La criminalità utilizza strumenti informatici in grado di cifrare i contenuti delle comunicazioni. Le forze dell'ordine cercano di affinare le tecniche investigative avvalendosi anch'esse delle nuove tecnologie, come nel caso del trojan chiamato anche captatore informatico. Elenchiamo le norme nel codice di procedura penale che legittimano o potrebbero legittimare l'utilizzo di questa tecnologia, analizzando alcune pronunce giurisprudenziali di legittimità che hanno affrontato il problema.
Prima parte (nel precedente numero): 1. Prmessa, 2. I tecnicismi del Trojan e l'approccio non sempre corretto della Corte di Cassazione.
Seconda parte (in questo numero): 3. Critiche "vecchie" e "nuove" ad alcuni orientamenti.

di Stefano Aterno

IL CAPTATORE INFORMATICO TRA ESIGENZE INVESTIGATIVE E LIMITAZIONI DELLA PRIVACY: UN BILANCIAMENTO NECESSARIO E URGENTE (II PARTE)

Stefano ATERNO è avvocato del foro di Roma e abilitato a patrocinare in Cassazione e presso le altre giurisdizioni superiori, Docente di diritto penale dell'informatica e delle nuove tecnologie presso l'Università LUMSA di Roma, membro del direttivo di IISFA, Assistente ordinario di Informatica Giuridica presso l'Università LUISS. Esperto degli aspetti giuridici della riservatezza dei dati personali e della sicurezza informatica.

3. Critiche "vecchie" e "nuove" ad alcuni orientamenti

Vale la pena pertanto di riprendere qui alcune critiche che vanno ad aggiungersi alle perplessità già espresse in precedenza[1]:
Il trojan altera il computer "target" e appare in contrasto con quanto stabilito dalla legge n. 48/2008 e dalle modifiche al codice di procedura penale; sarebbe quindi opportuno, allo stato, utilizzarlo ad esempio solo quando la legge consente il ricorso al ritardato sequestro (reati di associazione a delinquere di stampo mafioso ecc.); il software capta, monitorizza, registra anche comportamenti non comunicativi che non sono utilizzabili se tenuti all'interno di un domicilio (informatico); occorrerebbe pertanto porsi il problema se, nella prassi o *de iure condendo*, non sia il caso di differenziare l'attività di indagine su sistemi informatici "privati" e su quelli "pubblici".

1 Per le prime critiche sul tema si veda, Aterno, Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto, Memberbook Ilsfa, 2012, Forlì, Experta; Aterno, cit., Digital Forensics, in Aggiornamento - Digesto delle discipline penalistiche, 2013.

Ad avviso di chi scrive è necessario valutare se siamo di fronte ad un mezzo di ricerca atipico giustificato da esigenze reali e non altrimenti risolvibili. In altri termini, verificare se esiste la possibilità concreta di arrivare o meno all'acquisizione del contenuto del PC in altro modo, ad esempio attraverso una perquisizione e un sequestro del computer secondo il metodo classico (oppure, come si diceva sopra con il ritardato sequestro nei casi consentiti dalla legge). Soltanto in caso di assoluta impossibilità ad acquisire il contenuto in queste forme e con questi mezzi tipici di ricerca della prova, come sopra ricordato, si potrebbe giustificare il ricorso a mezzi atipici come il "captatore informatico". È questo il caso di sistemi informatici (es. servers, proxy, sistemi Cloud) allocati all'estero, magari in paesi che non forniscono assistenza alle richieste di rogatoria, oppure a dati allocati magari su piattaforme di *cloud computing* protette da sistemi di cifratura inattaccabili o comunque per loro natura non accessibili se non *on line* e con l'utilizzo di segretissime e complesse parole chiavi. Ecco magari in tutti questi casi potrebbe spiegarsi meglio (in diritto e in fatto) l'utilizzo del "virus di Stato" come mezzo atipico di ricerca della prova.

