Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica martedi 4 febbraio 2020 in relazione alla conversione in legge del decreto-legge 30 dicembre 2019, n.161, e in particolare per la materia delle intercettazioni attraverso sistemi di captazione informatica

Prof. Avv. Stefano Aterno

Gentilissimo Presidente,
invio per suo tramite anche agli altri onorevoli componenti della Commissione questi appunti relativi alla mia audizione avvenuta il 4 febbraio scorso.

Il disposto normativo relativo alla Conversione in legge del decreto-legge 30 dicembre 2019, n.161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni rischia di essere già vecchio prima ancora di essere approvato e sarebbe opportuno valutare l'inserimento di importanti correttivi che andrebbero a:
- migliorare la tipizzazione del mezzo di ricerca della prova;
- aumentare le garanzie difensive nella fase successiva all'inoculazione del malware e nella fase finale della discovery delle attività effettuate da remoto;
- migliorare e potenziare la fase delle verifiche e del monitoraggio delle attività poste in essere dalle società private autorizzate all'inoculazione e all'intercettazione per conto delle Procure.

Dopo le pronunce della Cassazione[1] in materia di utilizzo del captatore informatico si è avuta estensione e una conseguente legittimazione delle molte funzionalità del captatore informatico, diverse e in aggiunta alla mera intercettazione tra presenti (anche in modalità cd itinerante).
Pertanto:

1. sono state pacificamente estese le funzioni del malware trojan (captatore informatico) anche alle **intercettazioni telematiche** soprattutto in considerazione dei flussi di comunicazioni in chiaro che il captatore riesce ad intercettare dal momento in cui viene inoculato all'interno del dispositivo; ma il Decreto legge n. 161 non menziona affatto tale applicazione del captatore in

relazione alle intercettazioni telematiche nonostante il ricorso alle telematiche cd attive sia ormai molto frequente.

Pertanto, sarebbe opportuno estendere la previsione normativa anche a tali tipologie di intercettazione anche allo scopo di evitare inutili eccezioni sull'atipicità dello strumento in tali modalità non previste dal Legislatore e ciò che forse più importa l'esclusione delle stesse intercettazioni telematiche con il trojan dall'archivio di cui all'art. 89 disp. Attuazione così come modificato dallo stesso decreto n. 161.

2. in questi anni sono state effettuate attività con il captatore anche su **dispositivi informatici ed elettronici fissi** (almeno fin dal 2004 per le indagini della sentenza Virruso – Cassazione 2010 e comunque fino ad oggi) e pertanto la tipizzazione che fa il DL del captatore come mezzo di ricerca della prova per i soli dispositivi portatili porterebbe ad escludere l'ammissibilità dell'utilizzo degli elementi di prova acquisiti sui dispositivi fissi o comunque a costringere i giudici e la giurisprudenza a forzare l'utilizzo anche per questi dispositivi;
si tenga presente che se la normativa del DL n. 161 non prevederà correttivi sul punto non potranno essere adeguate, senza incorrere in inutili forzature le adeguate garanzie che giustamente il DL prevede per le intercettazioni ambientali e tra presenti;
pertanto sarebbe opportuno, dopo la parola "dispositivo elettronico", eliminare la parola "portatile" in tutte le parti del decreto legge;

- 3. è assai limitativo parlare oggi solo di "captatore informatico" quando gli strumenti in uso alla criminalità impongono nuove e maggiori tecniche di captazione e di elusione degli apparati di cifratura (ormai con i telefoni Encrochat, cellulari cifrati olandesi BQ Acquaris, per citare solo alcuni, il solo captatore non serve più a nulla essendo necessari nuovi e diversi strumenti di Hacking), pertanto è più corretto e, in previsione futura, più efficace parlare di "attività di captazione informatica" al fine di prevedere ed estendere a livello normativo le opportune garanzie menzionate proprio dal DL n. 161 anche tutte le altre attività di captazione che la tecnologia rende e renderà possibile nel futuro e che non sono basate solo sul captatore ma sullo sfruttamento, in generale e in sintesi, delle vulnerabilità dei sistemi.

