Captatore informatico e regolamento tecnico: quid juris per la modalità "screen shot" ?

di Stefano Aterno

Si è perso molto tempo e oggi si arriva tardi a tentare di disciplinare l'utilizzo del Trojan per finalità di accertamento e repressione dei reati. Le soluzioni adottate scontentano tutti. Cerchiamo di capire se nella normativa post-decreto un equilibrio tra diritto di difesa ed esigenze investigative sarà possibile.

E' dal 2010 che, con la sentenza della Cassazione Virruso[1] è venuto alla luce questo mezzo molto invasivo che riduce le intercettazioni ambientali con le vecchie microspie a mezzi obsoleti e neanche lontanamente paragonabili alla grande potenzialità lesiva del captatore. Se andiamo a osservare da vicino le indagini descritte nella sentenza Virruso esse si sono svolte a Palermo nel 2004 grazie ad un software che possiamo definire il "padre" degli attuali captatatori ovvero ad un *malware* chiamato *Back Orifice* (il "nonno" si chiamava *Classer*). Sono passati quindi ben 13 anni dal primo uso noto di un trojan per attività investigativa.Un silenzio eccessivo e a tratti assordante che sta finendo anche per pregiudicare le potenzialità applicative del software in ambito giudiziario.

Occorreva legiferare sullo strumento prima, in un modo più sereno e organico prevedendo da un lato sin da subito nuovi mezzi di ricerca della prova, l'utilizzo di tutte o quasi tutte le funzionalità del software (a vantaggio delle indagini) e dall'altro lato garantendo con norme coraggiose poteri di impugnazione e di verifica difensiva ex post della difesa. Peccato, perché la proposta cd Quintarelli (sia la prima del febbraio 2016 sia la seconda del marzo 2017) aveva delineato una soluzione equilibrata proprio basata su questi criteri ma al di là di qualche contributo transitato nel decreto in approvazione la proposta si è arenata davanti agli opposti estremismi senza che nessuno riuscisse a farne una sintesi.

[1] ATERNO, paragrafo 12 della voce Digital Forensics (Investigazioni informatiche), pag. 243, Aggiornamento, Digesto Discipline Penalistiche, 2013, Utet

La proposta è ancora in commissione parlamentare in attesa di calendarizzazione ma evidentemente è talmente equilibrata che scontenta tutte le parti in gioco ma, guardando l'interesse collettivo ha indubbiamente un valore aggiunto.

Perché stiamo arrivando tardi ? Perché la Cassazione a Sezioni Unite Scurato del 2016, come ormai troppo spesso accade, è arrivata prima del Legislatore e, seppur rimarcando in generale la grande invasività dello strumento investigativo si è pronunciata solo su una parte delle attività potenziali dello strumento e tra l'altro sull'intercettazione tra presenti (a mezzo trojan) in un processo relativo al reato di cui all'art. 416 bis c.p. (associazione di stampo mafioso) per il quale, per giurisprudenza pacifica, non vi era alcun dubbio sull'applicazione dell'art. 13 della legge n. 152 del 1991 in virtù del quale non è necessario provare che nel luogo domiciliare sotto intercettazione si sta commettendo l'azione delittuosa. Pertanto anche le intercettazioni cd "itineranti" (che quindi ben possono riguardate più luoghi domiciliari tutelati) effettuate in virtù di istallazioni su smartphone e Ipad non rappresentano un grosso problema se i decreti autorizzativi indicano correttamente l'uso dello strumento e la modalità della captazione della voce tra presenti.

Le Sezioni Unite cd Scurato del 2016 non si occupano in realtà delle modalità più invasive del captatore, e comunque non avrebbero potuto, visto il contenuto dei ricorsi proposti.

Le recenti sentenze della Cassazione (Romeo e Occhionero del luglio e del settembre 2017) dimostrano che tutt'ora vengono utilizzate funzioni del trojan non disciplinate dal codice di procedura penale e che solo in parte, rientrando in mezzi di ricerca della prova tipici o comunque disciplinati e ammessi in giurisprudenza, si arriva a utilizzare degli elementi di prova raccolti.

