Trojan Horse: tornare alla riforma Orlando?

Il difficile equilibrio nell'impiego del captatore informatico

di Nello Rossi

direttore di Questione Giustizia

Sommario: 1. Il d.d.l. Zanettin - 2. La rincorsa tecnologica tra inquirenti e delinquenti - 3. I programmi " Trojan horse" e le loro modalità di impiego - 4.L'iniziale anomia e gli interventi dei giudici di merito e di legittimità - 4.1. Una prima bocciatura del Trojan: la sentenza Musumeci - 4.2. Il caso Scurato: la posizione assunta dalla Procura generale della Corte di cassazione - 4.3. L'emersione di un potenziale contrasto di giurisprudenza e la rimessione della questione alle Sezioni Unite - 4.4. La sentenza delle Sezioni Unite Scurato (n. 26889 del 28 aprile 2016) - 5. La riforma Orlando: l'uso del Trojan nei procedimenti per i reati di criminalità organizzata - 6. La c.d. legge Spazzacorrotti: l'estensione del captatore informatico alle indagini sui reati contro la PA - 7. Tornare alla riforma Orlando?

Un disegno di legge del Senatore Zanettin - che propone di escludere l'impiego del captatore informatico nei procedimenti per delitti contro la pubblica amministrazione – sta suscitando discussioni e polemiche. Nel dibattito politico e giornalistico sulla giustizia penale - ormai dominato da un meccanico susseguirsi di azioni e reazioni che spesso prescindono dal merito delle questioni sul tappeto per privilegiare ragioni di schieramento – sono scattati riflessi condizionati pregiudizialmente "oppositivi" o giudizi sommari che non esitano a qualificare le intercettazioni (tutte le intercettazioni, con qualunque mezzo effettuate e per qualunque reato adottate) come uno strumento di oppressione. Così la proposta è stata immediatamente "bollata" dagli uni come espressione di volontà di disarmo nel contrasto alla corruzione e come un favore alle organizzazioni criminali (le cui attività delinquenziali non sono peraltro escluse dalla sfera di utilizzo del Trojan) ed "esaltata" dagli altri come uno strumento di liberazione dallo strapotere di pubblici ministeri e giudici che se ne servirebbero "normalmente" per prave finalità di potere, di pressione, di intimidazione e di controllo dei cittadini. Per sottrarsi a queste grottesche semplificazioni polemiche - che sembrano divenute la cifra obbligata del confronto pubblico sulla giustizia- vale la pena di ripercorrere le fasi della vicenda istituzionale del Trojan per trarne indicazioni utili a delimitare correttamente la "desiderabile" sfera di applicazione di questo mezzo di ricerca della prova, tanto efficace quanto insidioso. Non dimenticando che l'estensione dell'utilizzo del Trojan Horse ai procedimenti per reati contro la pubblica amministrazione - e dunque al di là dell'originario confine dei reati di criminalità organizzata fissato dalla elaborazione giurisprudenziale e dalla riforma Orlando - è stata realizzata da una legge, la c.d. Spazzacorrotti, che costituisce uno dei frutti più discutibili della stagione del governo dei due populismi di Cinque Stelle e della Lega.

1. Il d.d.l. Zanettin

Una iniziativa legislativa del Senatore Zanettin, del gruppo di Forza Italia, riporta alla ribalta un tema spinoso: la sfera di applicazione del captatore informatico, il c.d. Trojan Horse

Il Senatore ha presentato un disegno di legge intitolato *«Modificazioni agli articoli 266 e 267 del codice di procedura penale e alla legge 9 gennaio 2019, n.3 in materia di utilizzo del captatore informatico nei procedimenti per i delitti contro la pubblica amministrazione»* con il quale propone di sopprimere - nel testo degli artt. 266 e 267 del codice di procedura penale che regolano rispettivamente "limiti di ammissibilità" e "presupposti e forme" del provvedimento che dispone le intercettazioni - il riferimento ai «*delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni……».*

Con l'effetto di precludere il ricorso al captatore informatico nelle indagini per gravi reati contro la pubblica amministrazione tra cui il peculato, la corruzione, l'induzione indebita a dare o promettere utilità.[1]

Nella relazione al d.d.l. il senatore proponente scrive che *«sotto il profilo delle indagini a mezzo trojan horse, i reati contro la Pubblica Amministrazione»* sono stati *«di fatto equiparati ai reati per criminalità organizzata e terrorismo»* dalla legge 9 gennaio 2019, n.3 - c.d. spazzacorrotti – che ha ammesso *«l'uso di tale invasivo mezzo di ricerca della prova anche per quanto concerne tali tipologie di reati»*.

E subito dopo aggiunge: *«Se da un lato l'utilizzo del trojan, introdotto nell'ordinamento penale italiano con la legge 23 giugno 2017, n. 23 - c.d. riforma Orlando - rappresenta lo strumento più penetrante ed efficace nel contrasto alla commissione di reati ritenuti di particolare gravità di tipo associativo e di terrorismo, dall'altro è lo strumento che più vìola la sfera di intimità dell'intercettato, con l'evidente rischio di una diversa destinazione d'uso atto a violare la privacy degli individui, nonostante la Corte di Cassazione (Cass. Pen., sez. V, 30 settembre 2020, n. 31064) abbia confermato che vada esclusa la riconducibilità del trojan agli strumenti di pressione sulla libertà fisica e morale il cui uso è vietato dall'articolo 188 del codice di procedura penale»*.

Di qui la proposta di introdurre modifiche agli articoli 266 e 267 del codice di procedura penale ed alla legge n. 3 del 2019, *«volte a prevedere l'esclusione dei reati contro la pubblica amministrazione dall'utilizzo del trojan nelle indagini»*.

Nel dibattito politico e giornalistico sulla giustizia penale e sui suoi mezzi - ormai dominato da un meccanico susseguirsi di azioni e reazioni che spesso prescindono dal merito delle questioni sul tappeto, privilegiando ragioni di schieramento – sono scattati riflessi condizionati pregiudizialmente "oppositivi" o giudizi sommari che non esitano a qualificare le intercettazioni (tutte le intercettazioni, con qualunque mezzo effettuate e per qualunque reato adottate) come uno strumento di oppressione.

