore fu ancora prorogata a dopo il 29 febbraio 2020. Nondimeno, la legge 28 febbraio 2020 n.7, di conversione del D.L. 161 del 2019, ha ancora una volta prorogato l'entrata in vigore a dopo il 30 aprile 2020, ossia al 1° maggio 2020.

L'ultimo colpo di coda è, infine, del 30 aprile scorso ed è legato alle vicende relative alla pandemia da COVID – 19.

Il D.L. 30 aprile 2020 n.28, in vigore dal 1° maggio successivo, modificando nuovamente l'art.9 D. Lvo. n. 216/2017, ha previsto che: "*Le disposizioni di cui agli articoli 2, 3, 4, 5 e 7 si applicano ai* procedimenti penali iscritti *dopo il 31 agosto 2020. La disposizione di cui all'art. 2, comma 1, lettera b), acquista efficacia a decorrere dal 1° settembre 2020*".

La riforma dovrebbe, dunque, entrare in vigore dal 1° settembre 2020.

Orbene, nelle more dell'entrata in vigore della c.d. riforma "*Orlando*" è però intervenuta la Legge "*anticorruzione*" del 9 gennaio 2019, n. 3, che ha apportato rilevanti modifiche alla disciplina dell'uso dei captatori informatici relativamente ai reati dei pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo ad anni 5, determinati ai sensi dell'art. 4 c.p.p.

Da un lato, si è resa pienamente operativa dal 31 gennaio 2019 la disciplina dell'impiego dei captatori informatici nelle intercettazioni effettuate su dispositivi mobili per i delitti

di cui all'art. 51 commi 3 *bis* e 3 *quater* c.p.p. (già prevista dal D. Lvo. 216 del 2017, ma con efficacia sospesa).

Dall'altro, con l'abrogazione del comma secondo dell'art. 6 del D. Lvo. 216 del 2017 e l'interpolazione degli artt. 266, co. 2 *bis* e 267, co. 1, c.p.p., è stata completamente estesa anche ai reati dei pubblici ufficiali contro la pubblica amministrazione la disciplina derogatoria di cui all'art. 13 D.L. n. 152/1991 in ordine alla possibilità di effettuare captazioni all'interno dei luoghi di privata dimora *ex* art. 614 c.p., anche in mancanza del fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

Infine, il D. L. n. 161 del 2019, completando il quadro, estende la previsione di cui sopra anche agli incaricati di pubblico servizio. L'art. 4 del D. L. citato, infatti, interviene sia sull'art. 6 del D. Lvo. 216/2017 che sugli artt. 266, co. 2 *bis* e 267, co. 1, c.p.p.

Nondimeno, con la legge di conversione n. 7 del 2020, il Legislatore interviene nuovamente sull'art. 266. co. 2 *bis* c.p.p., inserendo dopo la previsione relativa ai delitti di criminalità organizzata l'inciso "*e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'art.614 del codice penale"* con riferimento ai delitti dei pubblici ufficiali ed incaricati di pubblico servizio commessi contro la pubblica amministrazione.

Delle implicazioni pratiche e procedurali che afferiscono alle accennate riforme ci si occuperà diffusamente nel paragrafo che segue, dedicando particolare riguardo, tuttavia, ai soli interventi che hanno interessato la disciplina dei captatori informatici, esulando dall'oggetto della presente trattazione gli altrettanto importanti mutamenti intervenuti in relazione alla procedura di acquisizione e deposito del materiale intercettato.

Prima di concludere il presente paragrafo, appare opportuno, inoltre, dedicare alcune brevi riflessioni alle differenti discipline delle intercettazioni di comunicazioni informatiche o telematiche di cui all'art. 266 *bis* c.p.p., da un lato, ed alle modifiche apportate in ambito processuale dalla L. n. 48 del 2008 di recepimento della Convenzione di Budapest del 2001 sul *Cybercrime*, dall'altro.

L'art. 266 *bis* c.p.p. è stato introdotto dall'art. 11 della L. 23 dicembre 1993, n. 547 e prevede che: "*Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli*

commessi mediante l'impiego di tecnologie informatiche o telematiche[8]*, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi*".

La norma trova il proprio fondamento nella necessità avvertita dal Legislatore di adeguare l'ordinamento alle nuove forme di comunicazione realizzate attraverso sistemi informatici e, segnatamente, per effetto dell'introduzione dell'articolo in commento, viene ammessa anche l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici.

Per quanto riguarda, invece, le modifiche introdotte dalla L. n. 48 del 2008, come accennato in premessa, essa si è limitata ad apportare dei meri correttivi alle disposizioni già presenti nel codice, senza introdurre nuovi mezzi di ricerca della prova.

Nello specifico, gli interventi più rilevanti ai nostri fini hanno riguardato: la disciplina delle ispezioni (art. 244, comma 2, c.p.p.); gli obblighi e le modalità di custodia (art. 259, 2° comma c.p.p.); i sigilli e i vincoli sulle cose sequestrate (art. 260, 1° e 2° comma c.p.p.) ed infine gli accertamenti urgenti ed il sequestro (art. 354, comma 2 c.p.p.).

Per ogni disposizione sopra richiamata può dirsi che il Legislatore si sia limitato ad ampliare il mero oggetto della norma attraverso l'inserimento di espressioni che rimandano ad attività connesse a "*dati, informazioni e programmi informatici*" e, in alcuni casi, alla garanzia di mantenere inalterato il dato acquisito a seguito delle operazioni.

In definitiva, può sostenersi che l'ambito di applicazione del nuovo sistema si spinge oltre il terreno del *cybercrime*, aprendosi a qualsiasi tipologia di reato per cui si proceda, purché inerente ad attività connesse a dati, informazioni e programmi informatici.

1.1 I principali interventi in materia di captatori informatici.

La disciplina delle intercettazioni di conversazioni o comunicazioni telefoniche o di altre forme di telecomunicazione è disciplinata dagli artt. 266 e ss. c.p.p.

[8] Trattasi dei reati puniti dagli artt. 615 *bis*, 615 *ter*, 615 *quater*, 615 *quinquies*, 617 *quater*, 617 *quinquies*, 617 *sexies*, 640 *ter*, 491 *bis* c.p.

Lo stesso art. 266, c.p.p. disciplina i limiti di ammissibilità del ricorso ad un mezzo di ricerca della prova così invasivo, elencando una serie di reati per i quali e possibile disporre le operazioni di intercettazione.

Attraverso l'interpolazione del comma secondo dell'art. 266 c.p.p., l'art. 4, comma 1, lett. a) del D. Lvo. n. 216 del 2017 ha aggiunto al primo periodo le seguenti parole: "*che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*", ed è stato, inoltre, inserito un nuovo comma 2 *bis*, secondo cui 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'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.

L'art. 6, comma 1 del medesimo D. Lvo. ha, invece, esteso la disciplina di cui all'art. 13 D.L. 152/1991 anche ai delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'art. 4 c.p.p.

Per effetto di tale modifica, quindi, il presupposto per lo svolgimento di intercettazioni per tali delitti, non è più rappresentato dalla "gravità" indiziaria di un reato che rientra nella suddetta categoria, ma dalla mera "sufficienza" di tale base indiziaria e la durata dell'autorizzazione è fissata, inoltre, in quaranta giorni (e non in quindici, come nel caso di procedura ordinaria), mentre quella delle successive proroghe in venti giorni (e non quindici). [9]

Il comma secondo dell'art. 6 dello stesso decreto legislativo ha, invece, limitato in modo rilevante l'applicazione della disciplina speciale prevista per i reati di criminalità organizzata in caso di intercettazioni in luoghi domiciliari, prevedendo la necessità che le intercettazioni di comunicazioni tra presenti nei luoghi di cui all'art. 614 c.p. mediante

[9] "*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. (...) 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 codice penale, l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa. 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.*" (art. 13 D.L. n. 152/1991, convertito con L. n. 203/1991).

l'inserimento di un captatore informatico, nei casi dei delitti dei pubblici ufficiali contro la pubblica amministrazione previsti dal comma 1, avvenga "*quando vi è motivo di ritenere che ivi i stia svolgendo l'attività criminosa*".

Da tale modifica pareva discendere una sorta di "terzo binario" procedurale per quanto riguarda i delitti dei pubblici ufficiali contro la pubblica amministrazione, che si andava ad affiancare alla disciplina ordinaria prevista per i reati "comuni" di cui all'art. 266, co. 1 ed a quella speciale di cui al combinato disposto degli artt. 266, co. 2 *bis* (nuova introduzione) e 13, D.L. n. 152/1991 prevista per i reati di criminalità organizzata di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p.[10]

Tuttavia, tale limitazione è stata successivamente eliminata con l'abrogazione, ad opera della L. n. 3 del 2019, del comma secondo dell'art. 6 e con l'introduzione del riferimento ai delitti dei pubblici ufficiali contro la pubblica amministrazione agli artt. 266, comma 2 *bis* e 267, comma 1 c.p.p.

Pertanto, i presupposti richiesti per l'utilizzo dei captatori informatici su dispositivi portatili in caso di intercettazione di comunicazioni nei luoghi di privata dimora per i delitti di cui all'art. 51 comma 3 *bis* e 3 *quater* c.p.p. e dei pubblici ufficiali contro la pubblica amministrazione, in forza di tale modifica, adesso sono i medesimi.

Il fatto che il Legislatore non avesse deciso di estendere la disciplina derogatoria di cui all'art. 13 del D. L. n. 152 del 1991 anche agli incaricati di pubblico servizio aveva limitato incisivamente l'applicazione pratica della novella.