Mi riferisco in particolar modo all'acquisizione di parte del contenuto del sistema informatico o di ciò che entra e esce da esso attraverso la funzione "screen Shot" del captatore soprattutto per quanto riguarda i comportamenti comunicativi le cui tracce sono presenti all'interno dello smartphone[2] o la captazione tramite screen shot di dati che

[2] Si veda quando già indicato da questo Autore in, http://www.dirittopenaleinformatica.it/wp-content/uploads/2017/02/ATERNO_Il-TROJAN-dalla-A-alla-Z.pdf (febbraio 2017) e in Il trojan dalla A alla Z, in Sicurezza e Giustizia, Settembre 2017,

viaggiano in Rete, che vengono in prima battuta acquisiti con intercettazioni telematiche tradizionali ma essendo cifrati sono impossibili da leggere e da decifrare[3].

Il trojan è un po' come i coltellini multi- uso, ha molteplici applicazioni e tante modalità di funzionamento. Non è però possibile ricondurre tutto dentro l'alveo delle intercettazioni ambientali e/o telematiche. Qui, per ragioni di spazio ci occupiamo degli screen shot perché allo stato appare lo strumento più utile a livello investigativo e sotto il profilo giuridico il meno esplorato. L'assenza di una chiara disciplina per l'utilizzo completo di ogni tipo di screen shot effettuato con il trojan è la dimostrazione che occorre riprendere la strada verso una normativa seria e completa sul trojan per uso investigativo. Con questa modalità "screen shot"si acquisisce ciò che appare sullo schermo dello smartphone o di un personal computer nel momento in cui l'utente utilizza lo strumento informatico. Con delle vere e proprie fotografie dello schermo effettuate dal software posto all'interno dello smartphone/pc, il malware acquisisce o può comunque acquisire le informazioni piu' svariate sia contenuti comunicativi sia contenuti non comunicativi. Non si tratta di intercettazione ambientale con l'uso del microfono, non si tratta di captare da remoto tutti i files e contenuti del supporto[4] ma soltanto fare una" foto" di ciò che appare a video. A discrezione dell'operatore, ogni tot secondi/minuti/ore (è possibile quindi anche variare il tempo) si può impostare uno screen shot che riprende l'attività che appare sullo schermo. Pensiamo alla rubrica, alla navigazione web[5], al contenuto di una email scritta o letta, ad un documento. Se la cadenza degli screen shot è frequente potrebbe captare anche una conversazione via chat in tempo reale, ovvero in corso tra due soggetti che si stanno scrivendo via chat. Cosa sono i messaggi tra due o piu' soggetti che appaiono nella chat di uno smartphone (es. What's app)? Sono molto simili ad una conversazione tra presenti in un domicilio informatico/telematico? E' forse molto diverso? Non è assolutamente difficile sostenere che siano esattamente la stessa cosa e ciò pone alcuni problemi proprio per l'invasività del trojan inoculato nello smartphone.

---

[3] [3] Si veda quando già indicato da questo Autore in, http://www.dirittopenaleinformatica.it/wp-content/uploads/2017/02/ATERNO_Il-TROJAN-dalla-A-alla-Z.pdf

[4] Questo lo possono fare altre funzionalità del trojan opportunamente predisposte.

[5] Su questo si veda www.dirittopenaleinformatica.it

Se con lo screen shot si riesce a captare una conversazione via chat tra due soggetti in tempo reale ovvero in corso di svolgimento (non tecnicamente detta anche sincrona) che differenza c'è con una telecamera o una macchina fotografica che riprende il contenuto comunicativo (qualsiasi) di un soggetto che dialoga o che scrive con un altro soggetto situato anche fuori dal luogo in cui è ripreso ?[6] Con la pronuncia della Corte Costituzionale del 2002, n. 135 si stabilì proprio l'utilizzabilità in via interpretativa delle riprese visive di messaggi gestuali e altri comportamenti comunicativi alla *disciplina della intercettazione ambientale in luoghi di privata dimora.* Non ci sono differenze con questo principio sancito dalla Corte costituzionale del 2002[7] e tale assunto ben potrebbe essere domani utilizzato

[6] Si pensi a linguaggi gestuali o fogli e altro genere di scritti sotto la porta ma ripresi da telecamere occultate nella stanza.