Così la proposta è stata immediatamente "bollata" dagli uni come espressione della volontà di disarmo nel contrasto alla corruzione e come un favore alle organizzazioni criminali (peraltro non escluse dalla sfera di utilizzo del trojan)[2] ed "esaltata" dagli altri come uno strumento di liberazione

---

[1] DISEGNO DI LEGGE
ART. 1
(Modifiche all'articolo 266 del codice di procedura penale)
1. All'articolo 266 del codice di procedura penale al comma 2-bis le parole "e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4." sono soppresse.
ART. 2
(Modifiche all'articolo 267 del codice di procedura penale)
1. All'articolo 267 del codice di procedura penale sono apportate le seguenti modificazioni:
a) al comma 1, terzo periodo, le parole "e dai delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4" sono soppresse;
b) al comma 2-bis, primo periodo, le parole " e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4" sono soppresse.
ART. 3
(Modifiche alla legge 9 gennaio 2019, n.3)
1. All'articolo 1 della legge 9 gennaio 2019, n.3, al comma 4 le lettere *a)* e *b)* sono soppresse.

[2] Nel corso di una audizione alla Commissione Giustizia della Camera, che si è svolta il 21 dicembre, il deputato del Movimento 5 Stelle Cafiero De Raho ha sostenuto che *«Le norme inserite nella legge Spazzacorrotti sui reati contro la PA rispondevano a una precisa esigenza nata in ambito giudiziario: servivano a colpire le condotte corruttive delle mafie. Mafia e corruzione sono realtà criminali strettamente legate, chi pensa di tenerle separate fa riferimento a una realtà superata ormai da decenni. Le organizzazioni criminali mettono le mani sugli appalti e sui soldi pubblici proprio attraverso la commissione dei reati contro la PA. »*
Negli stessi termini si è espressa una parte della stampa che si è detta preoccupata del venir meno sul versante anticorruzione di un incisivo strumento di ricerca della prova come il trojan horse e ha interpretato la proposta di legge di cui si parla come un ulteriore tassello di una operazione di indebolimento della lotta alla corruzione

dallo strapotere di pubblici ministeri e giudici che se ne servirebbero "normalmente" per prave finalità di potere, di pressione, di intimidazione e di controllo dei cittadini[3].

Ad aumentare questo confuso vociare concorrono le torrenziali esternazioni del Ministro della Giustizia che resta in silenzio o aderisce a discutibili iniziative in tema di giustizia del governo di cui fa parte (dal decreto sui rave ai progettati condoni) per dedicarsi a polemiche veementi, superficiali e ingenerose nei confronti della magistratura.

In realtà la complessa e risalente vicenda istituzionale dell'utilizzo del Trojan horse non può essere liquidata con facili battute polemiche.

Perciò nel momento in cui una iniziativa legislativa la riporta alla ribalta e può rimetterla al centro della discussione, la breve storia del Trojan merita di essere ripercorsa con spirito critico ed apertura alla ricerca di una soluzione equilibrata.

2. La rincorsa tecnologica tra gli inquirenti e delinquenti

All'origine dell'intera vicenda c'è quella che si potrebbe chiamare la "rincorsa tecnologica" tra soggetti che delinquono da un lato, e magistrati e forze di polizia dall'altro.

Nell'ambito delle tecnologie informatiche e nel campo della telematica progrediscono infatti con straordinaria velocità e quasi di pari passo tanto le tecnologie di "captazione", che si fanno via più sofisticate ed invasive, quanto le tecniche di "elusione" di ogni captazione possibile, che si affidano di volta in volta alla impenetrabilità degli apparecchi utilizzati, alla inaccessibilità di particolari reti di comunicazione o alla adozione di sistemi di criptazione dei messaggi scambiati.

Le valutazioni sul potenziale invasivo dei più moderni meccanismi di captazione devono perciò essere sempre compiute avendo presente che parallelamente e contemporaneamente si affinano e si moltiplicano anche i mezzi ed canali di comunicazione strutturati in modo da sottrarsi ai tradizionali strumenti di acquisizione.

Mezzi e canali che spesso fondano la loro diffusione - oltre che sulla facilità dei contatti e sulla gratuità del servizio offerto, di regola compensato dagli introiti pubblicitari o dal valore delle informazioni sulla utenza raccolte attraverso di esse - proprio sulla loro vera o presunta inaccessibilità.

Se dunque è legittimo nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei virus informatici come il trojan horse, suscettibili di ledere riservatezza, dignità e libertà delle persone, è del pari legittimo ricordare che siffatti strumenti sono oggi in grado di penetrare canali " criminali" di comunicazione o di scambio di informazioni utilizzati per la commissione di gravissimi reati contro le persone.

Così che, se si valuta l'impiego dei virus informatici in una delle loro molteplici funzionalità - quella relativa alle intercettazioni di conversazioni - si può sostenere che essi consentono in qualche misura un recupero dell'efficacia perduta o compromessa delle tecniche di captazione più tradizionali.

3. I programmi "Trojan horse" e le loro modalità di impiego.

La dottrina che si è occupata dell'argomento ha fornito efficaci descrizioni dei programmi di tipo "*trojan horse*" e delle loro potenzialità per la captazione del contenuto di dati e programmi informatici nonché per la realizzazione delle stesse intercettazioni [4]

che fa seguito alla cancellazione dei reati contro la pubblica amministrazione dall'elenco dei reati ostativi ai benefici penitenziari.

[3] Per un esempio di questo approccio v. P. Sansonetti, *E'finita la Repubblica delle spie: Trojan addio, torma il diritto,* Il riformista, 23 dicembre 2022

[4] Testaguzza, *I sistemi di controllo remoto: fra normativa e prassi*, in Dir. Pen. e Processo, 2014, p. 759 e ss.

Si tratta di software che, prescindendo dalle autorizzazioni dell'utente, si installano su di un sistema scelto come "obiettivo" (sia esso un *personal computer*, un *tablet* od uno *smartphone*) e ne acquisiscono determinati poteri di gestione, funzionando come una sorta di microspia telematica.

Tali programmi sono concepiti e costruiti per installarsi in modo occulto sugli apparecchi da monitorare ed agiscono senza rivelare all'utente la propria presenza. In particolare essi comunicano attraverso Internet, in modalità nascosta e protetta, con un centro remoto di comando e controllo che li gestisce; catturano ciò che viene digitato sulla tastiera, visualizzato sullo schermo o detto al microfono; possono cercare tra i file presenti sul computer "ospite" o su altri connessi in rete locale; dispongono di contromisure che li rendono in grado di nascondersi ai più accreditati antivirus; sfruttano le vulnerabilità, spesso non ancora note, dei sistemi operativi o degli applicativi per aggirare controlli o contromisure che potrebbero ostacolarli od inibirli.