Infatti, secondo un'interpretazione letterale della disposizione, i delitti in oggetto erano riconducibili solamente a quelli di cui al Capo I, Titolo II del Libro II, c.p., ossia quelli ricompresi tra gli artt. 314 e 335 *bis* c.p. (i quali, peraltro, sono delitti che possono essere commessi anche da incaricati di pubblico servizio). Secondo questa impostazione, quindi, sarebbero stati posti fuori dal campo di applicazione della riforma reati quali la turbata libertà degli incanti (art. 353 c.p.) e la turbata libertà di scelta del procedimento del contraente (art. 353 *bis* c.p.).

[10] Più approfonditamente si veda sul punto: *L. PALMIERI, La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni.,* in *Dir. pen. cont*., fasc. 1/2018, p. 63 ss.

Per ovviare al problema, con l'art. 4 del D. L. n. 161 del 2019 si è provveduto ad estendere la disciplina in oggetto anche agli incaricati di pubblico servizio.

In sede di conversione del decreto, avvenuta con L. n. 7 del 2020, è stato, inoltre, previsto un ulteriore onere motivazionale per il Giudice, prevedendo che nel decreto autorizzativo che abbia ad oggetto delitti dei pubblici ufficiali ed incaricati di pubblico servizio, puniti con la pena della reclusione non inferiore nel massimo ad anni 5 *ex* art. 4 c.p.p. vengano indicate – nel caso di captazioni da espletare all'interno dei luoghi di privata dimora - le "*ragioni che ne giustificano l'utilizzo*".

Oggetto delle due riforme è stato anche l'art. 267 c.p.p., rubricato "*Presupposti e forme del provvedimento*", relativamente ai decreti di autorizzazione di operazioni di captazioni mediante l'inoculazione di *Trojan* sui dispositivi elettronici portatili.

Introducendo una serie di condizioni ulteriori rispetto a quelle richieste per le normali intercettazioni tra presenti, l'art. 267, comma 1, c.p.p. richiede che il decreto di autorizzazione indichi: *i*) "*le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini*"; *ii*) nonché, se si procede per delitti diversi da quelli di criminalità organizzata e dei delitti dei pubblici ufficiali e incaricati di pubblico servizio contro la P.A. "*i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono*".

Per cui, in ogni caso, è stato previsto un onere motivazionale rafforzato per il Giudice in caso di autorizzazione di operazioni di captazione su dispositivi portatili mediante captatore; per i soli reati diversi da quelli sottoposti alla disciplina derogatoria, quando si autorizzano le captazioni, il decreto dovrà indicare, anche indirettamente[11], i luoghi ed il tempo di attivazione del microfono.

Nel primo caso, quindi, potrebbe presumersi che il riferimento alla *necessità* dell'utilizzo del captatore non sia da intendere come *indispensabilità* dello strumento per svolgere le

[11] L'indicazione indiretta dei luoghi e del tempo di attivazione del microfono sembra potersi ricondurre alla natura itinerante del dispositivo, che potrebbe renderne disagevole per il Giudice l'esatta indicazione. Dal momento che i presupposti di cui al comma 1 dell'art. 267, c.p.p. sono previsti a pena di inutilizzabilità del dato captato *ex* art. 271 c.p.p., si è data la possibilità al Giudice di riferirsi, ad esempio, al soggetto portatore del dispositivo o ad incontri specifici dello stesso con altri soggetti, così da non vanificare le potenzialità applicative della nuova modalità di captazione.

indagini. Pertanto, la necessità del ricorso al *Trojan* andrà ponderata caso per caso dal Giudice.

Nella seconda ipotesi, invece, si avranno due distinte modalità applicative dello strumento: sempre consentito, a prescindere dalla diretta o indiretta indicazione dei luoghi e del tempo di attivazione, per i reati che beneficiano della disciplina derogatoria in caso di captazione nei luoghi di privata dimora *ex* art. 266, co. 2 *bis* c.p.p.; indicazione dei luoghi e del tempo di attivazione del microfono quando si proceda per i delitti "comuni" di cui al comma primo dell'art. 266 c.p.p., nonché per tutti quei reati di criminalità organizzata o contro la P.A. che non rientrino nella previsione di cui, rispettivamente, agli artt. 51, comma 3 *bis* e 3 *quater* e 266, co. 2 *bis* (nuovo conio) c.p.p.

Il successivo comma 2 dell'art. 267 c.p.p. prevede la possibilità per il P.M., in caso di urgenza e quando vi è fondato motivo che dal ritardo possano derivare gravi pregiudizi per l'indagine, di disporre con decreto motivato le intercettazioni. Tale decreto andrà immediatamente comunicato (non oltre le 24 ore) al Giudice, il quale, nelle successive 48 ore, deciderà sulla convalida dello stesso.

Qualora le operazioni di intercettazioni avvengano mediante l'inoculazione del captatore ed abbiano ad oggetto, esclusivamente, i delitti previsti dal comma 2 *bis* dell'art. 266 c.p.p., il P.M. potrà disporre con decreto motivato le intercettazioni, ma, a tal fine, oltre ai requisiti di cui al comma 1 dell'art. 267 c.p.p., dovrà precisare *"le ragioni di urgenza che rendono <u>impossibile</u> attendere il provvedimento del giudice*". Per cui, ancora una volta, sembra che il Legislatore abbia predisposto presupposti più stringenti per l'utilizzo del captatore nelle operazioni di intercettazione tra presenti rispetto a quelli richiesti per i provvedimenti aventi ad oggetto i delitti "comuni" di cui al comma 1 dell'art. 266 c.p.p.

Delle operazioni così disposte, ai sensi dei commi primo e secondo dell'art. 268 c.p.p., è redatto verbale in cui è trascritto, anche sommariamente, il contenuto delle conversazioni.

Come precisato sopra, il D. L. n. 161 del 2019 è intervenuto sulle modalità di esecuzione delle operazioni, abrogando l'originario testo della riforma introdotto con il D. Lvo. 216 del 2017, e ha riformulato, inoltre, il comma 2 *bis* dell'art. 268 c.p.p., [12]prevedendo che:

[12] Allo stesso modo il D. L. n. 161 del 2019 ha abrogato il comma 2 ter e ha riformulato i commi 4,5,6,7, e 8 dell'art.268 c.p.p., nonché ha pure abrogato gli artt. 268 *bis,* 268 *ter* e 268 *quater* (introdotti dal D. Lvo.

"*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*".

Per quanto riguarda le concrete modalità attraverso le quali saranno fornite le indicazioni e sarà esercitata la vigilanza da parte del P.M. sembrano non rinvenirsi ragioni ostative all'emanazione, da parte delle Procure, di circolari a carattere generale contenenti le indicazioni da seguire e, inoltre, dal momento che ogni procedimento può richiedere diversi livelli di attenzione in base alla complessità dell'oggetto e al numero dei soggetti coinvolti, non si esclude parimenti che ogni P.M., nell'ambito della propria indagine, possa fornire precipue indicazioni agli operatori di P.G. su come eseguire la redazione dei c.d. brogliacci al fine di rispettare il disposto del nuovo comma 2 *bis* dell'art. 268 c.p.p.

Infine, sul versante dell'uso del captatore su dispositivi portatili per intercettazioni tra presenti, al comma 3 *bis* dell'art. 268, c.p.p., è stata introdotta la possibilità per gli inquirenti, ai sensi dell'art. 348, co. 4, c.p.p., di servirsi dei tecnici privati delle società che forniscono i *Trojans* alle Procure per le operazioni di avvio e/o cessazione delle captazioni.

Relativamente alla possibilità di utilizzare i risultati acquisiti nel corso delle operazioni in procedimenti diversi da quelli nei quali sono disposti, era previsto un generale divieto al comma 1 dell'art. 270, c.p.p., salvo che tali elementi fossero risultati indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.

Il D. Lvo. 216 del 2017 era intervenuto al riguardo, inserendo un ulteriore comma 1 *bis* all'art. 270 c.p.p., prevedendo che: "*i risultati delle intercettazioni tra presenti operate con captatore informatico (…) non possono essere utilizzati per la prova di <u>reati diversi</u> da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza*".

216 del 2017) riportando, salvo alcune modifiche, la disciplina di deposito e acquisizione del materiale ottenuto all'assetto tradizionale ante-riforma.

Quindi, la modifica introdotta con la riforma *Orlando* aveva esteso il divieto di cui al comma 1 dell'art. 270 c.p.p., nel caso in cui si fosse trattato di operazioni compiute mediante captatore su dispositivi portatili, anche per la prova di *reati diversi* e non solo per l'utilizzo del dato acquisito in procedimenti diversi, salva l'indispensabilità per l'accertamento di delitti per i quali è previsto l'arresto in flagranza. Ne derivava, che anche all'interno dello stesso procedimento, in questi casi, il risultato ottenuto mediante captatore – salva l'ipotesi dei delitti per i quali è obbligatorio l'arresto in flagranza – non fosse utilizzabile.

Orbene, il D. L. n. 161 del 2019 è intervenuto anche su questo punto, rimodulando i commi 1 e 1 *bis* dell'art. 270 c.p.p.

Al primo comma dell'art. 270 c.p.p. è stato inserito un ulteriore riferimento ai delitti di cui all'art. 266, co. 1 c.p.p. oltre a quello relativo ai reati che prevedono l'arresto in flagranza. Peraltro, adesso i dati acquisiti, per essere utilizzati in procedimenti diversi da quelli autorizzati, devono risultare "*rilevanti*" ed "*indispensabili*", non più solo indispensabili come nella precedente previsione.

L'utilizzabilità delle intercettazioni così acquisite presuppone, quindi, o che il reato sia tanto grave che per esso il Legislatore abbia previsto l'arresto obbligatorio in flagranza, ovvero che rientri in uno di quei delitti per i quali già *ab origine* sarebbe stato possibile autorizzare l'operazione. Tali elementi, in ogni caso, dovranno risultare rilevanti – e quindi andrà dimostrata tale rilevanza dal P.M. – ed indispensabili per la prova di tali delitti.

