Il Trojan dalla A alla Z.
Esigenze investigative e limitazioni della privacy:
un bilanciamento necessario

di Stefano Aterno

Sommario: Premessa; 1. I tecnicismi del Trojan e l'approccio non sempre condivisibile della Corte di Cassazione; 2. Critiche "vecchie" e "nuove" ad alcuni orientamenti ; 3. Il tema delle intercettazioni tra presenti con il captatore anche fuori dai casi di criminalità organizzata. La sentenza Scurato del 2016 delle Sezioni Unite della Corte di Cassazione; 4.Le ipostesi legislative sul tavolo. 4.1 La proposta Quintarelli 4.2 L'art. 84 lett. e) del DDL Orlando recante modifiche al Codice di procedura penale.

Premessa

Sempre più di frequente la criminalità utilizza strumenti informatici (hardware e software) in grado di far perdere le tracce dei delitti commessi. Le forze dell'ordine rincorrono con grande difficoltà, affinando tecniche investigative e nuove tecnologie spesso in assenza di norme giuridiche di riferimento: è oggi noto il caso del Trojan chiamato anche captatore informatico[1] ma in realtà è uno strumento usato da molto tempo seppur con diverse versioni software.

L'acquisizione occulta on line da remoto del contenuto digitale di un supporto informatico collegato alla rete Internet è uno dei metodi con i quali, tra le altre cose è possibile entrare, non senza difficoltà, in ogni spazio informatico d'interesse investigativo, si pensi ad esempio all'accesso ad un account cifrato su piattaforma in Cloud computing.

Quali norme nel codice di procedura penale legittimano o potrebbero legittimare l'utilizzo di questa tecnologia ?

---

[1] Per uno dei primi scritti completi e specifici sul captatore si consenta il rinvio a ATERNO, paragrafo 12 della voce Digital Forensics (Investigazioni informatiche), pag. 243, Aggiornamento, Digesto Discipline Penalistiche, 2013, Utet.; ATERNO, Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto, Memberbook IIsfa, 2012, Forlì, Experta

Cercheremo di rispondere a questa domanda anche alla luce di alcune pronunce giurisprudenziali di legittimità[2] che hanno affrontato il problema.

1. I tecnicismi del Trojan e l'approccio non sempre corretto della Corte di Cassazione;

La prima di queste è la sentenza della Corte di Cassazione del 2010 che trae origine da alcune indagini per associazione a delinquere di stampo mafioso e all'utilizzazione di un captatore informatico (software virus trojan)[3] disposto con decreto di acquisizione di atti ai sensi dell'art. 234 c.p.p., emesso dal pubblico ministero.

Il decreto aveva ad oggetto l'acquisizione in copia della documentazione (informatica) memorizzata all'interno del personal computer in uso ad uno degli imputati e installato presso alcuni uffici Comunali.

L'atto, pur autorizzando una mera acquisizione in copia degli atti, non presupponeva un'attività di intercettazione di comunicazioni informatiche ai sensi degli artt. 266 bis ss. c.p.p. e tale richiesta non fu portata all'attenzione del giudice per le indagini preliminari. Invero, il decreto disponeva la registrazione non solo dei files esistenti, ma anche dei dati inseriti in futuro nel personal computer, in modo da acquisirli periodicamente. Le concrete modalità esecutive del decreto, consistite nell'installazione, all'interno del sistema operativo del personal computer, di un captatore informatico erano in grado di memorizzare i files già esistenti e di registrare in tempo reale tutti i files elaborandi, innescando in tal modo un monitoraggio occulto e continuativo del sistema informatico.

Il problema che la Cassazione ha affrontato fu di stabilire se l'attività captativa fosse o meno un'attività di intercettazione telematica. La Corte di Cassazione nelle motivazioni, non ha ritenuto che questa captazione fosse un'attività di intercettazione telematica ex art. 266 bis c.p.p. in quanto la registrazione non avrebbe avuto ad oggetto «un flusso di

---

[2] Cass. pen., sez. V, (14-10-2009) 29-4-2010, n. 16556, CED, 246954, Virruso. Per il primo commento alla sentenza si consenta il rinvio ad ATERNO*, Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto, Memberbook IIsfa, 2012, Forlì, Experta; Cass. VI, 26/5/2015, n. 27100 Musumeci, Rv. 265654; Cass. S.U. Ud. 8.4.2016, (dep. 1.7.2016), n. 26889, Scurato.*

[3] Software Trojan nascosto che consente all'utilizzatore di prendere il completo controllo del computer o dello smartphone; all'epoca probabilmente fu utilizzato un Software dal nome "Back Orifice".

comunicazioni» che presuppone un dialogo con altri soggetti, ma «una relazione operativa tra microprocessore (?? ndr) e video del sistema elettronico» ovvero «un flusso unidirezionale di dati». Il decreto del pubblico ministero, hanno precisato i giudici di legittimità, si era limitato a disporre che, ad opera della polizia giudiziaria, fossero estrapolati sia i dati già formati e contenuti nella memoria del personal computer in uso ad uno degli imputati sia quelli che in futuro sarebbero stati memorizzati. La Corte ha anche chiarito che per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici, non potendosi ritenere intercettazione di un flusso di comunicazioni la captazione di un'elaborazione del pensiero e la sua esternazione in scrittura su di un personal computer oppure mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura.

Secondo questa sentenza della Suprema Corte, pertanto, l'attività di captazione in questione deve essere ricondotta nel concetto di "prova atipica", sottratta alla disciplina prescritta dagli artt. 266 ss. c.p.p., con conseguente e pacifico utilizzo dei risultati. La Corte ha risposto anche ad altre eccezioni ovvero ha ritenuto, che l'attività captativa non avesse violato né l'art. 14 Cost. né l'art. 15 Cost.

Il personal computer, infatti, si trovava nella locale sede di un ufficio pubblico comunale, ove sia l'imputato sia gli altri impiegati avevano accesso per svolgere le loro mansioni e ove potevano fare ingresso, sia pure in determinate condizioni temporali, il pubblico degli utenti e il personale delle pulizie, insomma una comunità di soggetti non particolarmente estesa, ma nemmeno limitata o determinabile a priori in ragione di una determinazione personale dell'imputato.