I *trojan horse* possono operare anche come le usuali cimici, o microspie per intercettazioni ambientali, fisicamente collocate nelle abitazioni, con la differenza che, in questo caso, si tratta di prodotti software installati surrettiziamente sul computer o altro apparecchio elettronico.

Nelle versioni più evolute questi software possono operare come veri e propri sistemi di controllo remoto (RCS: *remote control systems*), funzionare in modo autonomo, senza l'intervento diretto di persone responsabili, come strumenti (potenzialmente) onnipresenti ed "*always on*".

Come la dottrina[5] ha opportunamente sottolineato, per intercettare le comunicazioni realizzate attraverso l'impiego di apparati mobili collegati a WI-FI "aperte" o effettuate da utilizzatori di sistemi crittografati, è necessario avvalersi di un modello diverso dalle intercettazioni telematiche "classiche", fondate sulla assistenza tecnologica degli operatori che forniscono un accesso alla rete e dirette alla acquisizione dei soli dati che vi fluiscano "in chiaro".

Il *software trojan* si occupa della captazione della voce dell'utilizzatore e di quella dell'interlocutore dopo esser stata decifrata. Le informazioni così ottenute vengono mandate a *server* esterni, collocati presso la sala di ascolto. Ovviamente, questo avviene sfruttando la connettività del dispositivo elettronico scelto come *"obiettivo"*: laddove questo non abbia connettività, infatti, le informazioni verranno salvate in locale ed inviate al *server* non appena risulti disponibile un collegamento alla rete.

In sostanza tali *software* catturano quanto captato dal microfono e, conseguentemente, ogni qualvolta il computer risulti acceso con i microfoni attivati, potrà realizzarsi una vera e propria, intercettazione "ambientale".

La difficoltà maggiore riscontrabile in questo tipo di intercettazione è costituita dall'installazione del software RCS sul sistema *obiettivo* (la c.d "inoculazione") all'insaputa del suo possessore.

Installazione che può essere compiuta o mediante un accesso fisico al dispositivo elettronico scelto come obiettivo o grazie ad installazione remota (attraverso l'invio di allegati con messaggi di posta elettronica o l'invio di comunicazioni provenienti da gestori dei servizi di messaggistica o *social network* o l'invio di aggiornamenti di software o di applicazioni).

Da ultimo, sempre in dottrina[6], si è segnalato che, tutte le volte in cui si parla di "captatore informatico" in ambito investigativo è necessario distinguere tra due diverse modalità operative: quella *on line search* e quella *on line surveillance*.

I programmi appartenenti alla categoria della *on line search* (modalità acquisitiva di dati) consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico individuato come obiettivo; i dati e le informazioni sono quindi trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione tramite la rete Internet in modalità nascosta e protetta.

Attraverso i programmi che realizzano la c.d. *on line surveillance* (modalità captativa di flussi informativi) invece, è possibile captare il flusso informativo intercorrente tra le periferiche (video, tastiera, microfono, webcam, ecc.) e il microprocessore del dispositivo target, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo

[5] Testaguzza, *Digital forensic. Informatica giuridica e processo penale*, Cedam, 2014, p.81 e ss.
[6] Torre, *Il virus di Stato nel diritto vivente tra esigenza investigative e tutela dei diritti fondamentali*, in Dir. Pen. e Processo, 2015, p. 1163 e ss.

(*screenshot)*, digitato attraverso la tastiera (*keylogger*), detto attraverso il microfono, o visto tramite la webcam del sistema target controllato.

A conclusione di questa rapida disamina preliminare occorre mettere in luce un dato di estrema importanza.

La molteplicità di funzioni dei programmi informatici di cui si discute non deve indurre a credere di essere di fronte a strumenti onnipervasivi e onnipotenti, suscettibili di dar vita ad un potere invasivo esercitabile senza limiti o in forme incontrollabili sotto il profilo tecnico o giuridico.

Al contrario è possibile l'apposizione di limiti tecnici preventivi all'impiego dei virus informatici (ad es., inibendo *a priori* l'operatività di alcune delle loro molteplici funzioni acquisitive).

Inoltre, ciò che più conta in questa sede, è possibile dettare i limiti giuridici delle modalità di utilizzo dei captatori (ad es. escludendo che i programmi di *on line surveillance* possano essere utilizzati per effettuare videoriprese o che i programmi *on line search* siano impiegati per acquisire dati, al di fuori o in contrasto con le regole in tema di perquisizioni e sequestri).

Ancora una volta, dunque, come avviene del resto in altri delicatissimi campi dell'esperienza umana, sono la legge ed il diritto a fissare i confini delle possibilità offerte dalla tecnologia, commisurandole ai principi dello Stato democratico di diritto, ai diritti individuali ed alle esigenze e sensibilità della collettività.

4. L'iniziale anomia e gli interventi dei giudici di merito e di legittimità

Come è noto il Trojan è stato inizialmente usato nelle indagini quando non vi era nessuna norma che ne regolava l'impiego.

E' stata dunque la giurisprudenza di merito e di legittimità a dover affrontare il tema della legittimità e delle modalità di impiego del nuovo mezzo di ricerca della prova che - se installato su di un dispositivo elettronico mobile – realizzava una sorta di intercettazione itinerante.

4.1.Una prima bocciatura del trojan: la sentenza Musumeci

La prima risposta del giudice di legittimità sull'uso del captatore informatico fu sostanzialmente di segno negativo.

Nella sentenza n. 27100 del 26.5.2015 (Musumeci), relativa all'impiego del *trojan horse* in un procedimento per reati di criminalità organizzata, la Sesta Sezione penale della Corte di cassazione affermò che *« l'intercettazione di conversazioni tramite il c.d. agente intrusore, che consente la captazione "da remoto" delle conversazioni tra presenti mediante l'attivazione, attraverso il c.d. virus informatico, del microfono di un apparecchio telefonico smartphone, dà luogo ad un'intercettazione ambientale che può ritenersi legittima, ai sensi dell'art. 266, comma secondo, cod. proc. pen. in relazione all'art. 15 Cost., solo quando il decreto autorizzativo individui con precisione i luoghi in cui espletare l'attività captativa. »*

In sostanza la pronuncia si risolveva in una bocciatura del *trojan* come dispositivo idoneo a porre in essere una intercettazione itinerante, sostenendo che l'art. 266 c.p.p. disciplinava una intercettazione "ambientale", legittima solo in ambienti specificamente individuati.