In merito alla previsione di cui al comma 1 *bis*, invece, fermo restando quanto previsto dal comma 1, i risultati ottenuti mediante l'inserimento di un captatore informatico su dispositivo mobile "*possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione qualora risultino indispensabili per l'accertamento dei delitti indicati dall'art. 266, co. 2* bis".

Va da subito rilevato che il descritto mutamento di indirizzo si deve ad una importante pronuncia delle Sezioni Unite [13]intervenuta nelle more della maturazione del termine per l'efficacia dell'art. 270 c.p.p. così come interpolato dal D. Lvo. 216 del 2017.

Passando, infine, al tema dei divieti di utilizzazione disciplinati dall'art. 271 c.p.p., può affermarsi che i casi di inutilizzabilità possono essere suddivisi in due categorie: una di carattere *generale* ed una di carattere *particolare*.

Preliminarmente va rilevato che con il D. Lvo. n. 216 del 2017 era stato introdotto un comma 1 *bis* all'art. 271 c.p.p., secondo il quale i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sono da ritenersi in ogni caso inutilizzabili.

In estrema sintesi, dunque, le due categorie di inutilizzabilità sopra accennate possono così suddividersi: la prima (*generale*) concerne quei dati acquisiti fuori dai casi previsti dalla legge (artt. 266 e 103, co. 5, c.p.p.) o senza che si siano osservate le previsioni di cui agli artt. 267 (presupposti e forme del provvedimento autorizzativo) e 268, commi 1 e 3, c.p.p. (mancata o inesatta redazione del verbale e mancato compimento delle operazioni per mezzo degli impianti della Procura, salvo ipotesi espressamente indicate), nonché in caso di trasgressione delle disposizioni relative all'uso dei captatori (artt. 271, commi 1 e 1 *bis*, c.p.p.); la seconda (*particolare*), riguarda invece la summenzionata ipotesi dell'utilizzabilità del dato acquisito in procedimenti diversi da quello autorizzato *ex* art. 270 c.p.p.

[13] Cass. Sez. Unite, n. 51 del 28/11/2019, dep. 2020, *Cavallo e altri.* Della pronuncia citata e dei problemi pratici relativi all'esatta identificazione di cosa abbia inteso il Legislatore con la locuzione "altro procedimento" ci si occuperà più approfonditamente nel paragrafo *2.1.* del presente elaborato, al quale si rimanda.

Capitolo II

SOMMARIO: 1. Il cd. "Virus di Stato". – 2. Problematiche emerse ed emergenti dall'applicazione pratica dello strumento: 2.1 Il "Trojan" nelle intercettazioni. – 2.2 Il "Trojan" nel caso di ispezioni, perquisizioni e sequestro digitale.

1. Il cd. "Virus di Stato".

Chiarito il quadro normativo di riferimento adesso è il caso di occuparsi del captatore informatico e delle sue potenzialità.

Il captatore è uno strumento che infiltrandosi in maniera occulta su un dispositivo elettronico permette di controllarlo in maniera pressocché totale, senza che il proprietario del dispositivo ne sia al corrente.

Lo strumento opera attraverso una tecnica informatica conosciuta come *Remote Control System* (*RCS*), che permette di controllare da remoto il dispositivo *target.*

Il *Trojan* agisce attraverso due moduli, un *client* ed un *server*: il primo è il programma che consente di controllare da remoto il dispositivo; il secondo, invece, è il programma che aggira le difese (*antivirus*) del dispositivo *target*, rendendosi invisibile ai processi di sicurezza dello strumento colpito.

Quest'ultimo, come un vero "cavallo di Troia", si maschera da applicazione di uso comune – come aggiornamento del sistema operativo, un *upgrade* di un'applicazione o una banale *mail* – inducendo il bersaglio a dare seguito all'operazione richiesta dal sistema informatico. Al suo interno il *server* cela, tuttavia, una funzione ignota che consente di creare una *"backdoor*", ossia un collegamento tra uno o più sistemi del dispositivo bersaglio ed il *client* del captatore, consentendo un controllo da remoto del dispositivo.

Perché possa aversi l'infezione ed il successivo controllo del dispositivo *target* è, in ogni caso, necessaria una connessione di rete, sia essa ad *internet*, *ethernet* o *LAN*, pertanto i dispositivi che possono essere oggetto di inoculazione sono tutti quelli dotati della moderna tecnologia *Smart* (*smartphone, tablet, computer, smart tv,* quasi tutte le automobili di recente produzione, etc.).

Il captatore può essere inserito anche manualmente dagli inquirenti, ma in questo caso è necessario che il dispositivo bersaglio sia per qualsiasi motivo a disposizione di quest'ultimi e tale modalità di inoculazione, evidentemente, è quella più rischiosa per il buon esito delle indagini.

Mediante *Trojan* è quindi possibile:

- attivare il microfono, intercettando le comunicazioni che avvengono tra i presenti nella portata del raggio del dispositivo *target*;
- azionare la *webcam*, ottenendo così la possibilità di realizzare *videoclip* e scattare fotografie, o solamente vedere attraverso l'occhio della telecamera;
- captare il traffico dati, sia in arrivo sia in partenza dal dispositivo, sia esso relativo alla navigazione sia esso concernente la posta elettronica (*web mail* e *out look*);
- prendere visione di ciò che appare sullo schermo (*screenshot*) o che viene digitato sulla tastiera (*keylogger*);
- perquisire l*'hard disk* ed estrarne copia, totale o parziale;
- tracciare la posizione GPS;
- *uplodare*, cioè inoculare e memorizzare nel sistema informatico *target* qualsiasi tipo di file salvandolo a piacimento in qualsiasi parte del sistema.[14]

A tali funzionalità deve aggiungersi anche la possibilità di acquisire le comunicazioni che vengono effettuate per mezzo delle moderne applicazioni di *instant messaging* (*Whatsapp* e simili), le quali consentono non solo lo scambio di messaggi, ma anche di immagini, video, *link*, etc.

Tali applicazioni, infatti, a differenza delle tradizionali forme di comunicazione via telefono, che richiedono la collaborazione del gestore di telefonia per sdoppiare il segnale comunicativo e diramarlo in contemporanea verso gli uffici della Procura, utilizzano esclusivamente la rete, prescindendo completamente da qualsiasi rapporto con il gestore di telefonia mobile.

Nello specifico, in questo caso il trasferimento di dati avviene attraverso una sorta di meccanismo di "impacchettamento" delle informazioni (sottoforma di *bits*) che poi vengono inviate a destinazione; ogni singolo "pacchetto" di dati contiene inoltre sia

[14] Si veda *S. ATERNO, Il* Trojan *dalla A alla Z. Esigenze investigative e limitazione della privacy: un bilanciamento necessario*, *Online*, p. 9 ss.

l'indirizzo del mittente che quello del destinatario. Trattandosi tuttavia, nella maggior parte dei casi, di uno scambio di dati criptato (*end to end*, *pin to pin*) non sarà possibile, in caso di intercettazione, conoscere i dati così veicolati e compressi nel "pacchetto", ma solo i soggetti comunicanti e gli orari di inoltro e consegna.

Per cui, in sostanza, gli inquirenti, con i nuovi applicativi di messaggistica, non possono più procedere a un mero ascolto passivo, tramite la captazione di un flusso di dati, delle comunicazioni intercorrenti tra due utenze telefoniche; al contrario dovranno introdursi – con l'inganno mediante il *Trojan* – all'interno del dispositivo ove possono prendere visione delle conversazioni criptate, dal momento che all'interno dello stesso esse risultano in chiaro.

Nell'ambito delle multiformi potenzialità delle quali sono dotati questi strumenti, si suole inoltre distinguere tra due macroaree funzionali riconducibili alla *online search* ed all'*online surveillance.*

La prima consente di perquisire da remoto il contenuto del hard-disk e di farne copia totale o parziale; i dati così acquisiti sono trasmessi in tempo reale o ad intervalli prestabiliti agli organi di investigazione tramite la rete internet in modalità nascosta e protetta. Attraverso i programmi di online *surveillance* è possibile, invece, captare il flusso informatico intercorrente tra le periferiche video, microfono, tastiera, *webcam* ed il microprocessore del dispositivo bersaglio, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che: viene visualizzato sullo schermo (*screenshot*), digitato sulla tastiera (*keylogger*) o pronunciato al microfono.

Come emerge da questa breve disamina delle funzionalità dei captatori informatici, è chiaro che le potenzialità di un simile strumento assumono un peso rilevante per le Procure nella conduzione delle indagini. Tuttavia, la mancanza di una disciplina normativa dedicata a *tipicizzare* le prestazioni del captatore e a regolarne l'uso ha richiesto che gli operatori del diritto riconducessero ciascuna delle varie funzioni a quelle tipologie di mezzi di ricerca della prova ora tipici (ispezioni, perquisizioni, sequestro ed intercettazioni), ora atipici (art. 189 c.p.p.), mentre, da più parti, si sollecitava l'intervento del Legislatore per disciplinare i casi, i modi e i limiti del ricorso a questo moderno

strumento tecnologico di controllo quasi "orwelliano", [15]nel tentativo di trovare un punto di equilibrio tra esigenze investigative e tutela dei diritti fondamentali.

2. Problematiche emerse ed emergenti dall'applicazione pratica dello strumento

Oggetto dei paragrafi che seguono saranno alcune tra le principali problematiche applicative conseguenti all'uso dei captatori nel corso delle indagini.
Invero, ancorché gli spunti di riflessione emergenti dell'applicazione pratica dello strumento siano molteplici, per ragioni contenutistiche e con l'auspicio di non appesantire oltremodo la trattazione, si è operata una cernita tra le più rilevanti problematiche sottese al coordinamento dei nuovi interventi legislativi con la prassi applicativa scandita nel corso degli anni dagli interventi della giurisprudenza di legittimità sul punto.