Nel caso di specie non poteva essere invocata la tutela costituzionale della riservatezza della corrispondenza e in genere delle comunicazioni, giacché quanto riprodotto in copia, non era un testo inoltrato e trasmesso col sistema informatico privato e personale, ma "soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario".

Non si è posto neanche il problema circa l'applicabilità della disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei files memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria. Si era trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa poteva essere compiuta una seconda volta se solo si fosse poi approdato ad uno sviluppo dibattimentale del procedimento.

Sotto il profilo della prova atipica e della sua formazione la Corte ha altresì escluso la violazione della disciplina di cui all'art. 189 c.p.p., in quanto la mancata acquisizione in contraddittorio della prova documentale estrapolata dal personal computer era dipesa dalla scelta difensiva del rito abbreviato, e la prescrizione, ex art. 189 c.p.p., che impone al giudice di procedere in contraddittorio tra le parti riguarda l'assunzione delle fonti di prova e non dei mezzi di ricerca della prova.

Tale decisione della Suprema Corte è stata aspramente criticata[4] in quanto ha dimenticato e lasciato irrisolti molteplici aspetti.

Appare difficile smentire che siffatta attività di captazione da remoto attraverso un software trojan autorizzato dal pubblico ministero non sia un'intercettazione di comunicazioni informatiche o telematiche. Il personal computer per poter trasmettere dati all'organo di polizia era necessariamente connesso alla rete internet tramite Internet serve provider[5] e tra i dati captati da remoto vi era certamente, anche in parte, il flusso di dati relativi alla navigazione su Internet ovvero a comunicazioni effettuate tra il personal computer e l'Internet serve provider. Non è dato sapere di eventuali comunicazioni via chat o altre piattaforme informatiche di comunicazioni tra più soggetti (IRC, messanger,

---

[4] Si consenta un rinvio all'unico articolo pubblicato in materia, ATERNO, Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto, Memberbook IIsfa, 2012, Forlì, nonché al ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in Manuale di Computer Forensics, 2012, Forlì, nonché al già citato ATERNO, paragrafo 12, pag. 243, Aggiornamento, Digesto Discipline Penalistiche, e si veda da ultimo, TESTAGUZZA, Exitus acta probat "Trojan" di Stato: la composizione di un conflitto, in Archivio penale, maggio – giugno 2016.

[5] Il virus necessariamente inviava attraverso la rete i dati captati alla stazione ricevente degli investigatori.

skype[6], ecc.) ma ove vi fossero state non vi sarebbero stati dubbi sull'applicabilità delle garanzie dell'art. 266 bis c.p.p.

In caso di intercettazione di navigazione sulla rete internet il tema è più complesso e meriterebbe una trattazione a parte. Si rimanda pertanto su quest'ultimo punto a opere più specifiche che hanno affrontato anche tecnicamente la tematica[7].

Le caratteristiche tipiche specifiche del software trojan utilizzato fin dal 2004 non sono note, ma sarebbe utile la loro presenza negli atti del processo a garanzia delle operazioni compiute dal nuovo sistema tecnologico intrusivo. Ciò che emerge dalla sentenza è sufficiente però per capire almeno in parte cosa è stato (ed è..) in grado di fare tale software[8].

Gli apparati investigativi sono stati in grado di inoculare e installare sul PC dell'indagato un programma "fantasma" capace di inviare in maniera occulta tutti i documenti in formato word che l'indagato scriveva e tutte le aggiunte o correzioni che con il tempo (8 mesi) eseguiva sui documenti word redatti e memorizzati sull'hard disk del computer d'ufficio dell'indagato (non sembra fosse un PC portatile). Non erano affatto documenti che il soggetto inviava a terzi o che inviava per posta elettronica o pubblicava sulla rete internet e quindi non erano comportamenti comunicativi.

Stupisce anche il punto in cui la Corte di Cassazione ritiene che la prova raggiunta sia una prova atipica e quindi disciplinata dall'art. 189 c.p.p. In realtà, a ben vedere, trattandosi di files informatici contenuti su supporti informatici tipizzati e introdotti nel nostro ordinamento con la legge n. 547/1993, forse qui non è tanto in discussione la prova atipica ma il mezzo con la quale è stata acquisita la prova e quindi l'utilizzo di mezzi atipici di ricerca della prova.

Parte della dottrina[9] si domanda se siano configurabili mezzi di ricerca della prova atipici soprattutto quando le circostanze di fatto e di diritto consentono di acquisire gli elementi

---

[6] All'epoca dei fatti di cui in sentenza (2004), il sistema di comunicazione via skype non era ancora stato inventato.

[7] ATERNO-CAJANI-COSTABILE-MATTIUCCI-MAZZARACO, in Manuale di Computer Forensics, cit., 2012. Si veda, per una prima analisi tecnica sul punto, AA.VV, in Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunicazioni voip, Riv. Internet, 2008, 558 ss.

[8] Oggi questi software sono molto più evoluti rispetto al 2004 e in grado di svolgere attività ancora più sofisticate; si veda, per un utilizzo molto commerciale e ormai comune e diffuso, il software win spy, scaricabile dalla Rete e facilmente rintracciabile digitando il nome nei motori di ricerca.

[9] TONINI, Manuale di procedura penale, cit., 258.

di prova attraverso l'utilizzo dei tipici mezzi di ricerca come perquisizioni, sequestri o ritardati sequestri. Si tende a negare tale categoria non prevista dal codice di procedura rilevando che i mezzi di ricerca della prova sono posti in essere prevalentemente nel corso delle indagini preliminari in situazioni nelle quali è impossibile il contraddittorio con la difesa davanti al giudice come indica l'art. 189 c.p.p.

Di contro, le Sezioni Unite della Cassazione[10] hanno affermato che è possibile configurare mezzi di ricerca della prova atipici come per esempio le video-riprese d'immagini in luoghi diversi dal domicilio attraverso un'interpretazione adeguatrice dell'art. 189 c.p.p. nel senso di configurare un contraddittorio posticipato e successivo sull'utilizzabilità degli elementi acquisiti[11]. La medesima pronuncia ha anche affermato che ove le video-riprese avvengono invece in luoghi domiciliari o di privata dimora non sono utilizzabili quelle aventi ad oggetto comportamenti non comunicativi. È di tutta evidenza che soltanto un'interpretazione della norma in questo senso è rispettosa del principio di legalità della prova.