4.2. Il caso Scurato: la posizione della Procura generale della Corte di cassazione

In un successivo procedimento (imp. Scurato), anch'esso per reati di mafia, nel corso del quale era stato utilizzato il captatore informatico, la difesa invocava, sempre dinanzi alla Sesta Sezione penale della Suprema Corte, il precedente della sentenza Musumeci al fine di far dichiarare l'inutilizzabilità delle intercettazioni effettuate tramite il *trojan*[7].

[7] In particolare difensore del ricorrente deduceva l'illegittimità del decreto con cui il GIP aveva autorizzato *"le operazioni di intercettazione di tipo ambientale tra presenti che avverranno nei luoghi in cui si trova il dispositivo elettronico in uso a ....."* nonché l'inutilizzabilità dei risultati relativi a tali captazioni -

La Procura generale della Corte di cassazione replicava con un'ampia memoria[8] nella quale criticava l'impostazione della sentenza Musumeci, chiedendo che venisse riconosciuta la legittimità delle intercettazioni effettuate con il *trojan* in un procedimento per reati di criminalità organizzata nel quale era applicabile la speciale disciplina delle intercettazioni dettata dall'art. 13 del d.l. n 152/1991.

Il tema al centro della riflessione dalla Procura era quello delle "intercettazioni tra presenti" poste in essere, nell'ambito di un procedimento per delitti di criminalità organizzata, grazie all'installazione di un virus informatico in un apparecchio elettronico portatile in uso ad una persona, intercettazioni necessariamente prive di una preventiva indicazione dei luoghi dove deve avvenire la relativa captazione.

La questione giuridica fu affrontata dall'ufficio requirente sulla base di una attenta lettura delle norme del codice di procedura penale che disciplinano le "intercettazioni tra presenti" e, soprattutto, del testo della norma derogatrice dettata dall'art. 13 del d.l. n. 152/91 per le intercettazioni nei procedimenti per reati di criminalità organizzata.

Si osservò che il codice di rito non parlava di "intercettazioni ambientali" ma faceva invece riferimento ad *"intercettazioni di comunicazioni tra presenti"* (art. 266, u.c. c.p.p.) nonché ad intercettazioni di comunicazioni tra presenti destinate ad avvenire *" nei luoghi indicati dall'art. 614 c.p."* (norma incriminatrice delle diverse fattispecie del reato di violazione del domicilio che a sua volta menziona le abitazioni, gli altri luoghi di privata dimora e le relative appartenenze).

Lo stesso valeva per l'art. 13 del d.l. n. 152 del 1991, norma speciale derogatrice per le indagini sui reati di mafia e terrorismo, che stabilisce: *" In deroga a quanto disposto dall'articolo 267 del codice di procedura penale, l'autorizzazione a disporre le operazioni previste dall'articolo 266 dello stesso codice è data, con decreto motivato, quando l'intercettazione è necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi.....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."*

In sostanza le categorie di intercettazioni deducibili dai testi normativi erano due: quella – più ampia - delle *"intercettazioni di comunicazioni tra presenti"* e quella - più circoscritta - delle *"intercettazioni di comunicazioni tra presenti nei luoghi di privata dimora "*.

E queste ultime erano sottoposte a requisiti autorizzativi differenziati a seconda che fossero disposte o meno in procedimenti per delitti di criminalità organizzata.

Non che l'espressione "intercettazioni ambientali", largamente impiegata dalla dottrina e dalla giurisprudenza, fosse sbagliata o scorretta. Ma la locuzione era entrata in uso e si era affermata in un periodo nel quale le possibilità di intercettazione in luoghi chiusi offerte dalle tecniche di captazione erano quasi sempre connesse alla installazione in uno o più "ambienti" predeterminati di microspie destinate alla captazione.

Se dunque la dizione di intercettazione ambientale non trovava un diretto riscontro nel dato normativo (ma aveva avuto la più ridotta funzione di descrivere efficacemente lo stato delle cose sino ad un certo stadio dello sviluppo tecnologico) essa non poteva essere "ipostatizzata" ed assunta come valido punto di partenza di un ragionamento che, enfatizzando il concetto di intercettazione

---

effettuate a mezzo di un virus autoinstallante attivato su di un apparecchio portatile in uso a .....- per violazione degli artt. 15 Cost., 8 CEDU, 266, comma 2, e 271 c.p.p.. Ad avviso della difesa era stato eluso il divieto posto dall'art. 266, comma 2, c.p.p. di effettuare intercettazioni all'interno di private abitazioni a meno che all'interno di esse non si stia svolgendo una attività criminosa e, sotto diverso profilo, che l'intercettazione era stata autorizzata in violazione degli artt. 15 Cost. e 8 CEDU per non essere stati preventivamente indicati i luoghi in cui la captazione doveva essere effettuata, aggirando i limiti posti dall'art. 266, comma 2, c.p.p. e ponendo in essere intercettazioni non soggette ad alcuna restrizione spaziale i cui risultati devono essere ritenuti inutilizzabili.

[8] La memoria della Procura generale (redatta da N. Rossi e A. Balsamo) è integralmente pubblicata in allegato alla sentenza Cass. SSUU pen. 28 aprile 2016 (dep. 1 luglio 2016) n. 26889 in Diritto penale contemporaneo, 4 luglio 2016. La sentenza è stata poi annotata da G. Lasagni, *L'uso dei captatori informatici (Trojans) nelle intercettazioni tra presenti,* in Diritto penale contemporaneo, 7 ottobre 2016

"ambientale", giungesse ad escludere la legittimità di ogni intercettazione tra presenti non strettamente collegata ad un predeterminato "ambiente".

A meno di non voler ripetere il percorso – a suo tempo magistralmente svelato e criticato da Riccardo Orestano [9]- dei giuristi che, dopo aver elaborato, a partire dalle norme, le categorie dogmatiche finivano poi con il ragionare solo o prevalentemente sulla base di queste ultime, svincolandosi progressivamente dai testi normativi.