2.1 Il "Trojan" nelle intercettazioni.

Come è stato accennato, v. *infra,* con la L. n. 3 del 2019 il legislatore ha provveduto ad estendere, quasi integralmente, la disciplina derogatoria di cui all'art. 13 del D. L. n. 152 del 1991 ai più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione.

Infatti, con l'abrogazione del comma secondo dell'art. 6 del D. Lvo. n. 216 del 2017, si era provveduto ad eliminare il limite dell'applicazione dell'uso dei captatori su dispositivi portatili per effettuare intercettazioni tra presenti nei luoghi di privata dimora solo quando vi fosse motivo di ritenere che ivi si stesse svolgendo l'attività criminosa.

Con il successivo D. L. n. 161 del 2019, poi, si era estesa tale previsione anche alla qualifica soggettiva degli incaricati di pubblico servizio ed infine, con la legge di conversione n. 7 del 2020, si era predisposto un peculiare onere motivazionale per il G.i.p. al momento dell'emissione del decreto autorizzativo, prescrivendo che il decreto – per i soli delitti contro la PP.AA. – indicasse anche le "*ragioni che ne giustificano l'utilizzo*".

[15] I captatori sono stati, infatti, definiti da alcuni autori come una sorta di moderno "*panopticon* benthamiano" in grado di vigilare, occultamente e costantemente, sugli aspetti più intimi della vita dei consociati. L'espressione è rinvenibile in *O. CALAVITA, L'Odissea del* Trojan Horse*, tra potenzialità tecniche e lacune normative*, in *Dir. pen. cont.*, fasc. 11/2018, p. 7.

Va inoltre ricordato che l'art. 9 del D. Lvo. n. 216 del 2017, contenente le disposizioni transitorie, si occupava esclusivamente degli artt. 2, 3, 4, 5 e 7, non menzionando l'art. 6 in oggetto, il quale sarebbe dovuto entrare in vigore, quindi, già dall'26 gennaio 2018. Parimenti, l'abrogazione del comma secondo dello stesso articolo è divenuta efficace, con l'entrata in vigore dell'art. 1, comma 3 della L. n. 3/2019, il 31 gennaio 2019.

Ciò posto, sul punto si erano delineati due diversi orientamenti.

Il primo, basato su un'interpretazione strettamente letterale, a fronte dell'espressa esclusione dell'art. 6 D. Lvo. 216/2017 dalla previsione dell'art. 9 medesimo D. Lvo., riteneva già applicabile – a far data dal 26 gennaio 2018 relativamente alla disciplina intermedia (*terzo binario* di cui si veda *infra*) e dal 31 gennaio 2019 per quanto riguarda la previsione definitiva – la disciplina derogatoria prevista per i reati di criminalità organizzata dall'art. 13 D. L. n. 152 del 1991, così come interpretato alla luce dei principi espressi dalla sentenza a Sez. Un. *Scurato*, per i procedimenti aventi ad oggetto i reati dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo ad anni 5, determinati ai sensi dell'art. 4 c.p.p.

Il secondo, invece, sulla scorta di un'interpretazione logico sistematica, riteneva che, dal momento che le altre disposizioni relative alla disciplina dei captatori informatici subivano il deferimento temporale di cui all'art. 9 D. Lvo. cit., ammettere l'immediata applicabilità della sola previsione dell'art. 6 avrebbe comportato un'applicazione disorganica dell'istituto, considerato, peraltro, che la maggior parte delle norme delle quali si era prorogata l'entrata in vigore, riguardava proprio le modalità operative delle procedure di acquisizione, deposito e archiviazione dei dati captati (c.d. archivio digitale o riservato).[16]

[16] Secondo tale impostazione di pensiero, in sintesi, il fatto che l'utilizzo dei captatori informatici sia stato disciplinato per la prima volta da una norma (art. 4, D. Lvo. 216/2017) che ancora non è entrata in vigore comprometterebbe anche la successiva applicabilità dell'art. 6 medesimo D. Lvo., il quale, pur ammettendone l'efficacia già a far data dal 26 gennaio 2018 e, a seguito dell'abrogazione del comma secondo ad opera della L. 3 del 2019, dal 31 gennaio 2019, avrebbe ad oggetto l'applicazione di un istituto disciplinato nei suoi tratti essenziali (artt. 266, co. 2 *bis* c.p.p., 267 c.p.p., 268, co. 3 *bis*, 270 e 271 c.p.p.) da una norma non ancora efficace. Alla luce di una simile interpretazione, pertanto, anche la disciplina relativa ai più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione sconterebbe la postergazione dell'entrata in vigore dell'art. 4 D. Lvo. 216 del 2017. L'art. 1, comma 4, della legge n. 3 del 2019, in particolare, non ha disciplinato l'intera materia del captatore informatico, essendosi limitato, invece, ad estendere la disciplina dell'art. 266, comma 2-*bis*, c.p.p. ai reati più gravi dei pubblici ufficiali contro la pubblica amministrazione. La modificazione non riguarda il testo originario dell'art. 266 c.p.p., ma il nuovo comma risultante dalle modifiche del D. Lvo. n. 216 del 2017, non ancora vigente o, quanto

Secondo la prima delle due tesi di pensiero esposte, ad una simile interpretazione non avrebbero ostato gli interventi operati - prima dall'art. 4 del D. Lvo. 216 del 2017 e poi dall'art. 1, co 4 della L. n. 3 del 2019 - agli artt. 266 e 267, dei quali, invece, era stata rinviata l'entrata in vigore.

Con riferimento all'art. 266, co. 2 *bis*, c.p.p., si tratterebbe di disposizione avente ad oggetto i "*limiti di ammissibilità*" dello strumento in esame, rendendo "*sempre consentita*" l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile anche per i reati contro la pubblica amministrazione[17]. Oltretutto, in tali casi, qualora si dovesse ritenere non ancora pienamente operativa la disposizione di cui all'art. 266, co. 2 *bis*, c.p.p., perché oggetto di una modifica introdotta dall'art. 4 del D. Lvo. 216 del 2017, la norma applicabile sarebbe comunque l'art. 13 del D. L. 152 del 1991, al quale fa espresso riferimento l'art. 6, comma 1, del D. Lvo. cit., già in vigore.

Per quanto riguarda, invece, la previsione di cui all'art. 267 c.p.p., avente ad oggetto i presupposti del decreto autorizzativo, deve rilevarsi che anche questa norma della legge n. 3 del 2019 è entrata in vigore, non essendo stato differita la sua efficacia nel tempo.

Per cui, qualora si ritenesse tale riforma inapplicabile perché, anche in questo caso, incide su una disposizione del codice riformata dal D. Lvo. n. 216 del 2017, sarebbe comunque possibile il ricorso al captatore informatico anche per le indagini in tema di delitti di pubblici ufficiali contro la pubblica amministrazione in forza del citato art. 6, comma 1, D. Lvo. n. 216 del 2017.[18]

Sul punto, è da ultimo intervenuta una decisione delle Sezioni Unite civili della Suprema Corte di Cassazione, la n. 741 del 2020, la quale, occupandosi di un procedimento disciplinare a carico di un magistrato (il riferimento è alla nota vicenda *Palamara*, legata

meno, non applicabile. Ne consegue che la disciplina introdotta dalla legge n. 3 del 2019 non può trovare immediata applicazione, perché "*subisce*" il differimento previsto per le disposizioni del D. Lvo. n. 216 del 2017, rispetto al quale non ha una propria autonomia.

[17] Deve rilevarsi, in ogni caso, che la modifica in oggetto è stata operata con una norma del 2019 che, a seguito dello spirare dell'ordinario periodo di *vacatio legis*, oggi è pienamente efficace.

[18] Non occorrerebbe rispettare, pertanto, le peculiari garanzie in tema di motivazione "rafforzata" del decreto autorizzativo, ossia indicare le ragioni per le quali lo strumento è necessario nonché le circostanze di tempo e di luogo in cui è attivato il microfono. Per un'analisi più approfondita sul tema, si consiglia, *L. GIORDANO, Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte.*, in *Sist. Pen.*, 4/2020, p. 31 ss.

allo scandalo delle nomine orchestrate dall'ormai ex consigliere del C.S.M.), ha accolto il primo degli orientamenti esposti, ritenendo utilizzabili nel procedimento disciplinare *de quo* i risultati acquisiti dagli inquirenti mediante l'inoculazione di un captatore informatico su un dispositivo portatile, effettuate in forza del richiamo all'art. 13 del D. L. n. 152 del 1991 contenuto nell'art. 6 D. Lvo. n. 216 del 2017, così come interpolato dalla legge n. 3 del 2019.

In particolare, è stato rilevato che l'art. 6 d.lgs. n. 216 del 2017 è entrato in vigore il 26 gennaio 2018, non essendo tale disposizione indicata tra quelle per le quali l'art. 9 del medesimo decreto legislativo ha disposto il differimento della loro entrata in vigore.

La successiva modifica di tale norma, introdotta dall'art. 1, comma 3, della L. n. 3 del 2019 è a sua volta entrata in vigore, a differenza di altre disposizioni della medesima legge per le quali il legislatore ha differito l'entrata in vigore al 1° gennaio 2020, il decimoquinto giorno dalla pubblicazione della legge sulla G.U., avvenuta il 16 gennaio 2019.

Pertanto, secondo la Corte, «*la possibilità di utilizzare il captatore informatico preesiste e prescinde dalla modifica del testo codicistico operata dall'art. 4 del d. lgs. 216 del 2017, e deriva direttamente, come hanno precisato le sezioni unite penali, dall'art. 13 del d.l. 152 del 1991, norma il cui ambito di efficacia è stato esteso dall'art. 6 del d. lgs. 261 del 2017 anche ai più gravi reati contro la p.a.*».