Un altro punto di criticità all'utilizzo del "captatore" è l'assenza di qualsivoglia controllo diretto e ufficiale sull'attività che svolge l'operatore addetto alla captazione di tutto il contenuto del sistema "target". Quale garanzia ha il pubblico ministero che ha emesso il decreto e autorizzato la captazione sull'attività svolta nel caso in cui decidesse di ricorrere ad ausiliari di polizia esperti o a veri e propri consulenti tecnici? Un ufficiale di polizia giudiziaria assiste sempre a tutte le operazioni che vede e fa il tecnico davanti al proprio sistema? Sono tutte domande alle quali non è possibile dare risposta perché la procedura non è disciplinata ed è lasciata alla sensibilità delle diverse squadre di polizia giudiziaria e delle Procure della Repubblica.
Ad esempio, ad avviso di chi scrive, la redazione di un verbale di polizia giudiziaria, con il dettaglio delle operazioni eseguite nomina di eventuali ausiliari, l'indicazione delle specifiche tecniche del software[2], l'indicazione di date e orari nonché il dettaglio sintetico del monitoraggio effettuato, risolverebbe alcuni problemi.
Sarebbe altresì auspicabile una contemporanea attività di intercettazione telematica dei flussi informatici del sistema "attaccante" (una vera e propria auto-intercettazione telematica o al limite l'utilizzo di un *keylogger* con firma digitale applicato al sistema che controlla il trojan) e quindi dell'utenza della polizia giudiziaria o/consulente tecnico al fine di monitorare e garantire l'indagato da upload anche involontari che altererebbero la *scena criminis*.

Altra forma di garanzia delle operazioni potrebbe essere anche un'attività di *logging* di tutta l'attività che giornalmente svolge il *client* (Personal Computer) "attaccante"[3], con apposizione di firma digitale e marcatura temporale ai file prodotti dal sistema nonché ai file relativi all'acquisizione.

A ben vedere, concretamente il programma consente di captare in tempo reale tutto ciò che appare sul desktop o sul video del personal computer o dello smartphone e quindi anche la navigazione in internet oppure le comunicazioni via chat (di ogni genere e social network). Riesce a fare ciò attraverso gli *screen shot* (delle vere e proprie foto dello schermo). Pertanto non è vero quando affermato in alcune pronunce o da qualche Gip - ad oggi pochi a dire il vero - che è necessario soltanto il decreto per l'eventuale intercettazione "ambientale". Quindi è vero il contrario, il trojan può fare anche altro. Pertanto, tralasciando per un attimo gli *screen shot* di cui ci occuperemo tra poco, si può sostenere che tutta l'attività di documentazione e repertamento dei flussi telematici (esempio la modalità keylogger relativa alla captazione delle password digitate) necessita, ad avviso di chi scrive, di decreti di intercettazione telematica ex art. 266 bis c.p.p. e quindi del vaglio del giudice per le indagini preliminari.
Ciò racchiude in sé un altro problema di fondo: in uno stato di diritto con garanzie processuali codificate la corsa al risultato a tutti i costi non può comprimere le garanzie processuali, le garanzie difensive e il dovuto controllo del giudice per le indagini preliminari sugli strumenti investigativi che mettono in pericolo il contenuto delle comunicazioni e la riservatezza del domicilio (anche informatico).

Dopo anni di silenzio e di convinzione della giurisprudenza che la soluzione della "prova atipica" fosse la cura di tutti i mali, in epoca recente la Suprema Corte torna sul captatore con un paio di sentenze[4] che hanno portato ad una pronuncia delle Sezioni Unite che però ha risolto il problema solo in parte.
Le Sezioni Unite della Cassazione hanno fatto luce sul problema dell'utilizzo del virus Trojan a fine di indagini giudiziarie limitatamente ad una sola delle molteplici funzionalità operative dello strumento informatico in esame, ossia alla cd. intercettazione ambientale itinerante ovvero all'intercettazione di comunicazioni tra presenti *ex* art. 266 comma 2 c.p.p. potendo seguire il soggetto in una pluralità di luoghi (domiciliari e non).