[7] 7

La **Corte costituzionale**, con la sentenza, **24 aprile 2002, n. 135**, affrontando il tema della mancata omologazione, sul versante normativo, delle riprese videofilmate alle intercettazioni di comunicazioni fra presenti, ha dichiarato infondata la questione di legittimità costituzionale degli artt 189. e 266-271 cpp, sollevata in riferimento agli artt. 3 e 14 Cost. nella parte in cui non estendono la disciplina delle intercettazioni delle comunicazioni tra presenti nei luoghi indicati dall'art. 614 c.p., alle riprese visive o videoregistrazioni effettuate nei medesimi luoghi. Ha, in particolare, rilevato che le riprese in luoghi di privata dimora ben possono configurarsi come una forma di intercettazione di comunicazioni tra presenti che si differenzia da quella operata tramite gli apparati di captazione sonora solo in rapporto allo strumento tecnico di intervento, come nella ipotesi di riprese visive di messaggi gestuali. Ed ha concluso che, per tale fattispecie, *già ora è applicabile in via interpretativa la disciplina della intercettazione ambientale in luoghi di privata dimora.* Ove si fuoriesca dalla ipotesi della videoregistrazione di comportamenti di tipo comunicativo, venendo in considerazione soltanto la *intrusione nel domicilio in quanto tale*, è in gioco la sfera della libertà domiciliare che è bene diverso dalla libertà e segretezza delle comunicazioni e **richiede una disciplina normativa**, nel rispetto delle garanzie costituzionali dell'art. 14 Cost: disciplina che tuttavia non può discendere da una pronuncia additiva della Corte costituzionale. La Corte di cassazione (Cass., Sez. I, 29 gennaio 2003, n. 16965, Augugliaro ed altro, rv 224240)ha recepito i principi espressi dalla Corte costituzionale, affermando che sono utilizzabili i risultati delle video-registrazioni effettuate con videocamera all'interno di un0abitazione privata, in quanto esse sono previste dal vigente codice di rito, il quale, autorizzando, *ex* art. 266, comma 2,cpp, l'intercettazione delle comunicazioni -e non delle sole conversazioni tra presenti- comprende, nel proprio ambito previsionale, non solo la comunicazione convenzionale mediante l'uso del linguaggio, ma anche quella gestuale, mentre non regola, con conseguente inutilizzabilità processuale, ogni altra captazione di immagini non avente natura di messaggio intenzionalmente trasmesso da un soggetto ad un altro. Tale regolamentazione delle intercettazioni delle comunicazioni tra presenti, anche effettuate mediante video-registrazioni, non contrasta con gli articoli 14 e 15 Cost. e 8 Conv. eur. dei diritti dell'uomo, i quali stabiliscono che i diritti all'inviolabilità del domicilio e la segretezza di ogni forma di comunicazione possono essere limitati, per atto motivato dell'autorità giudiziaria, al fine di salvaguardare la sicurezza nazionale nonché l'ordine e la prevenzione dei reati.

Le oscillazioni giurisprudenziali sull'argomento appaiono essere state risolte dall'intervento della Corte di Cassazione SS. UU. (Sent. 28.3. 2006, n. 26795 –Prisco) che si è occupata della problematica delle videoregistrazioni, che ha preso le mosse dalla sentenza della Corte costituzionale n. 125 del 2002, secondo cui è necessario, ai fini del superamento della garanzia della inviolabilità del domicilio, non solo di un provvedimento motivato dell'autorità giudiziaria, ma anche di una compiuta disciplina legislativa delle ipotesi e delle modalità di limitazione della garanzia costituzionale; si può sostenere la riconducibilità

dalla giurisprudenza per legittimare di questi elementi di prova. Sono questi oggi gli argomenti sui quali vale la pena di discutere anche perché a fronte di una motivazione della Corte di Cassazione con queste argomentazioni ben poco spazio rimarrebbe al diritto di difesa.

Il decreto in fase di elaborazione presso il Ministero di Giustizia non disciplinerà queste modalità anche perché il Legislatore non ha ritenuto di indicarle nella delega. Inoltre il decreto reca anche un altro errore o una precisa volontà del legislatore : l'intercettazione tra presenti con il captatore può essere effettuata soltanto su "dispositivi elettronici portatili", e i personal computer fissi ? Di questo magari ci occuperemo in un altro momento.