Di qui alcune critiche mosse alla decisione di chiusura del giudice di legittimità adottata nel caso Musumeci.

La prima critica fu di aver concentrato l'attenzione non sulla pregnante distinzione "normativa" tra intercettazioni tra presenti e intercettazioni tra presenti nei luoghi di privata dimora (e sui loro specifici requisiti autorizzativi) ma sulla distinzione, priva di agganci normativi, tra intercettazione tra presenti in ambienti predeterminati e intercettazioni prive di tale predeterminazione.

Posizione, questa, evidente nei passaggi della sentenza n. 27100/2015 nei quali si afferma che *"l'attivazione del microfono dà luogo ad una intercettazione ambientale "*; che *"non sembra potersi dubitare che l'art. 266, comma 2, c.p.p. nel contemplare l'intercettazione tra presenti, si riferisca alla captazione di conversazioni che avvengano in un determinato luogo e non ovunque"*; che *"l'intercettazione ambientale deve avvenire in luoghi ben circoscritti ed individuati ab origine"*.

La seconda, e per più versi decisiva, osservazione critica fu che la sentenza non aveva preso in considerazione la norma speciale derogatrice ex art. 13 del d.l. n 152/1991 che - per le intercettazioni domiciliari in procedimenti per delitti di criminalità organizzata – esclude espressamente il requisito autorizzativo previsto dall'art. 266, comma 2, c.p.p. e cioè la sussistenza di un *"fondato motivo di ritenere che nei luoghi"* di privata dimora *"si stia svolgendo l'attività criminosa."*

Per effetto di queste opzioni interpretative, la sentenza n. 27100/15 aveva omesso di valutare l'incidenza del regime derogatorio sulla disciplina delle intercettazioni tramite captatori informatici, con ciò ponendosi in contrasto con altre pronunce della Suprema Corte[10].

---

[9] R. Orestano, *Introduzione allo studio storico del diritto romano*, Torino, Giappichelli, 1963

[10] Ci si riferisce alle pronunce che avevano valorizzato la norma speciale dell'art. 13 per giungere alla conclusione dell'utilizzabilità delle intercettazioni tramite virus, proprio sul rilievo che *"le captazioni sono state disposte, trattandosi di reati in materia di criminalità organizzata, ai sensi dell'art 13 d.l. 13-51991 n. 152, conv. in l. 12-7-1991 n. 203, che testualmente prescinde dal predetto requisito, stabilendo che l'intercettazione di comunicazioni tra presenti è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 cod. pen. si stia svolgendo l'attività criminosa"*. (così Cass., Sez. VI, 8/4/2015 n. 27536 e, in termini analoghi, Cass., Sez. VI, 12/3/2015 n. 24237).

Del resto la tesi sostenuta nella sentenza n. 27100/15 in ordine alla necessità di individuare con precisione, a pena di inutilizzabilità, i "luoghi" nei quali le intercettazioni tra presenti devono essere espletate non trovava conferme in altre pronunce della Corte di cassazione.

La giurisprudenza aveva infatti sempre escluso la necessità di una siffatta indicazione, ad eccezione dei luoghi di privata dimora per i quali valga il disposto dell'art. 266 comma 2 c.p.p. (e non la norma derogatrice speciale). Assolutamente esplicita, in proposito, Cass., Sez. VI, n. 3541 del 5/11/1999, secondo cui «*l'intercettazione di comunicazioni tra presenti richiede l'indicazione dell'ambiente nel quale l'operazione deve avvenire solo quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 del codice penale. In tal senso i locali di uno stabilimento carcerario o, più ancora, la sala colloqui non sono luoghi di privata dimora*».

Laddove non si tratti di luoghi di privata dimora, la giurisprudenza aveva ritenuto sufficiente, per le intercettazioni "ordinarie", l'indicazione della tipologia di ambienti dove eseguire le intercettazioni.

In tale prospettiva si era collocata Cass., Sez. I, n. 11506 del 25/2/2009, che aveva considerato *"legittimo il decreto del pubblico ministero che disponga in via d'urgenza l'intercettazione dei colloqui con i familiari di alcuni detenuti senza indicare specificamente il luogo della intercettazione, che è sufficientemente individuabile nel riferimento alle sale colloqui della casa circondariale di detenzione"*.

La medesima *ratio* stava alla base anche dell'interpretazione accolta da Cass., Sez. II, n. 17894 dell'8/4/2014, secondo cui *"il trasferimento in altra struttura carceraria di un soggetto detenuto, nei cui confronti siano in corso operazioni di intercettazione ambientale regolarmente autorizzate, non comporta alcuna necessità di rinnovare il provvedimento autorizzativo delle attività di captazione ai fini della legittima prosecuzione delle stesse"*.

In definitiva nella memoria della Procura generale si sostenne che la normativa derogatoria speciale dell'art.13 del d,l. n. 152 del 1991 non escludeva che il giudice potesse autorizzare, motivando adeguatamente e coerentemente le sue determinazioni, le particolari intercettazioni foniche rese possibili dall'uso dei captatori informatici.

In particolare nessuna preclusione o controindicazione normativa era rinvenibile riguardo alle intercettazioni foniche realizzate in luoghi pubblici ed aperti e riguardo alle captazioni nel domicilio del soggetto intercettato, poiché, già sulla base della disciplina vigente, questi avrebbe potuto essere destinatario di un decreto del giudice che estendesse motivatamente le intercettazioni tradizionali ad una pluralità di stanze della sua abitazione o alle relative pertinenze.

Il profilo più fortemente problematico era un altro e atteneva alla possibilità che il soggetto intercettato si recasse, portando con sé l'apparecchio elettronico nel quale era stato inoculato il virus, nei luoghi di privata dimora di altre persone, dando così vita ad altrettante intercettazioni domiciliari.

In realtà il legislatore aveva già fornito, sia pure in un contesto tecnologico diverso, una chiara indicazione sul punto quando aveva espressamente escluso - per le intercettazioni tra presenti in luoghi di privata dimora disposte in procedimenti di criminalità organizzata - il requisito autorizzativo previsto dall'art. 266, comma 2, c.p.p. per tutte le altre intercettazioni

Nella norma derogatoria era dunque prefigurato un peculiare e specifico bilanciamento di interessi nel cui ambito la segretezza delle comunicazioni e la tutela del domicilio subivano più consistenti limitazioni in ragione della eccezionale gravità e pericolosità, per gli individui e per la intera collettività, dei reati di criminalità organizzata.