L'art. 4 del D. Lvo. n. 216 del 2017 era intervenuto anche sul testo dell'art. 270 c.p.p., avente ad oggetto l'utilizzabilità in altri procedimenti degli esiti delle captazioni.

Il comma primo dell'art. 270 c.p.p. prevedeva una generale inutilizzabilità dei risultati delle intercettazioni in procedimenti diversi da quelli per i quali le operazioni erano state autorizzate, salvo che si trattasse di elementi indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.

Il D. Lvo. n. 216 del 2017 aveva aggiunto il seguente comma 1 *bis*, estendendo tale divieto – per le operazioni effettuate tramite captatore informatico su dispositivi portatili – anche alla prova di "reati diversi" all'interno del medesimo procedimento.

Pertanto, da un lato, il dato letterale era un ulteriore elemento a favore di quella tesi che riteneva le nozioni di diverso reato e diverso procedimento come entità diverse e non

quali sinonimi dello stesso segmento procedurale; dall'altro, con tale intervento, pareva che il Legislatore avesse voluto evitare un eventuale uso trasversale dei risultati acquisiti anche all'interno del medesimo procedimento quando si fosse proceduto mediante *Trojan*.

Orbene, prima di procedere all'analisi degli ulteriori interventi normativi sul punto, si rende necessario chiarire cosa debba intendersi per "*diverso procedimento*".

La differenza tra reato diverso e procedimento diverso trova fondamento, stando alla giurisprudenza, non sulla mera diversità numerica della registrazione dei procedimenti, ma sulla diversità sostanziale dei fatti storici individuati.

Condivisibile ritenere che nell'ambito dello stesso procedimento si deve applicare la regola del «*diverso procedimento*» quando con l'intercettazione si accertano reati non connessi (criteri ex art.12 e 16 c.p.p.).

Preliminarmente va rilevato che, secondo pacifica giurisprudenza, la legittimità delle captazioni andava valutata al momento dell'autorizzazione delle intercettazioni e non una volta acquisito il dato, poiché la genuinità dell'operazione doveva discendere da un decreto autorizzativo che fosse legittimo da principio, e non legittimato *ex post* in forza di una eventuale coincidenza tra i risultati acquisiti ed i presupposti normativi richiesti.

Per questa giurisprudenza, in caso, pertanto, di indagini unitarie o connesse o collegate, anche se non effettivamente riunite o viceversa suscettibili di separazione, per il nuovo reato scoperto durante l'intercettazione i risultati della stessa sarebbero stati utilizzabili, in quanto «procedimento diverso» non equivale a «reato diverso».

Ne derivava che in caso di eventuale modifica del reato o dell'imputazione, se il decreto autorizzativo fosse stato ritenuti legittimo fin dal principio, il dato così acquisito sarebbe stato utilizzabile.[19]Secondo questa impostazione, quindi, Il divieto di utilizzazione non

[19] Cfr. *Cass. Sez. VI*. 26.8.2016 n. 35536. *Rv*. 267598: "*i risultati delle intercettazioni telefoniche disposte per un reato rientrante tra quelli indicati nell'art. 266 c.p.p. sono utilizzabili anche relativamente ad altri reati per i quali si procede nel medesimo procedimento, pur se per essi le intercettazioni non sarebbero state consentite*";
Cass. Sez. VI, 4.7.2017 n.31984, *Rv.* 270431: "*qualora il mezzo di ricerca della prova sia legittimamente autorizzato all'interno di un determinato procedimento per uno dei reati di cui all'art. 266 c.p.p. i suoi esiti sono utilizzabili senza alcun limite per tutti gli altri reati relativi al medesimo procedimento*."; pure, *Cass. Sez. VI*, 1.7.2015 n. 27820, *Rv*. 264087; *Cass. Sez.* VI 25.11.2015 n. 50261, *Rv*. 265757.

opererebbe quando si tratti del medesimo filone di indagine, o comunque di indagini anche solo collegate e vale anche per i reati emersi successivamente e per provare i quali non sarebbe ammessa l'intercettazione ai sensi dell'art.266 c.p.p.

Tuttavia, tale orientamento, recentemente è stato radicalmente rimeditato dalla sentenza a Sezioni Unite della Corte di Cassazione n. 51 del 2020, *Cavallo*.

La Corte con questa pronuncia ha affermato due principi di diritto: «*il divieto di cui all'art. 270 c.p.p. 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 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 c.p.p. a quelli in relazione ai quali l'autorizzazione era stata* ab origine *disposta, sempreché rientrino nei limiti di ammissibilità previsti dalla legge*»; l'utilizzazione dei risultati è vietata quando il reato diverso da quello in relazione al quale era stata disposta l'autorizzazione, anche se con questo connesso, non rientra fra quelli per cui l'intercettazione è ammissibile (art. 266 c.p.p.).

Secondo il primo principio, dunque, l'inutilizzabilità non opera solo quando si tratti di reati connessi ex art. 12 c.p.p., e solo se per tali reati l'intercettazione risulti ammissibile (ai sensi degli artt. 266 e 267 c.p.p.).

Per il Supremo Consesso, la soluzione va individuata facendo riferimento alla *ratio* del divieto di utilizzazione.

Lo statuto costituzionale delle intercettazioni richiede la predeterminazione tassativa dei presupposti di legge e un provvedimento motivato dell'autorità giudiziaria.[20]

Circoscrivere l'utilizzabilità dei risultati è una garanzia destinata ad evitare che gli effetti dell'interferenza si moltiplichino al di là di quanto strettamente necessario.

Il divieto di cui all'art. 270 comma 1 c.p.p. ha, dunque, lo scopo di mantenere costante il collegamento con le circostanze che giustificano la violazione del segreto delle comunicazioni e con i motivi addotti nell'autorizzazione del giudice, che includono, oltre

[20] L'autorizzazione del giudice infatti, secondo l'art. 15 Cost., non si limita a legittimare il ricorso al mezzo di ricerca della prova, ma circoscrive l'utilizzabilità del risultato ai fatti-reato che all'autorizzazione stessa risultino riconducibili: essa, infatti, deve dar conto "*dei soggetti da sottoporre al controllo*" e dei "*fatti costituenti reato per i quali in concreto di procede*". Cfr. Corte Cost., sentenza n. 366 del 1991.

all'accertamento degli indizi di un reato fra quelli previsti dalla legge, anche la valutazione dell'assoluta indispensabilità ai fini della prosecuzione delle indagini.

Ogni divieto di utilizzazione viene meno quando si scoprono delitti diversi per i quali è obbligatorio l'arresto in flagranza. È un caso tipicamente eccezionale e non occorre la connessione tra i reati. La scelta, del resto, non ha altra logica che quella dettata dalle esigenze di politica criminale, che sarebbero eccessivamente sacrificate qualora dall'intercettazione si ricavasse la prova di un reato particolarmente grave senza che si potesse farne uso, se non come *notitia criminis*.

Dunque, le Sezioni unite hanno optato per una soluzione intermedia.

Affrontando il problema concernente l'identità o la diversità dei procedimenti, hanno concluso che all'autorizzazione iniziale devono ritenersi riconducibili anche quei fatti di reato che si trovino in un rapporto di connessione sostanziale con quello per il quale l'intercettazione era stata disposta.

Il legame, cioè, sarebbe in tal caso originario e indipendente dallo specifico procedimento, in quanto di carattere oggettivo e predeterminato. La connessione ai sensi dell'art. 12 c.p.p. giustificherebbe l'utilizzazione dei risultati dell'intercettazione anche per i reati non espressamente contemplati nell'autorizzazione.

Alla luce di tali considerazioni, pertanto, una relazione occasionale, quale quella derivante dal collegamento delle indagini ai sensi dell'art. 371 c.p.p., o dall'appartenenza ad un medesimo contesto investigativo, dimostra che si è in presenza di procedimenti diversi. In questi casi, conseguentemente, opererà il divieto di cui all'art. 270 comma 1 c.p.p. (salva sempre l'eccezione concernente i delitti per i quali è obbligatorio l'arresto in flagranza).

Secondo l'altro principio di diritto enunciato, infine, l'utilizzazione dei risultati è vietata quando il reato diverso da quello in relazione al quale era stata disposta l'autorizzazione, anche se con questo connesso, non rientra fra quelli per cui l'intercettazione è ammissibile *ex* artt. 266 e 267 c.p.p.

Si tratta di una rigorosa applicazione della legge, posto che l'art. 266 c.p.p. vieta l'impiego di questo mezzo di indagine per i reati che non superino una soglia minima di gravità. I

risultati sono dunque inutilizzabili ai sensi dell'art. 271 c.p.p., poiché derivano da intercettazioni eseguite "*fuori dai casi consentiti dalla legge*".

Le conclusioni alle quali è pervenuta la Corte con la sentenza in esame hanno indotto il Legislatore del 2019 ad apportare ulteriori modifiche, con il D. L. n. 161 del 2019 e la relativa legge di conversione, all'art. 270 c.p.p.

Il comma 1 dell'art. 270 c.p.p. è stato così modificato: "*I risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'articolo 266, comma 1*".

Si estende l'ambito della possibilità di usare le intercettazioni originarie anche ai procedimenti che riguardino i reati per cui l'intercettazione è ammissibile (art.266 c.p.p.).

Orbene, in disparte l'inserimento di un pleonastico riferimento alla natura "rilevante" ed "indispensabile" dell'elemento acquisito, la novella sembra estendere leggermente la portata applicativa del principio espresso dalle Sezioni Unite.

Se infatti la Corte aveva ritenuto utilizzabili i risultati acquisiti qualora si fosse trattato di procedimenti connessi *ex* art. 12 c.p.p. e fossero state comunque rispettate le previsioni di legge, adesso la nuova norma amplia la possibilità di usare le originarie intercettazioni anche per i procedimenti diversi che abbiano per oggetto un reato per cui è consentita l'intercettazione *ex* art. 266, comma 1, c.p.p., quando questi risultino "rilevanti" e "indispensabili" per l'accertamento di tali reati.