Nel caso del trojan usato come captatore informatico è ancora più evidente che una interpretazione in questo senso dell'art. 189 c.p.p. può essere agevolmente condivisa solo e in quanto il personal computer sottoposto ad "acquisizione" non è classificabile come domicilio informatico[12].

La Corte di Cassazione non convince affatto quando sul punto ritiene «che, nella specie, dovesse essere osservata la disciplina prevista per gli accertamenti tecnici irripetibili, atteso che l'attività di riproduzione dei files memorizzati non aveva comportato l'alterazione, né la distruzione dell'archivio informatico, rimasto immutato, quindi consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria. Si era trattato di un'attività sempre reiterabile, alla cui esecuzione non era necessaria la partecipazione del difensore, poiché la stessa avrebbe potuto essere

---

[10] *Cass. pen., S.U., 28-3-2006, n. 26795.*

[11] TONINI, *Manuale di procedura penale, cit., 258.*

[12] *Per una attenta analisi del concetto di domicilio (informatico) relativamente all'uso del captatore per finalità investigative si veda l'ottimo contributo di* PINELLI,*Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato", in Diritto penale contemporaneo, 2017,* http://www.penalecontemporaneo.it/upload/PINELLI_2017a.pdf

compiuta una seconda volta se si fosse approdato ad uno sviluppo dibattimentale del procedimento».

Con riferimento alla mancata osservanza della disciplina prevista per gli accertamenti tecnici irripetibili (artt. 359 e 360 c.p.p.) e al mancato avviso alle parti e ai difensori la Suprema Corte però non convince perché non ha tenuto conto né ha motivato che:

– un sistema informatico sottoposto ad intrusione da parte di un "Trojan di Stato" è comunque alterato a livello strutturale e informatico;

– con il cosiddetto "captatore" all'interno del sistema informatico mutano alcune funzioni di sistema specifiche che consentono ad un operatore da remoto e connesso alla rete di prendere il possesso dello strumento e di far compiere allo strumento stesso una serie di operazioni fuori dal controllo dell'utente autorizzato modificando molte funzioni tipiche di sicurezza del sistema;

– di eseguire una serie di funzioni tipiche del software conosciute soltanto dal creatore dello stesso;

– di alterare anche accidentalmente il contenuto del sistema informatico non consentendo alla difesa di ripetere l'operazione di acquisizione;

È assai discutibile sostenere, come fa la Corte, che l'attività è sempre reiterabile in quanto è possibile compierla anche una seconda volta al momento del dibattimento. È come dire che una perquisizione domiciliare (irripetibile per eccellenza) è ripetibile "*n*" volte perché la difesa può tornarci quando vuole dopo che il locale è stato perquisito dalle forze di polizia. Non è proprio così o comunque non è assolutamente stato dimostrato come sia stata garantita la genuinità e integrità dei files acquisiti.

Esistono ed esistevano anche nel 2004 sistemi e procedure tecniche in grado di garantire che un file prima e dopo l'acquisizione non veniva modificato e che la copia effettuata può essere poi verificata dalla difesa e valutata nella sua integrità e genuinità[13].

---

[13] *Tecniche e procedure di hashing note soprattutto oggi in quanto la legge n. 48/2008 ha introdotto particolari disposizioni che necessitano di tali accortezze ma non vi è dubbio che sono tecniche conosciute a livello informatico anche nel 2004 tra le forze di polizia che effettuavano tali indagini ma delle quali non c'è menzione nella sentenza*

Stiamo parlando delle tecniche di hashing che avrebbero potuto garantire l'integrità e la genuinità dei file captati da remoto se effettuate prima dell'operazione e soprattutto con criterio e con la finalità di dimostrare poi alla difesa la genuinità della prova.

Questo tema è molto importante e delicato perché non può tacersi l'utilità di risolvere, anche legislativamente, il problema giuridico dell'ammissibilità di uno strumento tanto pericoloso quanto utile ed efficace in alcuni contesti specifici (criminalità organizzata, utilizzo illecito di sistemi criptati e di cloud computing allocati in server residenti in remote e sconosciute regioni del mondo, sistemi informatici e dati/informazioni non acquisibili altrimenti, ecc.).

Fermandosi a ciò che è noto attraverso l'analisi dei software in commercio sulla rete, ma consapevoli che nella pratica si tratta di strumenti ben più evoluti, vale la pena elencare qualche specifica tecnica, alcune criticità e le possibili soluzioni con il rispetto delle garanzie processuali.

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:

– entrare nel sistema "target" e prende il completo controllo di tutte le funzioni inibendo l'antivirus e controllando anche la webcam, la navigazione e la posta elettronica (sia web mail sia della posta scaricata in locale es. outlook MS);

– è in grado di attivare i microfoni del sistema e ascoltare ciò che avviene nelle vicinanze del PC come una vera e propria intercettazione ambientale o comunque è in grado di intercettare eventuali comunicazioni telefoniche o telematiche effettuate con il sistema informatico (alcuni provvedimenti giudiziari, per questa attività, hanno già confermato e ritenuto correttamente necessario il decreto di intercettazione del Giudice per le indagini preliminari);

– è programmato per sfuggire agli antivirus in commercio;

– acquisisce e recapita on line all'investigatore, e quindi in tempo reale, tutto il contenuto del PC o dello smartphone (ogni tipo di file, log di navigazione web, posta elettronica, foto, dei siti web visitati);

-è in grado di fare gli screen shot ad intervalli di tempo regolari e predefiniti di tutto ciò che compare sullo schermo dell'apparato oggetto di "attacco".

– si può autodistruggere con un comando appositamente predisposto pulendo le sue tracce all'interno del PC ed è difficilissimo capire, ma soprattutto dimostrare successivamente, se e quando è stato istallato e soprattutto qual è stata la sua attività;

- può essere disattivato a distanza in qualsiasi momento e restare memorizzato per sempre all'interno dell'apparato;

– può uplodare ovvero inoculare e memorizzare nel sistema informatico "target" qualsiasi tipo di file salvandolo a piacimento in qualsiasi parte del sistema;

È chiaro che quest'ultima è un'operazione illecita che mai sarà svolta da una forza di polizia soprattutto se coordinata da una Procura della Repubblica; ma la domanda che possiamo e dobbiamo farci è se siamo sempre certi e sicuri che tali strumenti riescono ad essere sempre sotto il controllo dell'Autorità Giudiziaria.