Bilanciamento che si era tradotto nella possibilità di effettuare, previa motivata valutazione del giudice, intercettazioni tra presenti in luoghi di privata dimora "a prescindere" dalla dimostrazione che essi fossero sedi di attività criminose in atto.

In tale opzione legislativa era possibile cogliere due dati.

Da un lato il segnale normativo della estrema incisività dei mezzi di ricerca della prova da mettere in campo nei confronti dei delitti propri della criminalità organizzata.

Dall'altro lato, il riflesso del carattere per così dire "totalizzante" dei delitti della grande criminalità organizzata, che, per essere ideati, programmati e portati a compimento, reclamano attività che possono, e spesso debbono, svolgersi in permanenza e in tutti i luoghi frequentati dai soggetti sospettati di esserne gli autori; così da rendere all'occorrenza necessaria una compressione di diritti assai più intensa di quella realizzabile nel corso di investigazioni per altri pur gravi reati o nei confronti di altri soggetti.

In altri termini, introducendo la norma derogatrice dell'art. 13 del citato d.l. n. 152, il legislatore aveva accettato – limitatamente ai procedimenti per delitti di criminalità organizzata - il "rischio" di intercettazioni che si svolgessero in luoghi di privata dimora anche nei casi in cui non fosse fondatamente ipotizzabile lo svolgimento di attività criminose.

In altri termini, quando fossero indicati i destinatari della captazione e la tipologia di ambienti (diversi dai luoghi di privata dimora) in cui eseguirla, l'intercettazione restava utilizzabile anche qualora venisse effettuata in un altro luogo rientrante nella medesima categoria.
In particolare, il principio per cui erano utilizzabili i risultati delle intercettazioni di comunicazioni tra presenti anche quando nel corso dell'esecuzione intervenisse una variazione dei luoghi in cui deve svolgersi la captazione, è stato affermato da Cass., Sez. VI, n. 15396/2008 dell'11/12/2007, in una fattispecie nella quale l'autorizzazione dell'intercettazione tra presenti aveva ad oggetto la sala colloqui della casa circondariale dove si trovava l'imputato e le operazioni di captazione erano proseguite presso la sala colloqui della casa circondariale presso cui lo stesso era stato successivamente trasferito, e da Cass., Sez. V, n. 5956/2012 del 6/10/2011, in un caso in cui la captazione ambientale era stata trasferita dalla vettura oggetto di autorizzazione ad altra vettura successivamente acquistata dall'indagato sottoposto ad intercettazione. Si tratta di un orientamento che trova il suo antecedente in Cass., Sez. I, n. 4561 del 30/6/1999, che ha ritenuto utilizzabili i risultati di una intercettazione ambientale autorizzata per una autovettura nella disponibilità dell'indagato ed eseguita su diversa autovettura, sempre nella sua disponibilità.
Ed è appunto riferendosi a tali pronunce, che una parte della dottrina aveva parlato del riconoscimento della "dinamicità" delle intercettazioni, eseguibili in ambienti diversi frequentati dal soggetto sottoposto a controllo.

Ed era alla luce di tale "accettazione", frutto di un accurato e risalente contemperamento di valori ed interessi, che l'eventualità di intercettazioni domiciliari- conseguenti alle modalità di impiego ed alla mobilità dell'apparecchio elettronico sede del captatore - non appariva in contrasto con la normativa vigente in tema di intercettazioni e non risultava confliggente con le norme di rango costituzionale poste a presidio della segretezza delle comunicazioni, del domicilio e della riservatezza[11].

4.3. L'emersione di un potenziale contrasto di giurisprudenza e la rimessione della questione alle Sezioni Unite

Il collegio, valutate le prospettazioni delle parti, ravvisava un potenziale contrasto con la sentenza n. n. 27100/15 del 26.6.2015 della stessa Sezione e rimetteva la questione alle Sezioni Unite della Corte di cassazione, così sintetizzando, a conclusione di una approfondita motivazione della sua ordinanza (Cass., Sez. VI, ord. n. 59 del 10/3/2016 in proc. n. 13884/16) le questioni da sottoporre alle Sezioni Unite:

- *se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi dove debba avvenire la relativa captazione;*
- *se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, c.p.p.;*
- *se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.*

4.4. La sentenza delle Sezioni Unite Scurato (n. 26889 del 28 aprile 2016)

Nel decidere il caso e le questioni controverse [12] le Sezioni Unite giungevano alla conclusione che *«l'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico in un dispositivo elettronico è consentita nei soli procedimenti per delitti di criminalità organizzata per i quali trova applicazione la disciplina di cui all'art. 13 del D.L. n. 151 del 1991, convertito dalla legge n. 203 del 1991, che consente la captazione anche nei luoghi di privata dimora, senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto »*

Nella motivazione la Corte sottolineava che, in considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso.

In sostanza, secondo la Corte, con riferimento ai delitti di criminalità organizzata, il legislatore aveva operato uno specifico bilanciamento di interessi, optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio tenendo conto della eccezionale gravità e pericolosità, per l'intera collettività di tali reati, bilanciamento sfociato nella possibilità di effettuare, previa motivata valutazione del giudice, intercettazioni tra presenti in luoghi di privata dimora a prescindere dalla dimostrazione che essi fossero sedi di attività criminose in atto e, quindi, senza alcuna necessità di preventiva individuazione ed indicazione dei luoghi stessi.

---

[11] D'altro canto va ricordato che il più ampio tema delle "intercettazioni casuali" non è nuovo ed è stato più volte affrontato e risolto della giurisprudenza della Corte costituzionale e del giudice di legittimità in sentenze che non hanno mai optato per soluzioni di pregiudiziale negazione e inutilizzabilità ma hanno attentamente esercitato l'arte della distinzione, sceverando le intercettazioni oggetto di preclusioni normative assolute o sottoposte a specifici regimi autorizzativi preventivi da quelle per le quali nella legge tali requisiti non sono rinvenibili (cfr. al riguardo Corte cost. n. 390 del 2007; Corte cost. n. 113 del 2010; Corte cost. n. 114 del 2010; Cass., II, 16.11.2012, sulle intercettazioni dirette o casuali dei parlamentari).