Pare, dunque, che il reato diverso emergente nel corso delle operazioni, purché rientrante nei parametri di gravità previsti dall'art. 266, comma 1, c.p.p., finisca col legittimare *ex post* i risultati acquisiti, permettendone l'utilizzo anche in procedimenti diversi (e quindi non connessi *ex* art. 12 c.p.p.).

Si vedrà, dunque, come la futura applicazione pratica dell'istituto ad opera della giurisprudenza coordinerà il novellato art. 270 c.p.p. con i principi espressi dalle Sezioni Unite *Cavallo*.

La riforma predispone, inoltre, una disciplina dedicata con riferimento ai risultati acquisiti mediante l'impiego di captatori informatici su dispositivi mobili.

Il successivo comma 1 *bis* dell'art. 270 c.p.p., infatti, così si esprime: "*Fermo restando quanto previsto dal comma 1, i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione qualora risultino indispensabili per l'accertamento dei delitti indicati dall'articolo 266, comma 2-bis*".

Ne deriva, dunque, una completa utilizzabilità dei risultati così acquisiti solo per i particolari reati enumerati al comma 2 *bis* dell'art. 266 c.p.p., ossia i delitti di criminalità organizzata di cui all'art. 51 commi 3 *bis* e 3 *quater* c.p.p. ed i delitti dei pubblici ufficiali e degli incaricati di pubblico servizio commessi nei confronti della pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo an anni cinque, determinata ai sensi dell'art. 4 c.p.p.

È stata, dunque, consentita la prova di ulteriori reati rientranti nella previsione di cui all'art. 266 co. 2 *bis*, c.p.p., previo giudizio di "indispensabilità" probatoria degli esiti conseguiti durante le operazioni per le quali era stato autorizzato l'impiego di captatori informatici su dispositivi portatili.

In questo modo, pare che il Legislatore del 2019 abbia voluto mitigare il rigore della precedente riforma *Orlando*, che aveva il fine di restringere l'ambito di operatività – seppure indirettamente – del *Trojan horse* (Cfr. art. 270, comma 1 *bis*, c.p.p. ante-riforma 2019).

In ogni caso, l'inciso "*fermo restando quanto previsto dal comma 1*" sembra deporre a favore di un'interpretazione secondo la quale anche i risultati acquisiti mediante l'utilizzo di captatori informatici su dispositivi mobili dovrebbero ritenersi inutilizzabili per i procedimenti diversi, intesi come procedimenti non collegati ai sensi dell'art. 12 c.p.p. al procedimento principale, salvi i casi in cui gli elementi così acquisiti risultino indispensabili per la prova di reati rientranti nella previsione d cui all'art. 266, co. 2 *bis* c.p.p., per i quali le captazioni sono "*sempre consentite*".

2.2 Il "Trojan" nel caso di ispezioni, perquisizioni e sequestri online.

Nel presente paragrafo si avrà modo di analizzare alcuni impieghi del captatore effettuati dalle Procure nel corso delle indagini che si discostano dalla disciplina dalle intercettazioni.

Infatti, come accennato, le multiformi potenzialità applicative dello strumento, spesso hanno permesso un uso distorto o quantomeno dubbio dei *Trojan* da parte degli inquirenti, che nel silenzio della legge hanno sfruttato in maniera efficace le potenzialità dei captatori per effettuare operazioni di *online search* e *online surveillance*, riconducendo tali attività talora alle ipotesi tipiche delle ispezioni, perquisizioni o del sequestro, talaltra ricorrendo alla prova atipica *ex* art. 189 c.p.p. per introdurre all'interno del procedimento gli elementi così acquisiti.

Preliminarmente, si ritiene opportuno ricordare brevemente cosa debba intendersi per ispezione, perquisizione e sequestro secondo quanto previsto dal dato normativo.

L'ispezione (art. 244 c.p.p.) consiste nell'osservare e descrivere persone, luoghi e cose allo scopo di accertare le tracce e gli altri effetti materiali del reato. Se il reato non ha lasciato tracce o effetti materiali (o se nel frattempo questi sono andati persi per qualsiasi motivo) l' A.G., se possibile, cerca di individuare il modo, il tempo e le cause di eventuali modificazioni, se è il caso, disponendo rilievi ed ogni altra operazione tecnica, anche in relazione a sistemi informatici e telematici, adottando misure tecniche atte ad assicurare la conservazione e l'immodificabilità del dato acquisito (art. 244, co. 2, c.p.p.).

Per cui, tale mezzo di ricerca della prova consiste sostanzialmente nell'osservazione esterna delle persone, dei luoghi o delle cose ed ha carattere prevalentemente descrittivo.

La perquisizione (art. 247 c.p.p.) consiste, invece, nel ricercare il corpo del reato o le cose pertinenti al reato al fine di assicurarle al procedimento, ovvero una persona da arrestare. La perquisizione può essere sia personale che locale e, per ciò che rileva ai nostri fini, a seguito della citata novella avvenuta con L. n. 48 del 2008, anche informatica. Quest'ultima, ai sensi dell'art. 247, comma 1 *bis* c.p.p., è disposta "*quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico*", anche qualora tale

sistema sia protetto da misure di sicurezza, e, anche in questo caso, devono essere adottate misure tecniche volte ad impedire l'alterazione dei dati e ad assicurarne la conservazione.

Infine, tra i tipi di sequestro, il sequestro probatorio di cui all'art. 253 c.p.p. è annoverato dal codice tra i mezzi di ricerca della prova e consiste, fondamentalmente, nella creazione di un vincolo di indisponibilità su una cosa mobile o immobile, attraverso uno spossessamento coattivo al fine di conservare immutate le caratteristiche della stessa e permettere, così, l'accertamento dei fatti.

Solitamente, ai sensi dell'art. 252 c.p.p., il sequestro segue alla perquisizione.

Tali mezzi di ricerca della prova sono atti che, sebbene compiuti "a sorpresa" per garantirne il buon esito, comunque una volta espletati vengono a conoscenza del soggetto che li subisce.

Le cosiddette ispezioni o perquisizioni *online* ed anche i sequestri di dati compiuti servendosi del captatore informatico hanno, invece, carattere occulto e spesso si sottraggono alle garanzie codicistiche, quali la consegna di una copia del decreto che dispone le operazioni (ispezioni di luoghi e di cose, perquisizioni e sequestro), ovvero l'avviso all'interessato della facoltà di farsi assistere da persona di fiducia, purché prontamente reperibile e idonea (ispezioni personali).

Con riferimento alle "nuove" e innominate modalità di mezzi di ricerca della prova espletate mediante captatore informatico, può operarsi una distinzione basandosi sulle funzionalità proprie dello strumento.

Nello specifico: quando il *virus* viene adoperato con una funzione di *keylogger* o per effettuare *screenshot* siamo in presenza di una mera attività di osservazione esterna che potrebbe essere ricondotta alla disciplina delle ispezioni; quando lo strumento viene adoperato per effettuare un'esplorazione del contenuto del disco rigido del dispositivo *target* potrebbe invece parlarsi di una perquisizione *online* ed infine, quando all'esplorazione del disco rigido del dispositivo consegua l'apprensione mediante copia dei dati in esso contenuti, tale operazione potrebbe essere ricondotta all'istituto del sequestro.

Tuttavia, come accennato, rilevano alcune differenze tra le modalità tipiche e quelle appena analizzate.

Infatti, la natura occulta dello strumento e la possibilità di agire costantemente sul dispositivo *target* servendosi di una connessione internet, permettono o permetterebbero un controllo ed una captazione continuative – oltreché occulte - che, invece, non sarebbero praticabili con delle tradizionali ispezioni, perquisizioni o mediante il sequestro.

Ciò posto, si rende opportuna l'analisi di alcune pronunce della Corte di legittimità che si sono occupate di una serie di problematiche relative ai diversi impieghi dei captatori nel corso delle indagini.

La più risalente è la nota sentenza *Virruso* (Cass. sez. 5, Sentenza n. 16556 del 14/10/2009), con la quale la Corte ha finito per conferire legittimazione indiretta ai mezzi atipici di ricerca della prova, pur avendo risolto il problema non tanto dalla prospettiva dello strumento di "cattura" utilizzato, quanto dal legittimo ingresso nel processo dell'elemento probatorio così raccolto, ai sensi dell'art. 189 c.p.p.

In questo caso l'utilizzo del captatore era stato disposto con un decreto del P.M. ed aveva ad oggetto la captazione ed il monitoraggio continuo, nonché occulto, del sistema informatico interessato, protrattosi per otto mesi e sottratto ad un controllo giurisdizionale.

Secondo la difesa tali operazioni andavano ricondotte alla disciplina delle intercettazioni telematiche di cui all'art. 266 *bis* c.p.p. e, per l'effetto, avrebbero richiesto un provvedimento autorizzativo motivato del giudice delle indagini preliminari, dietro richiesta del pubblico ministero. Ancora, oltre che di prove inutilizzabili *ex* art. 191, in quanto acquisite in violazione della disciplina normativa, si sarebbe trattato, ancor prima, di "prove incostituzionali", perché acquisite in spregio dei diritti fondamentali di cui agli artt. 14 e 15 Cost.

Secondo la Suprema Corte, tuttavia, nel caso di specie, il ricorso al captatore informatico per intercettare e clonare in tempo reale il flusso unidirezionale di informazioni (presenti e future) veicolate dall'utilizzatore sul proprio *computer* attraverso i comuni *software* di videoscrittura, non poteva ritenersi in conflitto con le tutele garantite dagli artt. 14 e 15 della Costituzione.

In relazione all'art. 15 Cost., i giudici rilevano come nel caso in esame si fosse in presenza di una semplice circolazione di dati contenuta all'interno del sistema informatico [21]del dispositivo intercettato che esula dalla concezione di comunicazione, la quale implica un flusso di dati tra più soggetti o quantomeno tra più sistemi infirmatici.