L'inoculazione del trojan è una tecnica di "remote forensics" delegata troppo spesso soltanto a consulenti nominati ausiliari di polizia giudiziaria che operano però lontano da un controllo di quest'ultima e tantomeno da quello del pubblico ministero. Non si ravvisano obblighi di redigere puntuali annotazioni con menzione di tutti i particolari dell'operazione occulta, degli strumenti utilizzati nonché delle date e degli orari delle operazioni svolte.

Tutto ciò è molto più di un'intercettazione telefonica o telematica che, in quanto tale, necessita dell'ausilio dell'operatore telefonico e quindi di un terzo con conseguente tracciamento esterno delle 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 previsto dalle norme vigenti o dalla prassi.

2. 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[14]:

[14] *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 IIsfa, 2012, Forlì, Experta; Aterno, cit., Digital Forensics, in Aggiornamento - Digesto delle discipline penalistiche, 2013.*

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".

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 o *Inter-cloud ovvero tra più 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 decide 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.

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[15], 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"[16], 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 attravso 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.

---

[15] La difesa deve sapere cosa ha fatto o è in grado di fare il software introdotto nel sistema.

[16] 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".

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[17] che hanno portato ad una pronuncia delle Sezioni Unite che però solo in parte ha risolto il problema.

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.

---

[17] *Cass., 6 Sezione, n. 27100 del 26/5/2015, Musumeci, Rv. 265654.*

Come si ebbe già modo di dire diversi anni fa[18], 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:

– entrare nel sistema "*target*" e prende il completo controllo di tutte le funzioni inibendo l'antivirus e controllando anche la webcam, la navigazione e la posta elettronica (sia *web mail* sia di *outlook*);

– è in grado di attivare i microfoni del sistema e ascoltare ciò che avviene nelle vicinanze del PC come una vera e propria intercettazione ambientale o comunque è in grado di intercettare eventuali comunicazioni telefoniche o telematiche effettuate con il sistema informatico;

– è programmato per sfuggire agli antivirus in commercio;

– acquisisce e recapita *on line* all'investigatore, ad intervalli di tempo predefiniti a piacere e quindi in tempo reale, tutto il contenuto del PC (ogni tipo di *file*, log di navigazione web, posta elettronica, foto, *screnn shots* dei siti web visitati);

– si può autodistruggere con un comando appositamente predisposto pulendo le sue tracce all'interno del PC ed è difficilissimo capire ma soprattutto dimostrare successivamente se e quando è stato istallato e soprattutto qual è stata la sua attività;

– può "uplodare" ovvero inoculare e memorizzare nel sistema informatico "*target*" qualsiasi tipo di file salvandolo a piacimento in qualsiasi parte del sistema;

È chiaro che quest'ultima è un'operazione illecita che mai sarà svolta da una forza di polizia soprattutto se coordinata da una Procura della Repubblica ma possiamo ritenere che tali strumenti siano sempre sotto il controllo dell'Autorità Giudiziaria?

È una tecnica di "*remote forensics*" delegata troppo spesso soltanto a consulenti nominati ausiliari di polizia giudiziaria che operano però lontano da un controllo di quest'ultima e tantomeno da quello del pubblico ministero. Non si ravvisano obblighi di redigere puntuali annotazioni con menzione di tutti i particolari dell'operazione occulta, degli strumenti utilizzati nonché delle date e degli orari delle operazioni svolte.

Tutto ciò è molto più di un'intercettazione telefonica o telematica che, in quanto tale, necessita dell'ausilio dell'operatore telefonico e quindi di un terzo con conseguente

[18] *Aterno, cit., Digital Forensics, in Aggiornamento - Digesto delle discipline penalistiche, 2013.*

tracciamento esterno delle 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 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. E' 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.

E' 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 c.p.p.

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 ? E' 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[19] 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.

[19] *Che appunto non viene intercettato perché magari transita su canale cifrato.*

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[20], possono essere effettuati anche i cd 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;
- 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 telematica sui generis nei casi di screen shot di siti web, pagine relative a connessione su server di rete, 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 in presenza di quei flussi di dati e di informazioni

[20] *E' 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.*

(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- HD 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 invece 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.

E' abbastanza pacifico che rispetto ai dati informatici "statici" nel PCllo 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[21]. E' 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"[22] 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"[23] 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).

---

[21] 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.

[22] 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

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

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 un po' più di sforzo 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.

3. Il tema delle intercettazioni tra presenti con il captatore anche fuori dai casi di criminalità organizzata. La sentenza Scurato delle Sezioni Unite della Corte di Cassazione.

Rispetto alle intercettazioni tra presenti effettuate con il virus fuori dai casi di criminalità organizzata, la Suprema Corte non si è dilungata e non ha affrontato affatto l'argomento se non in modo indiretto e negativo quando ha affermato, all'inizio e alla fine della parte motiva (pag. 23) che 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, smartphone), anche nei luoghi di privata dimora ex art. 614 cod. pen., pur non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa, limitatamente ai procedimenti per delitti di criminalità organizzata.

Il passaggio della sentenza è chiaro ma il dibattito sul tema è aperto e interessante[24].

Le Sezioni Unite, risolvono la questione portata alla loro attenzione e nello stesso tempo sembrano indicare criteri utili per distinguere le intercettazioni ambientali mediante utilizzo del *trojan* in tutte le altre ipotesi, in due categorie:

1. intercettazione di comunicazioni tra presenti, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi rientranti nella previsione di cui all'art. 614 c.p. nei quali si stia svolgendo l'attività criminosa;
2. intercettazione di comunicazioni tra presenti, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi diversi da quelli *ex* art. 614 c.p.

Nel passaggio argomentativo con il quale le Sezioni Unite escludono "de iure condito - *la possibilità di intercettazioni nei luoghi indicati dall'art. 614 cod.pen. con il mezzo del captatore informatico*", si afferma che mancherebbe un adeguato controllo del Giudice al momento dell'autorizzazione e vi sarebbe l'esigenza di mitigare il rischio di una pluralità di intercettazioni tra presenti in luoghi di privata dimora.