[12] Cass. SSUU pen. 28 aprile 2016 (dep. 1 luglio 2016) n. 26889 in Diritto penale contemporaneo, 4 luglio 2016 e in Cass. pen., 2016, p. 3546, citata alla nota 8.

Per procedimenti relativi a delitti di criminalità organizzata – proseguiva la Corte - dovevano poi intendersi quelli elencati nell'art. 51, commi 3-bis e 3-quater, cod. proc. pen. nonché quelli comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.

5. La riforma Orlando: l'uso del Trojan nei procedimenti per i reati di criminalità organizzata

Dato il rilievo e l'incisività del captatore informatico l'assenza di una regolamentazione normativa delle modalità e dei limiti del suo impiego non poteva durare troppo a lungo.

Uno dei punti cardine della riforma Orlando delle intercettazioni del dicembre 2017 (d.lgs. n. 216/2017) fu rappresentato proprio dal superamento di tale situazione di anomia.

Comunque la novella del 2017 si limitò a prendere in considerazione l'inoculazione del *trojan* su dispositivo elettronico portatile, al fine di consentire l'esecuzione delle intercettazioni tra presenti, e tralasciò di occuparsi dell'uso del captatore come mezzo destinato a finalità ulteriori, quali, a titolo esemplificativo, effettuare perquisizioni online, attivare la webcamera, acquisire il contenuto di comunicazioni e conversazioni intrattenute mediante applicazione di instant messaging (facebook, instagram, telegram), nonché decifrare le digitazioni effettuate sulla tastiera collegata al sistema (funzione di keylogger).

Nello specifico, il comma 2-bis dell'art. 266 c.p.p., introdotto ex novo dal d.lgs. n. 216/2017, stabilì che, nei procedimenti per i delitti di criminalità organizzata di cui all'art. 51, commi 3-bis e 3- quater, c.p.p., in relazione ai quali trovava già applicazione la disciplina derogatoria dell'art. 13 d.l. n. 152/199112, le intrusioni con impiego del captatore informatico nei luoghi di privata dimora erano «sempre» consentite.

Sul punto, la Relazione illustrativa al d.lgs. n. 216/2017, cit., p. 10, precisava: *«l'uso del captatore informatico è consentito, ai fini dell'intercettazione tra presenti in ambito domiciliare, soltanto se si procede per taluno dei delitti di cui all'articolo 51, commi 3-bis e 3-quater, c.p.p.*.

Al di fuori di quest'ambito procedimentale, l'uso dell'insidioso mezzo soggiace, in ambito domiciliare, al limite costituito dal presupposto dello svolgimento in atto, in tale luogo, di attività criminosa».

Si ribadiva così una disciplina duale delle captazioni occulte tra presenti con immissione della spia elettronica, confermando, anche in tale settore, il regime differenziato tra delitti di criminalità organizzata e reati "comuni".

Va sottolineato in proposito che la legge Orlando recepiva solo in parte l'orientamento delle Sezioni Unite sul tipo di procedimenti nei quali era utilizzabile il Trojan e si muoveva se mai nel più ristretto solco tracciato dalle richieste della Procura generale nel procedimento Scurato.

La Corte infatti, nella sentenza Scurato, aveva sostenuto che i procedimenti relativi a delitti di criminalità organizzata nel cui ambito era legittimo il ricorso al *trojan* erano *«quelli elencati nell'art. 51, commi 3-bis e 3-quater, cod. proc. pen. nonché quelli comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.»* mentre la legge circoscriveva la sfera di applicazione del captatore ai soli delitti di cui all'articolo 51, commi 3-bis e 3-quater, c.p.p. così come sostenuto nella memoria della Procura generale.

6. La c.d. legge Spazzacorrotti: l'estensione del captatore informatico alle indagini sui reati contro la PA

L'ultimo approdo della disciplina del *Trojan* è rappresentato dalla l. 9 gennaio 2019, n. 3 (c.d. legge "spazza-corrotti" o "anticorruzione") con la quale sono state introdotte misure, volte ad *«affrontare in modo efficace il fenomeno corruttivo e, in generale, per assicurare una maggiore incisività all'azione di contrasto dei reati contro la pubblica amministrazione»* sia sul piano del diritto penale sostanziale sia sotto il profilo investigativo e processuale, con la modifica di alcune disposizioni del codice di procedura penale e della l. 16 marzo 2006, n. 146, in tema di operazioni sotto copertura.

In tale legge - nel quadro di una strategia diretta a rafforzare il contrasto della corruzione - sono stati modificati gli artt. 266, comma 2-bis, e 267, comma 1, c.p.p., estendendo il campo applicativo della disciplina "speciale" sulle intercettazioni eseguite mediante inserimento del captatore informatico - precedentemente contemplata soltanto per i delitti di cui all'art. 51, commi 3-bis e 3- quater, c.p.p. - anche ai reati dei pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p.

In sostanza nella versione oggi in vigore l'art. 266, comma 2-bis, c.p.p. prevede che la captazione tra presenti mediante inoculazione del captatore elettronico su dispositivo mobile è "sempre" consentita (e cioè anche all'interno dei luoghi di privata dimora) non soltanto per i delitti di cui all'art. 51, commi 3-bis e 3-quater, c.p.p., come previsto dalla riforma Orlando ma anche qualora si proceda per taluni reati dei pubblici ufficiali contro la pubblica amministrazione.

E' questa, dunque, la normativa che il ddl Zanettin propone oggi di modificare, espungendo i procedimenti per reati contro la pubblica amministrazione dal novero di quelli nei quali è sempre ammesso l'uso del *Trojan Horse* e promuovendo un ritorno alla soluzione contenuta nella riforma Orlando che limitava l'impiego del Trojan alle indagini per i reati di criminalità organizzata.

7. Tornare alla riforma Orlando?

Nel ragionare di questa complessa tematica occorre andar oltre l'emotività e le pregiudiziali che caratterizzano l'attuale confronto politico e giornalistico sulle intercettazioni e avere costantemente presente due dati.