Per quanto riguarda, invece, la violazione dell'art. 14 Cost. i giudici si sono limitati ad escludere tale possibilità sulla base dell'ubicazione fisica del personal computer, che si trovava all'interno di un ufficio comunale accessibile ad una platea indistinta di soggetti e dunque sottratto all'esclusiva disponibilità del soggetto indagato.

Su quest'ultimo rilievo, tuttavia, bisogna soffermarsi ulteriormente per una serie di ragioni che potrebbero portare a ritenere insoddisfacente la risposta fornita dalla Corte.

In primo luogo, va rilevato come sin dalla legge 574 del 1993, che ha introdotto nel codice penale nuove norme in materia di criminalità informatica (artt. artt. 615 *ter*, 615 *quater*, 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.), le riflessioni dei penalisti, suffragate dal tenore letterale della relazione alla legge citata, avevano elaborato un nuovo bene giuridico tutelato da tali norme (segnatamente artt. 615 *ter* e 615 *quater* c.p.), consistente nel "domicilio informatico" quale "*espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti essenziali agli articoli 614 e 615 del codice penale*".[22]

Oltretutto, da tale punto di partenza, soprattutto alla luce di un'importante sentenza del *Bundersverfassungsgericht* tedesco del 2008[23] con la quale è stato riconosciuto un nuovo

[21] *"una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del personal computer."* (Cass. sez. 5, Sentenza n. 16556 del 14/10/2009).

[22] Così la relazione ministeriale del disegno di legge, p. 9.

[23] *Bundersverfassungsgericht*, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09, in *Dir. pen. cont*., Archivio 2010-2019 (Online) con commento di *A. VENEGONI* e *L. GIORDANO*, 8 maggio 2016. La Corte costituzionale tedesca, pur dichiarando la normativa del *Land Nord Rhein Westfalen* incostituzionale in quanto non rispettosa dei principi di proporzionalità e determinatezza, non ha escluso in assoluto l'ammissibilità del captatore informatico. Interessante l'argomento reputato decisivo per la citata declaratoria di illegittimità. Ritenendo insufficienti le garanzie offerte dalle norme costituzionali a tutela della segretezza delle telecomunicazioni (art. 10 *Grundgesetz*, d'innanzi *GG*) e dell'inviolabilità del domicilio (art. 13 *GG*) e, altresì, del diritto all'autodeterminazione informativa, il *Bundesverfassungsgericht* ha preso atto dell'esistenza di un nuovo diritto fondamentale "alla garanzia della segretezza e integrità dei sistemi informatici" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). Un diritto di rango costituzionale, ricavato da quella sorgente di diritti inviolabili che è la *Menschenwürde* (artt. 1, comma 1 e 2, comma 1 *GG*). Per un approfondimento sul punto *F. IOVENE, LE C.D. PERQUISIZIONI ONLINE TRA NUOVI DIRITTI FONDAMENTALI ED ESIGENZE DI ACCERTAMENTO PENALE,* in *Dir. pen. cont.,* fasc. 3-4/2014, p. 329 ss.

diritto fondamentale "*alla garanzia della segretezza e integrità dei sistemi informatici*", anche nel nostro ordinamento – sulla scorta dell'art. 2 Cost. quale norma "aperta" all'interno della quale ricondurre il diritto alla riservatezza e dell'art. 14 Cost. relativo alla tutela del domicilio – si potrebbe ipotizzare un diritto di tal fatta, dal momento che il "luogo digitale", spesso oggetto degli accertamenti in esame, contiene informazioni rilevanti e sensibili, che senza una puntuale regolamentazione degli istituti adoperati, rischiano di essere analizzate o apprese indistintamente, sia che abbiano inerenza ai fatti oggetto dell'indagine sia che ne siano estranee.

Peraltro, il concetto di domicilio informatico, per quanto innovativo e di certo rilevante, potrebbe addirittura risultare inadeguato alla tutela dei nuovi diritti "virtuali" appena accennati, qualora dovesse accogliersi la tesi che identifica gli spazi virtuali adoperati dagli utenti come una vera e propria "estensione" della personalità dell'individuo.

Invero, le conclusioni alla quali era pervenuta la Corte con la sentenza *Virruso* sembrano essere state condivise e, per certi versi, sviluppate dalla sentenza *Occhionero* (Cass., Sez. V, 30 maggio 2017, n. 48370).

In questa pronuncia, infatti, la Corte, oltre a ritenere utilizzabili i *virus* informatici anche per le intercettazioni di cui all'art. 266 *bis* c.p.p., smentisce le prospettazioni difensive, secondo le quali più che di un'intercettazione telematica si sarebbe trattato di un'operazione di ispezione/perquisizione con conseguente sequestro del flusso di dati contenuti nel dispositivo.

I giudici, in relazione alla seconda censura, rilevano che è irrilevante la modalità con la quale è stata effettuata l'analisi o la captazione sul dispositivo in quanto: *a*) c'erano stati dei decreti di sequestro emessi dal P.M. che avevano avuto esito negativo a causa del comportamento ostruzionistico tenuto dai due imputati e *b)* che il decreto autorizzativo avente ad oggetto le intercettazioni disposte *ex* art. 266 *bis* c.p.p. era idoneo a "coprire" le eventuali risultanze acquisite attraverso il monitoraggio costante del dispositivo in uso ai due indagati, anche nel caso in cui non si fosse trattato effettivamente di un flusso di dati telematici intercorrente tra più sistemi come richiesto dalla norma.

Per concludere l'analisi relativa alle ipotesi di utilizzo di captatori informatici per effettuare ispezioni o perquisizioni *online*, si ritiene necessario analizzare un'ulteriore pronuncia della Corte di legittimità avente ad oggetto perquisizioni effettuate a fini

meramente esplorativi a carico di una compagnia aerea, col fine di individuare soggetti trasportatori di sostanze stupefacenti (c.d. ovulatori) mediante l'analisi delle prenotazioni dei voli da questi effettate.

Il riferimento è a Cass. Sez. 4, Sentenza n. 19618 del 17/04/2012, con la quale la Corte ha rigettato il ricorso della Procura in ordine all'annullamento di un decreto del P.M. avente ad oggetto il sequestro e la perquisizione delle credenziali di accesso al sistema di *booking online* di una nota compagnia aerea, motivato dall'esigenza di poter identificare per tempo - in base ad una serie di parametri sintomatici desumibili dalle modalità di prenotazione dei voli (soprattutto eseguite last minute, in orario notturno, con rientro programmato entro pochissimi giorni dall'arrivo) - i passeggeri sospettabili di fungere da corrieri internazionali di stupefacenti.

In questo caso i giudici di legittimità hanno precisato che "*è da escludere un preventivo ed indefinito monitoraggio del sistema predetto in attesa dell'eventuale e futura comparsa del dato da acquisire a base delle indagini: si verrebbe altrimenti ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione*".

Il pregio di tale decisione è quello di fare luce sulle problematiche cui darebbe luogo la perquisizione informatica allorquando realizzata con modalità tali da fuoriuscire dai confini dell'art. 247 c.p.p. per arrivare a lambire quelli del mezzo atipico di ricerca della prova.[24]

La Cassazione, sostanzialmente, ha ribadito il divieto di condurre indagini di tipo esplorativo, in quanto tali non fondate sulla esistenza di specifiche notizie di reato ma indirizzate, essenzialmente, a raccoglierne, grazie all'impiego "*a strascico*" dei mezzi previsti dal codice per la ricerca della prova.

In merito, invece, alle ipotesi di utilizzo di un captatore informatico per effettuare dei sequestri *online*, degna di nota è la pronuncia Cass., Sezione IV Penale, sentenza n. 40903 del 28 giugno 2016, *Grassi ed altri.*

[24] Per un approfondimento si veda *L.BATTINERI, LA PERQUISIZIONE ONLINE TRA ESIGENZE INVESTIGATIVE E RICERCA ATIPICA DELLA PROVA* in *Digital forensics, Online.*

In un'indagine per associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti, gli inquirenti inserivano un *Trojan* all'interno di un computer collocato all'interno di un *Internet Point* utilizzato dagli indagati per accedere a unico *account* di posta elettronica su "*hotmail.com*". Attraverso il *Trojan* gli inquirenti acquisivano la *password* di accesso a tale *account* e la usavano per acquisire i messaggi di posta elettronica inviati e ricevuti, nonché quelli salvati nella cartella "bozze", usata come sistema di "parcheggio" delle comunicazioni scambiate tra i membri dell'associazione.

In questo caso la Corte ha dovuto sciogliere due differenti questioni giuridiche: la pima, relativa alla possibilità di acquisire mediante la procedura di cui all'art. 266 *bis* c.p.p. le *e-mail* inoltrate e ricevute anche quando non si sia in presenza di un contemporaneo flusso di dati; la seconda, aveva ad oggetto la possibilità di acquisire, mediante un decreto di sequestro *ex* art. 254 e ss. le *e-mail* che venivano volutamente scritte o poi "parcheggiate" nella casella "bozze", senza dover ricorrere ad una contestuale richiesta di rogatoria internazionale, in quanto dati contenuti in *servers* allocati all'estero nelle sedi dei rispettivi *providers*.

Orbene, partendo proprio da quest'ultima questione, il ragionamento effettuato dalla Corte è di particolare pregio giuridico e fa leva su un'analogia con la disciplina civilistica della detenzione.

Innanzitutto va chiarito che il flusso di comunicazioni – nelle parole stesse della decisione – avveniva per il tramite di una modalità "*singolare, ma non sconosciuta alla casistica criminale*", vale a dire attraverso il parcheggio delle *e-mail* nella "cartella bozze" dell'*account* comune di posta elettronica: la *mail*, quindi, veniva scritta, non inviata, ma semplicemente salvata nel file "bozze", per poi essere successivamente letta da altro indagato in occasione di un accesso successivo.