-4. Necessità di prevedere un sistema di controllo e monitoraggio (Logging) dei sistemi informatici e degli strumenti in uso presso le società private autorizzate dall'Autorità Giudiziaria a svolgere le intercettazioni. Il regolamento emanato con la legge Orlando, D.M. 20 aprile 2018 (Bollettino Min. Giustizia del 31

maggio 2018), non era sufficientemente puntuale nello specificare il monitoraggio e il tracciamento continuo del LOG e la loro conservazione automatica solo presso i locali della Procura della Repubblica. E' di tutta evidenza che tali strumenti di controllo avrebbero potuto impedire o limitare le situazioni, gli errori o i malfunzionamenti che sono accaduti in tempi recenti e che hanno avuto eco nazionale e internazionale. Non sfuggirà al lettore l'importanza di tali tracciamenti visto che la possibilità di monitorare l'attività degli strumenti che gestiscono le attività del captatore presso i locali delle società di intercettazione consentono anche, ove fosse necessario, la possibilità di ricostruire eventi, danni e abusi sui files contenenti le intercettazioni stesse.

5. Altra funzione del captatore che non è disciplinata dal DL n. 161 perché non riguarda le intercettazioni e è attinente ad altra e diversa materia è tutta la questione della captazione da remoto di documenti o altri dati che non rientrano nel concetto di "comunicazioni" o "comportamenti comunicativi".
E' uno dei punti più delicati in quanto concerne la delicata materia della cd perquisizione occulta da remoto, pur possibile in astratto con il captatore ma non disciplinata da alcuna norma dell'ordinamento, con la quale è tecnicamente possibile acquisire da remoto documenti e files senza le opportune garanzie difensive (es. la notifica all'indagato dell'atto di perquisizione classico). Questa attività di perquisizione o ispezione informatica oggi non è oggetto del DL in commento. Si sottolinea però l'importanza fondamentale che il legislatore preveda in futuro tali mezzi di ricerca della prova (con le opportune garanzie difensive come la notifica ritardata del provvedimento) al fine di evitare che la giurisprudenza ricorra ancora al concetto di prova atipica per legittimare attività con il captatore molto più simili alle ispezioni e alle perquisizioni piuttosto che alle intercettazioni.
Per questo tipo di attività di captazione informatica e per il suo tentativo di regolamentarlo si deve fare riferimento alla proposta inserita nel disegno di legge Quintarelli[2] di alcuni anni fa quando, insieme ad altre norme presenti nel disegno di legge, si cercò di prevedere un nuovo mezzo di ricerca della prova inserendo un articolo 254-ter nel codice di procedura penale in materia di osservazione e acquisizione da remoto (rinvio sotto al testo de iure condendo)

[2] https://www.camera.it/leg17/126?idDocumento=4260 . Si sottolinea come il disegno di legge Quintarelli stia riscuotendo grande interesse in sede internazionale attraverso numerose interrogazioni e richieste che grandi organizzazioni dei diritti umani e della persona stanno rivolgendo ai loro governi sulla necessità di regolamentare la loro disciplina sul trojan proprio come l'Italia stava facendo anni fa con questo disegno di legge (associazioni come Access now, Trasparency international, privacy international). Per tutti si veda in https://trojansandruleoflaw.org/

pertanto, si propone di:

g) all'articolo 270:

si modifichi eliminando "captatore informatico" e inserendo "attività di captazione informatica";

si modifichi inoltre eliminando "portatile" dopo "dispositivo elettronico" ;

1) il comma 1-*bis*è sostituito dal seguente: «*1-bis.* Fermo restando quanto previsto dal comma 1, i risultati delle intercettazioni tra presenti operate con ~~captatore informatico~~ attività di captazione informatica su dispositivo elettronico ~~portatile~~ possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'articolo 266, comma 2-*bis*.