Le vicende legate all'utilizzo dello strumento informatico sono emerse a livello giudiziario con la sentenza Virruso (Sez. 5, n. 16556 del 14/10/2009, dep. 2010, Rv. 246954) e a livello mediatico, con la vicenda delle indagini sulla cd "P4" e dell'arresto di Luigi Bisignani. Nel giugno 2011, il trojan e il suo utilizzo diventano informazioni di pubblico dominio, dopo che per anni gli investigatori italiani avevano cercato di mantenere riservato il suo utilizzo a fini di indagini penali assicurando alla giustizia anche importanti appartenenti ad organizzazioni mafiose.

Dopo tale episodio, il trojan come strumento investigativo scompare come un fiume carsico per riapparire nel caldo luglio del 2015, quando le conseguenze generate dall'attacco informatico effettuato ai danni della società milanese *Hacking Team*, con la conseguente compromissione del codice sorgente del software creato da quella società e la diffusione sul web di numerose email tra investigatori e dirigenti della società, mettono in serio pericolo anni di indagini giudiziarie.

2 *La difesa deve sapere cosa ha fatto o è in grado di fare il software introdotto nel sistema.*

3 *Per questo potrebbe essere utilizzato un sistema di keylogger implementato sulla macchina che intercetta/capta e quindi riceve il contenuto del sistema "target" in modo da registrare e garantire ogni attività che svolge il "trojan di stato".*

4 *Sentenza 6 Sezione, n. 27100 del 26/5/2015, Musumeci, Rv. 265654.*

Come si ebbe già modo di dire diversi anni fa[5] e come ricordato anche sopra, un software trojan in dotazione alle forze di polizia in quanto acquistato o noleggiato da società private italiane e straniere, oggi è in grado di effettuare una serie di operazioni, alcune molto invasive.

L'uso del Trojan è molto più di un'intercettazione telefonica o telematica che, in quanto tale, necessita dell'ausilio dell'operatore telefonico e quindi di un terzo soggetto vincolato a tracciare le operazioni. Qui non c'è tracciamento delle operazioni di captazione da remoto del contenuto di un computer o di uno smartphone, o meglio, nulla è attualmente previsto dalle norme vigenti o dalla prassi.
Seppur limitatamente ai soli aspetti legati all'intercettazione tra presenti tramite software trojan, le Sezioni Unite hanno avuto il pregio di chiarire gli aspetti giuridici e processuali sottesi e confermare la liceità delle intercettazioni relative a procedimenti di criminalità organizzata in quanto in tali casi l'indicazione del luogo risulterebbe irrilevante dal momento che le captazioni delle conversazioni nei luoghi di privata dimora non sono soggette ad alcuna disciplina in deroga rispetto ad altri luoghi in virtù dell'art. 13 del decreto legge n. 152 del 1991 (convertito dalla legge n. 203 del 1991).

La sentenza delle Sezioni Unite avrebbe dovuto indicare la strada anche rispetto ad un'altra funzione del software trojan, meno nota ma molto più invasiva, della mera intercettazione tra presenti. La sentenza in commento si sofferma solo sui motivi del ricorso delle difese in tema di intercettazioni tra presenti ma a pag.8 dimostra di essere consapevole che "*lo strumento tecnologico consente……..di perquisire l'hard disk e di fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira*.".
A tale affermazione però non segue un approfondimento degli aspetti giuridici. Se il software è in grado anche di acquisire da remoto i files e il contenuto memorizzato sul computer, sullo smartphone o sull'ipad tale attività non rientra tra le intercettazioni. Questo aspetto non può essere trattato separatamente in quanto costituisce tecnicamente una delle funzionalità del software attivabile da remoto dall'operatore in qualsiasi momento anche senza aver avuto l'autorizzazione da parte del pubblico ministero. Sotto il profilo giuridico tale attività non rientra certamente nel genere delle intercettazioni tantomeno telematiche e forse questo aspetto poteva essere affrontato da una pronuncia cosi importante. Di questi aspetti proveremo ad occuparci diffusamente più avanti.