Tale assunto porta però taluni[25] a ritenere pienamente legittime, quantomeno:

1.a l'intercettazione di comunicazioni tra presenti mediante utilizzo del *trojan*, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi rientranti nella previsione di cui all'art. 614 c.p. e nei quali si stia svolgendo l'attività criminosa, ove preventivamente indicati e motivati (in termini precisi) nella richiesta di intercettazione;

2.a l'intercettazione di comunicazioni tra presenti tramite utilizzo del *trojan*, in procedimenti diversi da quelli relativi a criminalità organizzata, in luoghi diversi da quelli *ex* art. 614 c.p., allo stesso modo preventivamente indicati in termini generici (luoghi pubblici e aperti al pubblico) nella richiesta di intercettazione.

In entrambi i casi sembrano infatti poter essere rispettati non solo i principi di garanzia sopra ricordati ma anche un criterio di logica e di coerenza vista la legittimità sempre riconosciuta delle "vecchie" intercettazioni tra presenti con microfoni direzionali o con microspie incorporate negli oggetti personali dell'indagato.

---

[24] Si veda tra i primi articoli a caldo, F. Cajani, Odissea del captatore informatico, in Cass. pen. 2016, in corso di pubblicazione.

[25] F. Cajani, cit.

La tecnologia, ormai da molti anni, consente di attivare da remoto il microfono di un dispositivo portatile preventivamente infettato da un *trojan* e sarebbe possibile richiedere al Giudice di autorizzare l'intercettazione di comunicazioni tra presenti in un luogo preventivamente indicato dal Pubblico Ministero nel quale (sia pure rientrante in uno di quelli *ex* art. 614 c.p.), si stia svolgendo l'attività criminosa. In questo caso non sarebbe impedito il controllo del Giudice al momento dell'autorizzazione, che pertanto non verrebbe disposta "al buio". Né si correrebbe il concreto rischio di dar vita ad una pluralità di intercettazioni tra presenti in luoghi di privata dimora, dal momento che tale luogo viene preventivamente indicato al Giudice ma è anche tecnicamente identificabile grazie al ricorso al cd. "*positioning*" o alla localizzazione effettuata dallo stesso *trojan* tramite il segnale GPS del dispositivo portatile.

Così, allo stesso modo, sarà possibile identificare anche il momento nel quale il dispositivo fuoriesca da tale ambito locale, al fine di terminare o attivare la captazione tramite attivazione/disattivazione del microfono.

In realtà è proprio l'uso di uno strumento invasivo e diabolico come il trojan che fa dire sostanzialmente alle Sezioni Unite che è utilizzabile solo in quei particolari limiti (criminalità organizzata e art. 13 dl. N. 152/1991) essendo le stesse Sezioni unite ben consapevoli che le intercettazioni tra presenti tradizionali continueranno ad essere usate come sempre si è fatto finora ma senza l'utilizzo del Trojan[26].

E' pur vero che tale tipologia di intercettazioni non erano propriamente oggetto del ricorso delle difese degli imputati, ma è un argomento che le motivazioni avrebbero dovuto affrontare più chiaramente ed in modo netto al fine di evitare una pericolosa situazione di incertezza su un tema.

C'è un altro punto che la sentenza avrebbe dovuto sviluppare meglio relativamente all'utilizzo del captatore informatico ovvero la necessità che tutte le operazioni, soprattutto quelle di inoculazione del software all'interno del dispositivo informatico (che ricordiamo, per consolidata giurisprudenza, è pur sempre equiparabile al domicilio informatico), vengano riportate in un verbale di operazioni di polizia giudiziari al fine di

[26] Si veda l'ottimo contributo di Luigi Giordano, *Dopo le sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo,* in Diritto penale contemporaneo*,* 2017.

responsabilizzare l'operatore che firmerà il verbale sulla particolare delicatezza di tutte le operazioni effettuate con il trojan.

Il problema della captazione da remoto de1 contenuto di un personal computer non ha avuto spazio nelle motivazioni delle Sezioni Unite. Non era certamente anch'esso oggetto di ricorso da parte delle difese ma visto che a pag. 8 la sentenza ha il merito di annoverare, tra gli altri, anche la capacità di perquisire l'hard disk in modo occulto e ripetuto nel tempo e di fare copia, totale o parziale, di tutte le unità di memoria del sistema informatico preso di mira nonché, aggiunge chi scrive, di modificare il contenuto stesso dell'apparato, sarebbe stato utile un *obiter dictum* sul punto.

Ad esclusione di tutto ciò che può essere captato all'interno del dispositivo con un decreto di intercettazione telematica grazie alla captazione dei flussi di corrispondenza (e non di memoria statica), tutto il resto è riconducibile si al sequestro o all'acquisizione di corrispondenza ma attraverso un'attività preventiva di perquisizione che deve trovare ragione e limite nelle norme previste dal codice di procedura penale e almeno in un decreto del pubblico ministero ex art. 247 o 256 c.p.p. Ecco su questo attendiamo la prossima sentenza degli eminentissimi giudici di cassazione.

L'apprezzato riferimento a questioni de iure condendo e a proposte di legge che in Parlamento suggeriscono uno strumento giuridico nuovo (controllo e acquisizione da remoto sottoposto ad autorizzazione periodica del Giudice) è un'indicazione importante che la Suprema Corte ha voluto dare ma siamo tutti consapevoli che il problema non si risolverà a breve considerati i tempi lunghi di approvazione.

Siamo di fronte a scenari ad oggi non immaginabili, il rischio di danni incalcolabili alla dignità e alla riservatezza degli indagati è molto alto e il prezzo non potrebbe che essere una restrizione che potrebbe danneggiare le indagini contro il terrorismo e la criminalità di stampo mafioso.

Senza voler fare la Cassandra ma basandosi solo sui fatti e sulla storia, è facile pensare che le vicende italiane di questi anni relative all'uso e alla diffusione delle intercettazioni che hanno violato la privacy degli indagati o dei cittadini saranno poca cosa rispetto ai rischi che si correranno con questo nuovo strumento.