C'è un punto importante nella delega e nel decreto che rappresenta il vero strumento di garanzia per tutte le parti e non solo per la difesa: il regolamento tecnico. Su questo punto spero che nessuno sia disposto a privare il sistema delle garanzie necessarie.

Il richiamo a tale regolamento è presente nell'art. 7 dello schema di decreto legislativo recante "disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82,83 e 84, lettere a)b)c) e d) della legge 23 giugno 2017, n. 103.

In sede di Commissione giustizia del Senato il richiamo al regolamento fu inserito con il cd emendamento Casson – Cucca fin dal giugno del 2016 e lo spunto venne preso proprio dalla proposta cd Quintarelli già depositata e ritenuto dal relatore e dalla commissione un punto fondamentale e molto importante.

Con decreto del Ministro della Giustizia, da emanare entro trenta giorni dalla data di entrata in vigore del decreto legislativo, saranno stabiliti i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante inserimento di captatore informatico su dispositivo elettronico portatile. I requisiti tecnici saranno stabiliti secondo misure idonee di affidabilità, sicurezza ed efficacia al fine di garantire che i

---

della sola captazione visiva di comportamenti di tipo comunicativo in luoghi di privata dimora alla disciplina delle intercettazioni di comunicazioni fra presenti, restando però impregiudicata la questione di costituzionalità delle ipotesi di videoregistrazione di immagini che non abbiano tale carattere; la necessità di una regolamentazione legislativa, in conformità dell'art. 14 Cost., nel caso di intrusione del domicilio con riprese visive non finalizzate alla intercettazione di comunicazioni.

programmi informatici siano correttamente utilizzabili. Il regolamento sarà destinato a regolare l'imprescindibile attività di monitoraggio delle postazioni che controlleranno da remoto o trojan e i file di log relativi dovranno garantire anche che i programmi informatici si limitino ad effettuare solo e soltanto le operazioni autorizzate.
Si tratta sostanzialmente di una azione di tracciamento cd *logging* di tutta l'attività che 24 ore su 24 svolge il client "attaccante" (personal computer delle forze dell'ordine che fa funzionare il trojan inoculato sull' obiettivo). L*'hashing* ormai viene effettuato di default dai software - trojan di ultima generazione su tutti i file esfiltrati ma a fronte di usi più "spinti", al fine di aumentare le garanzie difensive, sarebbe opportuno che venga apposta automaticamente una firma digitale e una marcatura temporale sia ai log di registro, sia ai file prodotti dal sistema nonchè ai file relativi all'acquisizione. E' di tutta evidenza che garantire la verificabilità ex post dei file acquisiti dal captatore nel momento in cui vengono acquisiti dall'interno del sistema (in copia) e la conseguente sicurezza che non è stato possibile per nessuno modificarli rappresenta la garanzia minima che una legge cosi invasiva per i diritti e le libertà dei cittadini deve avere. E' infatti evidente che la verifica ex post sullo smartphone dell'indagato in un momento successivo al sequestro potrebbe non essere più possibile per la cancellazione precedente del file da parte dell'indagato stesso o a causa di un evento accidentale.

Concludendo, 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. Occorrerà il captatore non determini un abbassamento del livello di sicurezza del sistema o del dispositivo su cui viene utilizzato, che venga assicurata in qualche modo la disinstallazione dei programmi al termine dell'uso autorizzato o al termine delle indagini, anche fornendo all'utente le informazioni necessarie a provvedervi in alcuni casi autonomamente. Sarà necessario anche prevedere nel regolamento l'obbligo per i produttori di captatori di fornire pubblicamente e gratuitamente gli strumenti software necessari per l'analisi dei report contenenti la registrazione delle operazioni.
L'importanza di questo regolamento tecnico (art. 7 dello schema di decreto) è fondamentale e centrale per l'intera struttura delle garanzie di difesa e per l'affidabilità

stessa del sistema investigativo e delle prove raccolte. L'augurio è che ciò sia percepito allo stesso modo dal Legislatore e da chi al ministero in questi giorni si sta apprestando a scriverlo.

Stefano Aterno
1 dicembre 2017