La delicatezza dell'uso di questo nuovo ed invasivo mezzo di ricerca della prova era nota da molti anni e il trojan era largamente utilizzato per finalità investigative ad ogni livello nonostante le norme del codice di procedura penale non prevedessero nello specifico alcune attività captative a distanza.
Per anni, almeno dal 2010 (con la sentenza Virruso del 2009) al 2015/2016 (fino alle sentenze Musmeci e Scurato) l'utilizzo del trojan anche in modalità acquisitiva a distanza è stata erroneamente motivata dalla giurisprudenza come prova atipica ai sensi dell'art. 189 c.p.p. È emerso fin da subito evidente che tale acquisizione, occulta da remoto, non poteva essere paragonata ad una prova acquisita nel contraddittorio tra le parti al pari di un Cd rom.

È di fondamentale importanza non confondere e comprendere bene la differenza tra cosa si acquisisce con le intercettazioni telematiche "passive" e cosa si acquisisce con quelle invece definite "attive" effettuate mediante trojan nonché la differenza con l'art. 189 cpp.

Quando è possibile parlare di flusso intercettabile? Ma soprattutto cosa s'intende per "flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi"(art. 266 bis c.p.p)? È possibile ritenere tale anche il flusso di dati e informazioni intercorrente tra più componenti dello stesso sistema informatico? E in tal caso è possibile utilizzare l'art. 266 bis cpp quando si procede con il captatore ad effettuare gli *screen shot*?
L'oggetto di un flusso di comunicazioni cifrato (es. fotografie scambiate con chat e sistemi di messaggeria, o via email) viene captato dal Trojan solo dopo essersi memorizzato nel sistema, non fa parte appunto del un flusso[6] perché non viene intercettato "mentre transita" bensì viene eventualmente acquisito come un "documento" presente nella memoria del sistema ovvero in un luogo che definiamo orami pacificamente come domicilio informatico. In questi casi non siamo davanti ad una intercettazione bensì ad una attività ispettiva o di perquisizione e di controllo, a cui segue l'acquisizione del file ovvero del documento all'interno appunto dell'apparato informatico/domicilio informatico.

L'intercettazione telematica classica ex art. 266 bis c.p.p intercetta il flusso dei dati dal server del gestore telefonico/internet service provider (che danno connessione) al personal computer dell'indagato ! Si pone nel mezzo del flusso tra due punti e capta il flusso dei dati che passano tra il pc e il gestore che fornisce connessione di rete. L'intercettazione telematica capta i dati che passano dal pc e vanno in rete**.** Viene captato il flusso dei dati che dall'interno di un supporto informatico (anche, ma non necessariamente, visualizzati sullo schermo) viene trasferito ad un altro sistema informatico.

Con il captatore o trojan accade una cosa un po' diversa perché a parte l'importante funzione di acquisizione di una copia di tutti i dati presenti in memoria o di parti di essi[7], possono essere effettuati anche i c.d. *screen shot* ovvero una sorta di fotografia digitale di ciò che appare sullo schermo del sistema o dello smartphone attraverso una banale funzione del sistema operativo, e quindi :

- documenti e file memorizzati sull'apparato (es. fotografie) che vengono visualizzati dall'ignaro utente per essere visti letti o modificati;
- pagine di siti web che l'utente sta visitando mentre naviga nella rete internet;

5 Aterno, cit., Digital Forensics, in Aggiornamento - Digesto delle discipline penalistiche, 2013.

6 Che appunto non viene intercettato perché magari transita su canale cifrato.

7 È noto che attualmente s'incontrano notevoli difficoltà attuative – come ad esempio batterie scariche e Gigabyte che finiscono - e per superare tali difficoltà, come ad esempio l'acquisizione di una enorme quantità di file, talvolta si ricorre ad acquisizioni semplificate.

