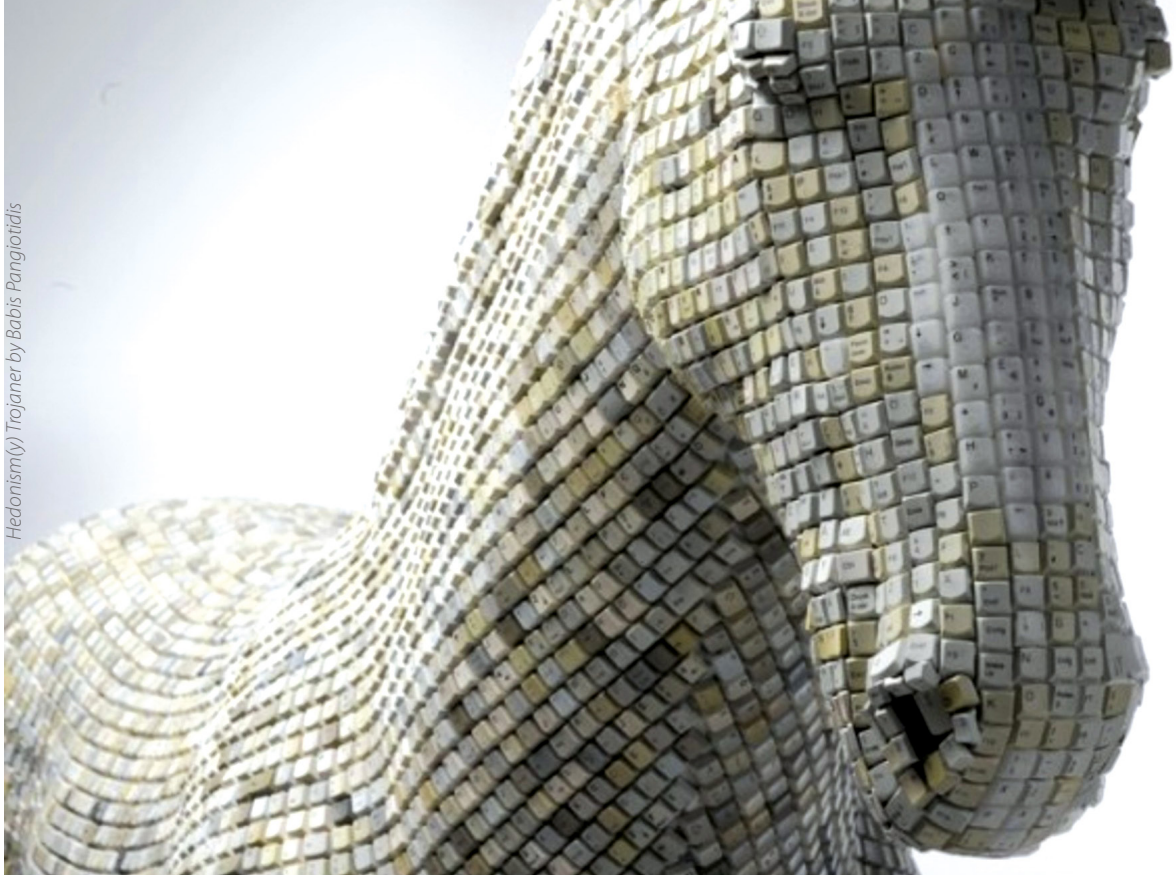


Hedonism(y) Trojaner by Babis Pangiotidis

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 (in questo numero): 1. Prmessa, 2. I tecnicismi del Trojan e l'approccio non sempre corretto della Corte di Cassazione.
Seconda parte (nel prossimo 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 (I 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.

1. Premessa

La criminalità utilizza strumenti informatici (*hardware* e *software*) in grado di far perdere le tracce dei delitti commessi e di cifrare i contenuti delle comunicazioni. Le forze dell'ordine rincorrono da sempre con grande difficoltà, cercando di affinare le tecniche investigative avvalendosi anch'esse delle nuove tecnologie. Tutto ciò avviene orami da troppo tempo in assenza di norme giuridiche di riferimento chiare e precise: è il caso del trojan chiamato anche captatore informatico[1] da molto tempo utilizzato ma solo recentemente oggetto di pronunce giurisprudenziali e tentativi di soluzioni normative.