4. Le ipostesi legislative sul tavolo

Come fu scritto,[27] al tempo in cui sembrava passare per buona senza forti opposizioni la tesi della cd prova "atipica" ex art. 189 cpp, si disse, nel quasi completo isolamento di quegli anni, che occorreva che intervenisse il Legislatore a disciplinare questo delicatissimo tema del captatore informatico. Dopo gli avvenimenti degli anni 2015 e 2016 che hanno coinvolto alcune società di informatica che si occupano di intercettazioni con l'utilizzo del trojan, e dopo un paio di sentenze della Suprema Corte di Cassazione (finalmente consapevoli, anche se in parte) che hanno puntualizzato alcuni principi per l'intercettazione tra presenti cd "itinerante" effettuata con il trojan,[28] è oggi imprescindibile una normativa specifica e puntuale che vada oltre la modifica del codice di rito e si occupi anche di produrre norme regolamentari che garantiscano tutte le parti (magistratura, difesa e forze di polizia) sull'uso corretto dei virus trojan inoculati nei sistemi telematici per finalità investigative di polizia giudiziaria. Qualcosa di concreto è stato fatto nell'estate del 2015 con l'inizio di un opera di studio e di proposta di legge seguita da un periodo di condivisione delle idee che ha portato al deposito della cd proposta Quintarelli.

4.1 La proposta cd Quintarelli

Per descrivere puntualmente l'articolato possiamo partire dall'art. 1 della proposta che introduce, con l'art. 254-ter c.p.p., un nuovo mezzo di ricerca della prova. Esso consente, in particolare di procedere all'osservazione delle attività realizzate con i dispositivi e all'acquisizione da remoto dei dati contenuti in un sistema informatico o telematico, diversi da quelli relativi al traffico. In ragione della pervasività del mezzo, il suo esperimento è subordinato a diverse condizioni. Prima di tutto, si prevede che l'utilizzo sia possibile solo qualora si proceda per i reati di criminalità organizzata,

---

[27] *Si veda appunto il riferimento fatto dall'Autore all'epoca sulla necessità di un intervento urgente del Legislatore, ATERNO, Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto, Memberbook IIsfa, 2012, Forlì, Experta., ATERNO, paragrafo 12 della voce Digital Forensics (Investigazioni informatiche), pag. 243, Aggiornamento, Digesto Discipline Penalistiche, 2013, Utet;*

[28] *Cass. VI, 26/5/2015, n. 27100 Musumeci, Rv. 265654; Cass. S.U. Ud. 8.4.2016, (dep. 1.7.2016), n. 26889, Scurato.*

limitatamente a quelle fattispecie che risultano talmente pervasive per cui non è possibile distinguere un ambito di attività o di vita personale estraneo all'associazione criminale, come sono quelli relativi al terrorismo ed alle associazioni mafiose. E' evidente che vi sono altre tipologie di reati molto gravi, che destano ribrezzo e sdegno sociale, per contrastare i quali l'utilizzo del captatore può offrire grandi possibilità, primo tra tutti la pedopornografia. Tuttavia trattasi di un punto di equilibrio con i diritti costituzionali di assai difficile individuazione; la definizione del perimetro di applicabilità è quindi un tema estremamente delicato. In questa proposta, oltre a definire con cura le garanzie delle parti e del procedimento, i proponenti hanno ritenuto opportuno limitare il perimetro dell'utilizzabilità, ai soli reati che attentano alla integrità dello Stato. Sarà una approfondita riflessione nel Parlamento, sede del processo democratico, a poter stabilire il perimetro di utilizzabilità più appropriato.

Proseguendo nell'esposizione dell'articolato, si prevede che il pubblico Ministero non possa disporre autonomamente la captazione, ma debba richiedere l'autorizzazione al giudice per le indagini preliminari. Infine, il giudice può concedere tale autorizzazione solo qualora vi siano gravi indizi di reato e qualora l'osservazione e l'acquisizione da remoto siano non meramente utili, ma assolutamente indispensabili per la prosecuzione delle indagini.

Attraverso il richiamo agli articoli 266-bis 1-quater e 1-quinquies e seguenti c.p.p., si dispone l'applicazione al nuovo mezzo di ricerca della prova di numerose norme che già disciplinano le intercettazioni informatiche e telematiche, in quanto compatibili (in particolare, in materia di durata ed esecuzione delle operazioni, ecc).

Tuttavia, a differenza che nelle intercettazioni informatiche, l'esecuzione materiale delle operazioni è demandata alla sola polizia giudiziaria, senza la possibilità di avvalersi di ausiliari esterni. Tale previsione è fondamentale per circoscrivere l'ambito di utilizzo dello strumento investigativo e dei relativi atti di indagine, anche in considerazione dell'impossibilità per le forze di polizia e per la magistratura di verificare l'attività di un tale soggetto (non ufficiale di polizia giudiziaria ma mero tecnico informatico) che opera distante dai loro occhi e dai loro uffici e spesso per mezzo di apparati telematici non verificabili e in *cloud*. Il decreto che dispone l'osservazione e l'acquisizione da remoto

deve essere notificato alle parti, nonché agli eventuali proprietari e utilizzatori del dispositivo bersaglio, entro 40 giorni. Tale termine può essere motivatamente prorogato dal giudice, su richiesta del PM, per ulteriori periodi di 40 giorni, fino al massimo di 12 mesi, in ragione della complessità dell'indagine, qualora dalla notifica possa derivare un grave pregiudizio alle indagini.

L'art. 2 interviene sull'art. 266-bis c.p.p., disciplinando espressamente, con quattro nuovi commi, l'uso dei captatori al fine di intercettare comunicazioni o conversazioni, anche tra presenti. Tale modalità di intercettazione è consentita solo in riferimento ai delitti indicati nel nuovo articolo 254-ter comma 1. La previsione di un tale limite si pone in continuità con quanto stabilito nella sentenza n.26889/2016, sopra citata, con la quale la Cassazione ha ritenuto possibile procedere all'intercettazione di conversazioni o comunicazioni tra presenti mediante captatore informatico, anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati ed anche se ivi non si stia svolgendo l'attività criminosa, solo in relazione a delitti di criminalità organizzata. Con una nuova disposizione di garanzia, il comma 1-quater stabilisce che, quando l'effettiva natura dell'organizzazione criminale non presenti connotati di pervasività tali da poter ostacolare una separazione tra attività illecita e ordinaria vita privata, il giudice può negare o revocare l'autorizzazione. Il successivo comma vieta un uso dello strumento tale da violare la dignità umana e prescrive che, nel limite del possibile, l'intercettazione avvenga nel rispetto del pudore e della riservatezza della sfera privata di chi vi è sottoposto. Con questa previsione si intende ribadire che la captazione da remoto di conversazioni, un potente e talvolta insostituibile strumento di indagine, non può svolgersi con modalità tali da sacrificare il principio personalista, pietra angolare del nostro ordinamento costituzionale, il cui rispetto deve prevalere sullo stesso interesse pubblico alla repressione dei reati.