- documenti, dati e immagini presenti e visualizzati durante l'accesso ad un sistema informatico collegato telematicamente e in uno spazio cloud;
- documenti, dati e immagini presenti e visualizzati durante l'accesso ad un server connesso con il sistema informatico dell'utente attraverso una linea dedicata (anche cifrata);
- account di posta elettronica sia nel caso di collegamento ad un account web mail sia in caso di accesso (anche off line) ai file di posta elettronica presenti nel sistema.

Potremmo parlare di "intercettazione sui generis" nei casi di screen shot di siti web, pagine webinternet, blog, server on line durante la loro visione in tempo reale da parte del soggetto sotto indagine. Solo in quest'ultimo caso, forse, potremmo parlare di intercettazione telematica sia pure sui generis ma in tutti i casi dobbiamo essere consapevoli che stiamo forzando l'interpretazione dell'articolo 266 bis cpp e il concetto di flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi. Tralasciando i casi più semplici in cui vi è un flusso tra più sistemi anche se riferibili ad uno stesso utente, il punto è se la norma dell'art. 266 bis c.p.p. può essere applicata anche tutti quei flussi di dati e di informazioni (comunicazioni) che non intercorrono tra più sistemi informatici bensì soltanto tra componenti dello stesso sistema informatico ovvero tra tastiera e schermo, tra hard disk e schermo o tra sistema operativo e display.

Potrebbe sembrare anche una forzatura dell'interpretazione normativa ma è anche vero che nell'interpretazione della norma processuale non si è condizionati da principi di tassatività tipici della norma penale ed è consentito talvolta il ricorso all'analogia. Certamente il dubbio più forte si pone rispetto agli screen shot dei files memorizzati nello stesso sistema e visualizzati sullo schermo in modo intellegibile grazie al flusso tra più componenti del sistema informatico; in assenza di qualsiasi altra interazione con altri sistemi informatici o con altri flussi.
Ma a ben vedere, l'ipotesi più garantista è quella che ritiene che siamo di fronte ad una attività del captatore simile all'ispezione di cui all'art. 244 cpp oppure ad una perquisizione (nel domicilio informatico dell'indagato) occulta e ad una acquisizione di copia del documento. Ma se ciò è più corretto sotto il profilo applicativo e normativo dovrebbe poi seguire la necessaria notifica dell'atto all'indagato in quanto trattasi di atti per i quali è prevista la presenza dello stesso.
È abbastanza pacifico che rispetto ai dati informatici "statici" nel PC o sullo smartphone l'acquisizione con il trojan della copia digitale non è il risultato di una intercettazione telematica.

Questa interpretazione restrittiva non lascia le forze dell'ordine senza uno mezzo di ricerca della prova, perché esistono mezzi tipici di ricerca della prova rappresentati dalla perquisizione e dal sequestro dei supporti informatici dai quali possono essere estratti i dati ivi contenuti. Vista l'esistenza di mezzi di ricerca tipici della prova è di tutta evidenza che non è possibile ritenere un mezzo atipico di ricerca della prova il captatore e i dati acquisiti di nascosto all'interno del supporto. Costante giurisprudenza e la dottrina migliore da sempre hanno ritenuto impossibile ipotizzare l'esistenza di un mezzo di ricerca della prova atipico quando per raggiungere lo stesso risultato investigativo (acquisire il contenuto di un PC) si può procedere al suo sequestro e poi all'acquisizione del suo contenuto con le normali tecniche di computer forensics.

La sentenza Virruso sulla prova atipica confonde lo strumento di acquisizione con l'oggetto acquisito. Inutilizzabile, tanto nel 2009 quanto oggi, è il trojan/captatore informatico quale mezzo di ricerca della prova atipico e che non necessita di essere disciplinato dalla legge o legittimato dalla giurisprudenza, perché esistono mezzi tipici di ricerca della prova che possono essere utilizzati al suo posto. Continuare oggi (anno 2017) a sostenere, che il captatore è una "prova atipica" ex art. 189 c.p.p. è profondamente errato perché il contenuto del supporto informatico o il dato relativo allo schermo sono dati informatici compiutamente disciplinati dal codice. Semmai il captatore è un mezzo di ricerca atipico che, come però si è sin qui cercato di motivare, non si giustifica a fronte del possibile impiego di mezzi di ricerca della prova tipici e classici come la perquisizione e il sequestro.