Il primo: il potenziale di invasività del *Trojan* è enormemente superiore a quello di altri strumenti di captazione, in ragione della sua attitudine a realizzare una intercettazione itinerante, suscettibile di svolgersi in una pluralità di luoghi, anche di privata dimora, con una pluralità di interlocutori, molti dei quali assolutamente estranei ad ogni attività criminosa. L'eccezionale forza di penetrazione nella sfera privata del captatore impone perciò che il bilanciamento tra le opposte esigenze della tutela della collettività e del rispetto della vita privata - necessario per tutte le intercettazioni – debba essere, nel caso dell'uso del *Trojan,* particolarmente rigoroso.

Il secondo dato: l'impenetrabilità delle organizzazioni criminali e la natura dei delitti della grande criminalità organizzata che, per essere ideati, programmati e portati a compimento, reclamano attività che possono, e spesso debbono, svolgersi in permanenza e in tutti i luoghi frequentati dai soggetti sospettati di esserne gli autori; così da rendere all'occorrenza necessaria una compressione del diritto alla vita privata assai più intensa di quella realizzabile nel corso di investigazioni per altri gravi reati.

La combinazione di questi due elementi fa sì che uno strumento eccezionalmente invasivo come il *Trojan* si giustifichi per contrastare i reati di eccezionale pericolosità ed allarme sociale posti in essere da organizzazioni protette da meccanismi di omertà e appaia invece non assolutamente necessario e sproporzionato per altri pur gravi reati.

In altri termini, se le garanzie dettate dagli artt. 14 e 15 della Costituzione e dall'art. 8 della Convenzione europea dei diritti dell'uomo non precludono il ricorso al *Trojan* nelle indagini su reati che mettono a rischio le condizioni della convivenza collettiva come i reati di criminalità organizzata, per altri, pur gravi reati, appaiono legittime valutazioni diverse.

Del resto il bilanciamento realizzato nella riforma Orlando non faceva altro che richiamare ed adattare al *Trojan* l'equilibrio raggiunto per la generalità delle intercettazioni tradizionali dall'art. 13 del dl n. 152 del 1991, norma che consentiva intercettazioni più penetranti nei procedimenti per i reati del crimine organizzato in considerazione delle caratteristiche proprie delle organizzazioni criminali e dei reati da esse commessi.

Per l'applicazione del *Trojan* al di là della sfera dei reati di criminalità organizzata- realizzata dalla legge Spazzacorrotti - non possono essere invocate le vitali ragioni di tutela della collettività ricorrenti nei confronti della criminalità organizzata; così che la devastante invasione della sfera privata realizzata dal *Trojan* ben può essere considerata un prezzo sproporzionato e non strettamente necessario nell'ambito di una società democratica per il contrasto ai reati amministrativi.

Come è noto l'articolo 8 della Cedu - che sancisce il diritto di ogni persona al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza – condiziona la possibilità di ingerenza di una autorità pubblica nella vita privata alla sussistenza di tre requisiti: una previsione legislativa, il perseguimento di una delle finalità legittime, tassativamente indicate dalla norma, che ricomprendono sia una ampia serie di interessi dello Stato e della collettività sia la protezione di diritti e libertà altrui; la necessità della misura, nell'ambito di una società democratica, per il conseguimento dei predetti obiettivi.

In sostanza l'ingerenza dell'autorità pubblica, per essere compatibile con la norma convenzionale, deve rispondere ad un bisogno sociale imperativo e risultare proporzionata alla finalità legittima perseguita.

E questa proporzione, che appare certamente ricorrente nel contrasto delle attività delittuose delle associazioni criminali, risulta socialmente e giuridicamente discutibile [13]quando il Trojan è usato per reati comuni.

Tornare alla legge Orlando, ripristinando il meditato e risalente bilanciamento in tema di intercettazioni previsto dall'art. 13 del dl n. 152 e applicato riguardo al Trojan dal d.lgs. n. 216/2017 sembra perciò una soluzione ragionevole che non dovrebbe destare scandalo e potrebbe essere agevolmente adottata sgombrando il campo da feroci polemiche e sospetti di volontà di un controllo sociale totalizzante da parte della magistratura.

Naturalmente il ritorno alla legge Orlando non escluderebbe in assoluto l'impiego del *Trojan* nelle indagini sui reati contro la pubblica amministrazione ma ne consentirebbe l'utilizzo alle stesse condizioni giuridiche delle intercettazioni tradizionali e dunque in luoghi pubblici o in luoghi di privata dimora ove vi sia fondato motivo di ritenere che vi si stia svolgendo l'attività criminosa.

Sarebbe decisiva in queste ipotesi la possibilità di modulare tecnicamente l'impiego del Trojan, attivandolo o disattivandolo a seconda delle circostanze note *aliunde* agli inquirenti sugli spostamenti del portatore del dispositivo elettronico portatile nel quale è inserito il captatore o sugli sviluppi dell'attività criminosa oggetto di indagini (ad es. quando sia noto agli inquirenti che in un determinato luogo di privata dimora è programmato il pagamento di un compenso per corruzione).

In definitiva ciò che verrebbe precluso è l'intercettazione itinerante in una pluralità di luoghi di privata dimora indeterminabili a priori.

Intercettazione che può risultare tanto più lesiva della sfera privata in quanto è in atto una tendenza ad utilizzare le intercettazioni al di fuori della sfera del processo penale ed in particolare in ambito disciplinare senza neppure consentire adeguate garanzie di ascolto diretto e di consultazione dell'intero compendio intercettato spesso indispensabile per esercitare l'attività difensiva.

[13] Al riguardo la Corte di cassazione nella sentenza n. 35010 del 30 settembre 2020 ha chiarito che in tema di intercettazioni ambientali a mezzo di captatore informatico ("trojan"), il riferimento al luogo di svolgimento dell'intercettazione tra presenti non costituisce presupposto di autorizzabilità, necessario ai fini del rispetto dell'art. 8 CEDU secondo l'interpretazione della giurisprudenza della Corte EDU, essendo, in via alternativa, consentito far ricorso all'indicazione del destinatario di essa ed in considerazione altresì della natura dinamica ed "itinerante" della captazione, che prescinde dal riferimento ai luoghi. Non è dunque ravvisabile un contrasto della normativa di cui si discute con l'art. 8 della Convenzione ma resta aperta, in sede culturale e politica la discussione sulla proporzionalità del ricorso al *Trojan* al di fuori della sfera dei reati di criminalità organizzata.