L'art. 3 della proposta, introduttivo di un nuovo art. 266-ter c.p.p., prevede anche la possibilità di attivare, per il tramite del captatore, le funzioni di acquisizione della posizione geografica del dispositivo.

L'art. 4, oltre ad alcune modifiche di coordinamento, prevede che le operazioni di cui all'art. 266-bis, commi 1-bis e 1-ter c.p.p. possano essere autorizzate solo quando ogni

altro mezzo di ricerca della prova risulti inadeguato. Vista l'estrema invasività dello strumento, si è optato per limitarne l'uso, come *extrema ratio*. Sia la richiesta del PM, sia il provvedimento del giudice, dovranno quindi essere motivate sul punto.

L'art. 5 introduce l'art 268-bis c.p.p., con il quale si prevedono ulteriori garanzie per lo svolgimento mediante programmi e strumenti informatici delle attività di cui agli art. 268-bis e 268-ter c.p.p.. Primariamente, gli strumenti e programmi utilizzati devono assicurare che i dati presenti sul dispositivo non vengano alterati o modificati e che i dati acquisiti siano conformi a quelli originali presenti sul dispositivo medesimo. Ugualmente, anche per la conservazione dei dati (una copia dei quali deve essere conservata negli uffici o impianti della Procura) deve essere garantita l'integrità, la genuinità e l'immodificabilità. Tali disposizioni risultano fondamentali alla luce delle potenzialità tecniche degli strumenti di osservazione e acquisizione dati da remoto, che possono non solo acquisire da remoto dati e programmi installati sul dispositivo bersaglio, ma anche modificarli e addirittura introdurli ex novo nel dispositivo stesso. In assenza di idonee garanzie di genuinità del dato, il captatore potrebbe infatti essere addirittura utilizzato per introdurre elementi incriminanti (per esempio, foto pedopornografiche) su un dispositivo all'insaputa del suo utilizzatore. Si prevede poi che il giudice, nel proprio decreto,individui i singoli dispositivi oggetto di captazione. In tal modo, si vuole evitare che il decreto diventi un'autorizzazione "in bianco" al PM, tale da consentirgli un controllo sproporzionato sulla vita del soggetto, operato attraverso la captazione di un numero potenzialmente indeterminato di dispositivi. Sempre nell'ottica di garantire la genuinità dell'operazione di captazione, il comma 5 stabilisce penetranti obblighi di documentazione della stessa, anche in relazione ai soggetti che vi prendono parte e ai programmi che vengono impiegati. Al termine delle operazioni il captatore deve essere rimosso dal dispositivo e di tale operazione viene redatto verbale; in caso di impossibilità di rimozione, devono essere fornite all'utente le istruzioni per provvedervi autonomamente. Il comma 8 prevede poi che i captatori debbano possedere i requisiti da stabilirsi con apposito regolamento del Ministro della Giustizia, emanato di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali.

L’art. 6 aggiunge un nuovo articolo 89-bis al D.Lgs n. 271/1989 (norme di attuazione, di coordinamento e transitorie del codice di procedura penale), indicando i contenuti necessari del futuro decreto sui captatori previsto dal citato art. 5, comma 8, del quale si prescrive l’aggiornamento almeno ogni tre anni. In particolare, i requisiti tecnici individuati dal decreto dovranno assicurare che l’installazione e l’attività dei captatori non alteri i dati acquisiti, né le restanti funzioni del dispositivo.

Sempre al fine di fornire un valido contrappeso all’utilizzo di questo potente e invasivo strumento investigativo, si individuano dei criteri direttivi ai quali i Ministeri competenti devono conformarsi nell’emanazione del decreto, così da garantire:

- l'istituzione di un sistema di omologazione dei captatori, affidato all’Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM);
- il diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dalla lo installazione fino alla loro rimozione, e di verificare tecnicamente che i captatori in uso siano certificati, fino a consentire l’ispezione del codice sorgente - previamente depositato presso un ente da determinarsi - e gli accertamenti tecnici informatici volti a verificare l’assenza di manipolazioni;
- la possibilità per la difesa, con tutte le garanzie del caso e gli obblighi di riservatezza e segreto, di verificare gratuitamente la presenza del captatore utilizzato in un registro nazionale dei captatori, gestito dall’ente di omologazione;
- la registrazione di tutte le operazioni svolte dal captatore, dalla sua installazione fino alla sua rimozione, poi messe integralmente a disposizione delle parti come allegato del fascicolo;
- che il captatore non determini un abbassamento del livello di sicurezza del sistema o del dispositivo su cui viene utilizzato;
- la disinstallazione dei programmi al termine dell’uso autorizzato, anche fornendo all’utente le informazioni necessarie a provvedervi autonomamente in alcuni casi;

- l'obbligo per i produttori di fornire pubblicamente e gratuitamente gli strumenti software necessari per l'analisi dell'allegato al fascicolo contenente la registrazione delle operazioni;
- la possibilità per le parti di richiedere ed eseguire in modo indipendente la verifica del processo di omologazione.

L'art. 7 modifica invece il preesistente art. 226 disp att. su intercettazioni e controlli preventivi sulle comunicazioni, al fine di adeguarne il contenuto all'introduzione dell'art. 254-ter e alle modifiche all'art. 266-bis c.p.p.

L'art. 8 prescrive che gli articoli da 1 a 7 della nuova normativa trovi applicazione alle attività di indagine avviate o proseguite dopo 90 giorni dalla pubblicazione in Gazzetta Ufficiale del decreto ministeriale sugli strumenti di osservazione e acquisizione da remoto.

L'art. 9 prevede un aumento delle pene qualora strumenti di osservazione e acquisizione da remoto vengano usati per scopi criminali cagionando danni alla sicurezza nazionale e alle infrastrutture critiche del Paese o qualora l'intrusione informatica avvenga al fine di trattare illecitamente dati personali sensibili o giudiziari, o comunque se a seguito dell'intrusione informatica tali dati vengono diffusi illecitamente.