La circostanza che tale strumento è in grado di acquisire da remoto, il contenuto senza che l'indagato se ne renda conto e che questo costituisce un'ottimo strumento investigativo, non è sufficiente a legittimarne l'utilizzo ma, come più volte sostenuto da questo autore, eventualmente a spingere il legislatore a disciplinarne l'uso.
L'ordinanza di rimessione alle Sezioni Unite da parte della Sesta sezione è intervenuta nel marzo del 2016 proprio nel momento in cui stava sorgendo un primo contrasto giurisprudenziale in virtù di una sentenza della sesta sezione (Sentenza 6 Sezione, n. 27100 del 26/5/2015, Musumeci, Rv. 265654) ed è intervenuta in relazione ad un uso limitato del captatore in funzione di apparato di intercettazione voce tra presenti.

Lo scopo di questa veloce fissazione probabilmente è stato quello di evitare un contrasto giurisprudenziale in una materia cosi difficile e specifica, tenuto conto della ormai diffusa utilizzazione del cd. agente intrusore e dell'alto grado di complessità tecnica. Il quesito al vaglio delle Sezioni Unite può essere sintetizzato in questo senso ovvero di comprendere se, anche nei luoghi di privata dimora ex art. 614 cod. pen., pure non singolarmente individuati e anche se ivi 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.

Al fine di comprendere le motivazioni delle Sezioni Unite è imprescindibile tenere presente che sotto un profilo giuridico la questione affrontata riguarda un procedimento di criminalità organizzata e sotto il profilo tecnico la captazione prescinde dal riferimento al luogo, trattandosi di una intercettazione ambientale per sua natura itinerante.
La Suprema Corte a tratti sembra affermare che deve escludersi la possibilità di intercettare nei luoghi indicati dall'art. 614 cod. pen., con il mezzo del captatore informatico al di fuori dei casi di criminalità organizzata e quindi al di fuori della disciplina derogatoria di cui all'art. 13 del decreto legge n. 152 del 1991 (convertito dalla legge n. 203 del 1991), che consente l'intercettazione tra presenti senza che, nel decreto di autorizzazione, vi sia l'obbligo di precisare il luogo nel quale è consentita l'intercettazione

né di dimostrare che in quel luogo si sta svolgendo l'attività criminosa. Nel sostenerlo da un lato sottolinea che il requisito autorizzativo incentrato sul "fondato motivo di ritenere che" nei luoghi di privata dimora "si stia svolgendo l'attività criminosa" è centrale e non consente alcun genere di eccezioni. Dall'altro lato ritiene che nel momento di autorizzare una intercettazione da effettuarsi a mezzo captatore informatico installato su un apparecchio portatile, il Giudice non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo verrà introdotto. Ciò porterebbe all'impossibilità di controllare l'effettivo rispetto della normativa in materia sulle intercettazioni domiciliari. A questo proposito aggiunge che, anche se fosse possibile seguire gli spostamenti dell'utilizzatore del dispositivo e sospendere la captazione nel caso di ingresso in un luogo di privata dimora, sarebbe impedito comunque il controllo del Giudice al momento dell'autorizzazione che quindi verrebbe disposta "al buio". Su quest'ultimo punto ci soffermeremo più avanti.

Per le indagini relative ai delitti di criminalità organizzata la sentenza in commento sottolinea che è prevista invece una disciplina speciale. L'art. 13 del citato decreto legge n. 152 del 1991 deroga al limite di cui all'art. 266 comma 2 del cod. proc. pen. e pertanto l'intercettazione domiciliare è consentita "anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa" ovvero anche quando non vi sono gravi indizi per ritenere che in quell'ambiente si sta svolgendo l'attività criminosa[8]. È di tutta evidenza il carattere eccezionale della normativa in relazione a fattispecie criminose per le quali è particolarmente molto difficile l'attività d'indagine. Il punto fondamentale sul quale s'impernia la motivazione della Suprema Corte è proprio sull'irrilevanza dell'indicazione dell'ambiente in questi particolari procedimenti penali.