La Suprema corte qualifica questa singolare modalità di comunicazione quale "*scambio comunicativo differito, in quanto sebbene la mail non [venga] inoltrata al destinatario, questi ne [prende] direttamente cognizione accedendo all'account di posta elettronica del mittente con la password di questi*". Ne discendere a parere della Corte che siffatto scambio di comunicazione, in quanto differito, debba esulare dal perimetro operativo delle intercettazioni, per essere correttamente ricompreso in quello del sequestro dei dati informatici.

Per quanto riguarda, invece, la necessità di esperire la procedura della rogatoria internazionale per poter acquisire i dati, i giudici rilevano che, sebbene, il *server* fosse gestito da un *provider* estero, lo spazio *cloud*, "*quale tecnologia che permette di elaborare, archiviare e memorizzare dati grazie all'utilizzo di risorse hardware e software distribuite nella rete (si pensi per fare gli esempi più comuni a dropbox. Google drive. Icloud)*",[25]rimaneva nella esclusiva disponibilità dell'utente, che era l'unico legittimato a potervi accedere tramite l'inserimento della *password* sul portale *@hotmail.com* fornito dal *provider*.

La Suprema Corte chiarisce, quindi, come il decreto di sequestro ex art. 254 e ss. c.p.p. avente ad oggetto le *e-mail* parcheggiate in un *account* straniero non richieda, a pena di inutilizzabilità, il ricorso alla rogatoria attiva in quanto "*la detenzione consiste nell'avere la disponibilità di una cosa, ossia nell'avere la possibilità di utilizzarla tutte le volte che si desideri pur nella consapevolezza che essa appartiene ad altri*".

Da tanto discende che i dati contenuti in uno spazio virtuale di memoria, anche se generato da un *server* allocato all'estero, sono detenuti dal titolare delle credenziali di accesso e non dalla società che gestisce il *server* che genera lo spazio di memoria virtuale; ne consegue, come nel caso portato all'attenzione della Corte, che la piena disponibilità da parte dell'indagato dei documenti memorizzati virtuali in territorio nazionale, trascina con sé, quale naturale e logica conseguenza, la sola attivazione della procedura di sequestro senza rogatoria.

Per quanto riguarda, invece, la procedura di acquisizione delle *e-mail* già inviate o ricevute la Corte giunge alla conclusione che per esse la cornice di copertura normativa possa e debba essere solo quella offerta dagli artt. 266 *bis* c.p.p., equiparando, quindi, il regime acquisitivo delle *e-mail* già ricevute e/o inviate con quella delle *e-mail* che vengono inviate e/o ricevute nel corso delle indagini.

Va, invero rilevato come gli orientamenti espressi sul punto, sia dalla dottrina che dalla giurisprudenza, non siano univoci.

[25]Sent. Cit. In altri termini, il *cloud computing* attiene al fenomeno, in costante evoluzione, di spazi di memoria virtuale (anche molto estesi) generati da *servers*, il cui accesso è consentito al solo titolare di credenziale e *password* e nei quali vengono archiviate foto, documenti di qualunque formato e genere, nonché video e numerose altre informazioni.

Infatti, secondo una prima tesi, laddove non vi sia "contestualità" tra il momento in cui si invia un'*e-mail* ed il momento in cui la stessa viene acquisita, il regime acquisitivo delle *e-mail* già inviate e/o ricevute, proprio perché flusso di dati già esaurito, dovrebbe ricadere sotto l'egida del sequestro. Secondo un altro criterio, invece, che fa leva sulle "modalità di effettuazione dell'atto", se l'attività di acquisizione è svolta in maniera occulta, il regime normativo sarebbe quello delle intercettazioni, viceversa, se l'attività di acquisizione è compiuta a sorpresa, la disciplina applicabile sarebbe quella del sequestro.

Tuttavia, la Corte, in questo caso, rifiuta tanto il "criterio della contestualità" quanto quello della "modalità di effettuazione dell'atto", per aderire al "criterio dell'inoltro".

Di seguito il passaggio argomentativo della decisione sul punto "*in realtà, alla luce del dettato normativo sopra richiamato, nella giurisprudenza di questa Corte di legittimità, anche a Sezioni Unite, si rinvengono elementi per poter affermare che il discrimen perché ci sia stato o meno flusso informativo - e quindi debba essere applicata la disciplina delle intercettazioni e non quella del sequestro - è nell'avvenuto inoltro dell'e-mail da parte del mittente. Perciò ritiene il collegio che quanto alle e-mail inviate o ricevute la risposta da fornire al quesito circa l'esistenza o meno di un flusso informativo sia positiva*".

Ciò posto, alcuni rilievi vanno tuttavia svolti in merito all'approdo al quale perviene la Corte.

In primo luogo, pare che i giudici di legittimità – ancorché, come chiarito, adoperino un'argomentazione di innegabile pregio giuridico – ignorino volutamente che l'art. 15 Cost. tutela "*ogni altra forma di comunicazione*" e quindi, anche quando questa avvenga, volutamente, ed in maniera "criminosamente" differita (stratagemma delle caselle "bozza") da parte dei soggetti indagati, appare arduo ritenere che in questo caso non ci si trovi di fronte ad una *forma di comunicazione*.

Ma, ancora, il criterio dell'inoltro accolto dalla Corte per ricondurre l'acquisizione delle *e-mail* inviate a ricevute alla disciplina delle intercettazioni, piuttosto che a quella del sequestro, farebbe dipendere il regime normativo applicabile da variabili indeterminate.[26]

[26] Basti pensare alla caduta di potenza della rete da cui derivi il mancato recapito di una *e-mail* spedita ma mai giunta al destinatario, o anche per avvenuta cancellazione del relativo indirizzo di posta elettronica.

Il "criterio della contestualità" (attualità della comunicazione rispetto all'atto acquisitivo) appare, viceversa, effettivamente idoneo ad offrire i maggiori crismi di oggettività; per cui, allorquando la captazione della *e-mail* avvenga in maniera contestuale alla sua trasmissione, dovrebbe ritenersi applicabile la disciplina delle intercettazioni; laddove, invece, l'acquisizione avvenga *off line*, si dovrebbe applicare la disciplina del sequestro.

Alla luce di tali considerazioni, non può non darsi atto di una recentissima pronuncia della Sezione VI della Corte di Cassazione (Cass., Sez. 6, 28/06/2019, n. 28269, *Pizzarotti*), secondo la quale "*è legittimo il sequestro probatorio di messaggi di posta elettronica già ricevuti o spediti e conservati nelle caselle di posta del computer, in quanto tali comunicazioni hanno natura di documenti ai sensi dell'art. 234 cod. proc. pen. e la relativa acquisizione non soggiace alla disciplina delle intercettazioni telefoniche ex art. 266 e ss. cod. proc. pen., la quale postula la captazione di un flusso di comunicazioni in atto*".

Secondo l'interpretazione accolta dalla Corte, i dati informatici rinvenuti in un *server* o in un *personal computer*, anche se consistenti in messaggi di posta elettronica "scaricati" e conservati nella memoria fisica dell'apparecchio elettronico, sono qualificabili come documenti ai sensi dell'art. 234 c.p.p. La relativa attività di acquisizione processuale, pertanto, non soggiace alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni.

L'attività di intercettazione, infatti, presuppone per sua natura la captazione di un flusso di comunicazioni nel momento stesso in cui si realizza.

Nel caso di specie, invece, il provvedimento di sequestro probatorio è intervenuto per acquisire *ex post* i dati risultanti da comunicazioni già avvenute e conservate nella memoria fisica del *computer*.

L'apprensione, pertanto, ha riguardato il risultato di una comunicazione, già definita e non più modificabile, che è stata eseguita con lo strumento informatico. In ragione della finalità probatoria, essa è sottoposta alla disciplina del sequestro, applicabile rispetto ad azioni di comunicazione ormai esaurite.[27]

[27] Per un approfondimento sul punto si veda *L. GIORDANO, PRESUPPOSTI E LIMITI ALL'UTILIZZO DEL CAPTATORE INFORMATICO: LE INDICAZIONI DELLA SUPREMA CORTE*, in *Sist. Pen*., 4/2020, p. 20 ss.

Considerazioni conclusive.

Dalle considerazioni che precedono emerge chiaramente come, a fronte di quanto è stato fatto, tanto ci sia ancora da fare in tema di captatori informatici.

Non può tacersi che le due riforme intervenute sulla disciplina delle intercettazioni si siano rivelate per certi versi incomplete e per altri versi inappaganti, soprattutto riguardo alla tutela da assicurare alle prerogative difensive dei soggetti sottoposti alle captazioni. Dall'altro lato, dal breve *excursus* di cui sopra, riguardante le altre applicazioni pratiche del *Trojan* nel campo delle ispezioni, delle perquisizioni e dei sequestri *online*, è emersa la chiara inadeguatezza degli strumenti tipici ai quali vengono ricondotte le diverse funzionalità dei captatori, nonché l'inopportuno ricorso al "grimaldello" della prova atipica per legittimare usi distorti, e spesso in palese frizione con le garanzie costituzionali, del *virus* di Stato da parte delle Procure.

Se questa, pertanto, è la situazione ad oggi, si auspica in una rimeditazione dell'intera disciplina da parte del Legislatore, che si ponga l'obiettivo di disciplinare compiutamente ed organicamente questo dirompente e poliedrico nuovo strumento di lotta al crimine, sulla falsa riga – magari – di alcune proposte di legge, che hanno avuto il pregio di prefissarsi un simile scopo[28], rimaste ahimè lettera morta.

[28] Il riferimento è al disegno di legge *Quintarelli ed altri, "Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi"* rinvenibile su https://www.camera.it/.