Tra la fine del 2016 e i primi mesi del 2017 numerose organizzazioni internazionali a tutela dei diritti della privacy si sono interessate ai lavori parlamentari italiani e alle norme in discussione in tema di trojan di Stato. Tra queste, AccessNow[29], che è una associazione non governativa impegnata nella tutela dei diritti digitali con sede a Bruxelles, ha effettuato una analisi della proposta di legge cd. "Quintarelli" e, se da un lato ha apprezzato gli aspetti innovativi e di completezza dell'impianto regolatorio dall'altro lato ha ravvisato le seguenti aree di miglioramento:

- trasparenza e rendicontabilità dell'uso dei Captatori;
- introdurre chiare regole di rendicontabilità nell'utilizzo del captatore per favorire, tramite una misura di trasparenza pari ai "Transparency Report" degli operatori telefonici internazionali, un controllo diffuso relativo all'impiego di questo strumento di investigazione;

[29] https://www.accessnow.org/

- operatività e regolamentazione nell'uso dei captatori all'estero ovvero su soggetti che si trovano su suolo estero e sono sottoposti a indagini da parte delle autorità italiane.

AccessNow riscontra che nella proposta di legge Quintarelli sarebbe opportuno inserire un divieto esplicito di operatività nell'uso dei captatori quando il dispositivo elettronico oggetto di inoculazione si trovi all'estero, limitando il cosi detto "*extraterritorial hacking*", cioè lo sconfinamento dell'operatività delle forze dell'ordine all'estero.

Ad avviso di chi scrive il tema è di grande importanza ma deve essere tenuto distinto dai casi in cui vi sono soggetti sotto indagine nel territorio italiano che si recano all'estero. Qui entrano in gioco normative di cooperazione e trattati internazionali che già prevedono alcune tutele certamente migliorabili.

Il caso diverso invece di inoculazione su un soggetto all'estero mai entrato nel nostro paese è, al di là di riferimenti impropri alla tecnica dell'instradamento delle intercettazioni, un tema importante, delicato e complesso. Per queste ragioni, ad avviso di chi scrive, appare più appropriato affrontarlo in ambito europeo ed internazionale attraverso una direttiva o una convenzione che vincoli agli stati membri firmatari ad una disciplina comune che non pregiudichi le esigenze di sicurezza sovranazionale antiterrorismo e al contempo non limiti il diritto di difesa e prevenga possibili abusi e violazioni della riservatezza dei cittadini stranieri[30].

4.2 L'art. 84 lett. e) del DDL Orlando recante modifiche al Codice di procedura penale

In altro modo e sotto altre forme, oggi il Parlamento, proprio mentre si scrive, sta cercando di trovare un punto di incontro sostanzialmente diverso sul tema captatore; lo sta facendo con la votazione adesso passata alla Camera dei Deputati), tra gli altri articoli, dell'art. 84 del DDL cd Orlando (recante modifiche al Codice di procedura penale. Vedremo se e quando sarà approvato quale sarà il testo definitivo, ma non possiamo non

[30] L'analisi AccessNow della PdL cd Quintarelli è stata pubblicata all'indirizzo http://www.civicieinnovatori.it/wp-content/uploads/2017/04/Access-Now-Comment-Disciplina-dell%E2%80%99uso-dei-captatori-legali.pdf

segnalare che questa norma prevede un utilizzo del captatore nella mera modalità intercettazione tra presenti anche se, differentemente dalla proposta Quintarelli, per qualsiasi categoria di reato. Il richiamo ai reati di cui all'art. 51 comma 3 bis e 3 quinques del codice di rito è relativo soltanto alle ipotesi in cui il pubblico ministero il potere di disporre d'urgenza l'inoculazione del trojan ed entro le successive 48 ore di farsi autorizzare dal giudice per le indagini preliminari. Ma resta fermo il disposto complessivo dell'articolo 84 lett. e) in base al quale, attraverso il meccanismo dell'attivazione e disattivazione del microfono dell'apparato si otterrebbe il rispetto dei principi affermati dalla Corte di Cassazione a Sezioni Unite del 2016 (Scurato) nei casi in cui si capti l'audio all'interno di un domicilio privato oppure all'esterno e salvi i casi in cui si proceda per reati associativi di stampo mafioso o di criminalità organizzata in genere. A proposito dell'attivazione e disattivazione del microfono è di vitale importanza il richiamo che l'art. 84 lett. e) fa al regolamento ministeriale con il quale si dovranno stabilire i requisiti tecnici di conformità del programma informatico utilizzabile.

Da criticare è il richiamo alla possibilità di ricorrere a società private nominate ausiliari di polizia giudiziaria e l'assenza di normativa chiara in tema di cristallizzazione e genuinità dell'attività del trojan da una parte e dei dati acquisiti dall'altra. Ci si augura che in fase di discussione nell'aula della Camera dei deputati almeno questo aspetto, tanto caro a chi scrive, venga chiarito e risolto.

E' di tutta evidenza che resta escluso, perché non previsto dalla norma, la captazione da remoto del contenuto del PC o dello smartphone.

In conclusione, appare evidente che permane l'esigenza di soluzioni tecniche e strumenti giuridici nuovi[31] sia per controllare e limitare eventuali abusi sia per consentirne un utilizzo puntualmente disciplinato nel rispetto di tutte le garanzie, soprattutto di quelle difensive.

Sappiamo bene che qualsiasi norma che il Parlamento approverà potrebbe non bastare e non essere sufficiente. Ma come in ogni tema delicato che investe la limitazione e il

---

[31] Si fa presente che ormai una proposta di legge cd Quintarelli sul captatore è ferma da quasi un anno in Commissione Giustizia e un'altra è stata presentata dal medesimo deputato (a firma di numerosi altri colleghi del gruppo Civici innovatori il 31 gennaio 2017 sempre in Commissione Giustizia. Altra norma sul trojan è presente nell'art. 84 sul DDL cd Orlando di riforma del codice di procedura penale.

controllo di diritti fondamentali della persona, occorrerà anche in questo caso, più di ogni altra cosa, una ricerca continua di trasparenza, un' altissimo senso di responsabilità dei ruoli da parte degli "addetti ai lavori" e, in generale, cosa molto importante per il futuro tecnologico della nostra società globale, la ricerca di nuovi valori e di un senso etico della tecnologia[32] e del suo utilizzo.

Roma febbraio/maggio 2017

Stefano Aterno

Avvocato

www.studioaterno.it

[32] *Giovanni Buttarelli: la privacy dei prossimi vent'anni, intervista del 8 maggio 2017, www.interlex.it/forum20/buttarelli_interv.html*