La sentenza Musumeci, sopra citata, riguardava un reato di natura associativa ma, sottolineano le Sezioni Unite, non ha considerato l'art. 13 del d.l. n. 152/1991 bensì si è limitata a rilevare che la captazione di conversazioni tra presenti con tale strumento entra in conflitto con la libertà di comunicare in più "ambienti" a seconda degli spostamenti del soggetto e nella completa assenza da parte del Giudice di previsione e quindi di autorizzazione specifica.

Le Sezioni Unite nel non condividere tale assunto per i motivi sopra ricordati aggiungono che dai testi normativi e emergono due categorie di intercettazioni: quella generale delle "intercettazioni di comunicazioni tra presenti" ed un'altra più limitata ovvero quella delle "intercettazioni di comunicazioni tra presenti nei luoghi di privata dimora". La sentenza Musumeci nell'accennare sempre a intercettazioni "ambientali"[9] non affronta la distinzione con la prima categoria ovvero con le "intercettazioni tra presenti" omettendo di confrontarsi con il dato normativo. Tra le altre cose, ricordano le Sezioni Unite a pagina 18 della sentenza, per costante giurisprudenza non occorre sempre indicare con precisione tutti "i luoghi" nei quali vengono effettuare le intercettazioni tra presenti. Tale indicazione è esclusa ad eccezione dei casi in cui si deve effettuare l'intercettazione "in luoghi di privata dimora"[10] e pertanto quando risultano indicati il destinatario della captazione e la tipologia di ambienti intercettati (diversi dai luoghi di provata dimora), l'intercettazione è utilizzabile anche qualora venga effettuata in un altro luogo rientrante nella stessa categoria (diverso dalla privata dimora).

Si può pertanto ritenere pacifico, anche se non chiaramente indicato dalla sentenza, che in tutti i luoghi pubblici o aperti al pubblico (non riconducibili all'art. 614 cod. pen) è possibile utilizzare il trojan per effettuare intercettazioni tra presenti anche fuori dai casi di delitti di criminalità organizzata ? La risposta potrebbe essere affermativa ma resta il problema a cui prima si faceva cenno e che meritava uno sforzo maggiore da parte della Cassazione ovvero capire come, anche tecnicamente e con prova certa, poter distinguere il momento in cui il soggetto intercettato si sposta con il dispositivo all'interno di una abitazione. La tecnologia e lo stesso strumento offrono soluzioni accettabili anche sotto il profilo delle garanzie come per esempio la possibilità di geolocalizzazione e di disattivazione dell'audio all'interno dell'abitazione. Per fare ciò però occorrerebbe una chiara indicazione di tali garanzie all'interno degli atti di autorizzazione del Giudice e una partecipazione attiva alla fase di stralcio da parte della difesa. Lo strumento è tanto invasivo (si ricorda che è in grado di modificare a piacimento il contenuto di un dispositivo) quanto utile alle investigazioni ma è necessario che sia compreso da tutti che lo sforzo sulle garanzie deve essere massimo. ©

8 Si vedano anche altre due sentenze non massimate della stessa Cass. VI, che avevano posto proprio l'art. 13 del d.l. n. 152/1991 a base della ritenuta utilizzabilità delle intercettazioni tramite "virus informatico" in procedimenti per delitti di criminalità informatica, Sez. 6, 8/4/2015, n. 27536; Sez. 6, 12/3/2015, n. 24237.

9 Locuzione utilizzata diffusamente in dottrina e in giurisprudenza ma non esaustiva e non comprensiva della intercettazioni tra presenti fuori da luoghi e ambienti di ogni genere

10 Cass. Sez. 1, 25/9/2009, n. 11506, Molè, Rv. 243044 ; Cass. Sez. 2, 8/4/2014, n. 17894, Alvaro.