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

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.

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,

2. 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 (Virruso) che trae origine da alcune indagini per associazione a delinquere di stampo mafioso nelle quali fu utilizzato 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* in via di elaborazione, 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 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 pose 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 criticata4 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 Server 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, Skype[6], ecc.) ma ove vi fossero state non vi sarebbero stati dubbi sull'applicabilità delle garanzie dell'art. 266 bis c.p.p.

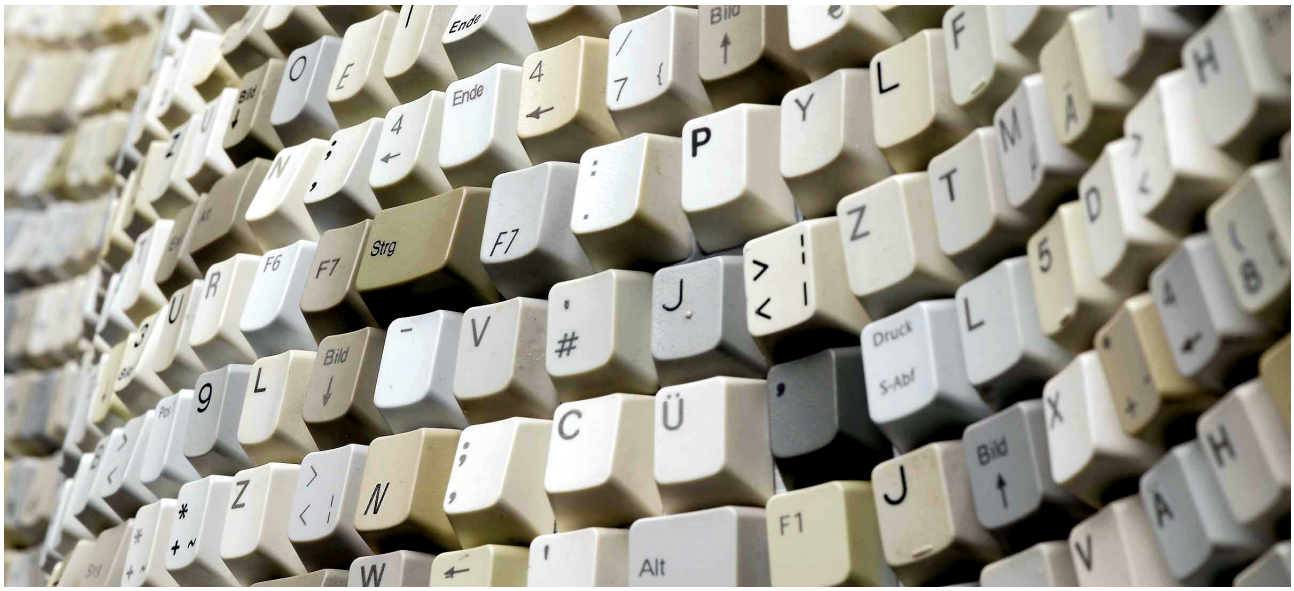
Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto, Memberbook Ilsfa, 2012, Forlì, Experta; Cass. Cass. VI, 26/5/2015, n. 27100 Musumeci, Rv. 265654; Cass. S.U. Ud. 8.4.2016, (dep. 1.7.2016), n. 26889, Scurato.

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".

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 Ilsfa, 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.

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



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 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*

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.

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

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 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 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 al momento dell'inoculazione;
- 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].
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 webmail 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 (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 *online* 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 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: siamo sicuri che su tali strumenti l'Autorità Giudiziaria riesce ad esercitare un controllo efficace?

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 dal 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 ma non è un buon motivo per non cominciare a ragionare diversamente.
Tutto ciò è molto più di un'intercettazione telefonica o telematica classica che, in quanto tale, necessita dell'ausilio dell'operatore telefonico e quindi di un terzo con il conseguente tracciamento esterno delle operazioni. Con il trojan 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. ©

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.