Intercettazioni telematiche di cui all'art. 266 bis cpp:

Pacificamente da anni il captatore effettua anche attività di intercettazione telematica: l'inoculazione all'interno di dispositivi elettronici consente di effettuare, sempre dietro richiesta del pubblico ministero e autorizzazione del giudice per le indagini preliminari sia le cd intercettazioni ambientali (anche itineranti, v. Cassazione SSUU 2016, Scurato) sia le intercettazioni telematiche di quei flussi di dati informatici in chiaro tipici di molte attività che gli utenti effettuano normalmente durante l'utilizzo dei dispositivi.
Pertanto, al fine di far confluire anche tali intercettazioni all'interno dell'archivio di cui all'art. 89 disp. Att.ne cpp, (ne verrebbero escluse !!) ma soprattutto al fine di tipizzare tutti i mezzi di ricerca della prova, eliminare ogni ricorso a mezzi di prova atipici che non prevedono garanzie difensive e di non disciplinare ciò che oggi è già un mezzo di ricerca della prova (atipico) appunto grazie alla capacità di intercettare i flussi telematici, è necessario:

prevedere il captatore ovvero l'attività di captazione informatica anche per le intercettazioni telematiche di cui all'art. 266 bis cpp

all'art. Art. 266, bis cpp, aggiungere alla fine dopo "sistemi" le parole "attraverso attività di captazione informatica"
Intercettazioni di comunicazioni informatiche o telematiche
Nei procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi attraverso attività di captazione informatica

2. Alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio1989, n.271, sono apportate le seguenti modificazioni:
a) l'articolo 89 è sostituito dal seguente:

«Art. 89. *(Verbale e registrazioni delle intercettazioni).*
Al primo comma,
(Omissis)

dopo le parole *"Quando si procede ad intercettazione delle comunicazioni e conversazioni tra presenti mediante"* sostituire le parole *"inserimento di captatore informatico su dispositivo elettronico portatile," e* aggiungere le parole "attività di captazione informatica su dispositivo elettronico," .

al secondo comma dell'art. 89 dopo la parola "attraverso" eliminare ~~captatore informatico in dispositivi elettronici portatili~~ e aggiungere "*attività di captazione informatica su dispositivo elettronico* ed eliminare portatili:
2. Ai fini dell'installazione e dell'intercettazione attraverso attività di captazione informatica su dispositivo elettronico ~~captatore informatico in dispositivi elettronici portatili~~ possono essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia.

Al comma 5 dello steso art. 89 disp att. ne:

dopo la parola "alla disattivazione" eliminare "captatore" e aggiungere "delle attività di captazione informatica su dispositivo elettronico"

cosi :
art. 89 disp att. comma 5:

5. Al termine delle operazioni si provvede, anche mediante persone idonee di cui all'articolo 348 del codice, alla disattivazione degli strumenti o delle attività di captazione informatica su dispositivo elettronico con modalità tali da renderlo inidoneo a successivi impieghi. Dell'operazione si dà atto nel verbale. »

*B)*l'articolo 89-*bis*è sostituito dal seguente:

« Art. 89-*bis (Archivio delle intercettazioni)*.
Omissis

Sostituire il comma 3 :

3. Con decreto del Ministro della giustizia sono stabiliti i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante inserimento di strumenti o comunque di attività di captazione informatica su dispositivi elettronici ~~portatile.~~

FUORI DAL CONTESTO DEL DL n. 161, si suggerisce una riflessione su tale possibile articolo:

- Ipotesi di ***perquisizione o ispezione da remoto*** con notifica ritardata dell'atto:

Art. 1 (Introduzione dell'articolo 254-ter del codice di procedura penale in materia di osservazione e acquisizione da remoto)

1. Dopo l'articolo 254-bis del codice di procedura penale è inserito il seguente:
"Art. 254-ter (Osservazione e acquisizione da remoto)

1. Nei procedimenti di criminalità organizzata, di stampo mafioso, di terrorismo, e negli altri procedimenti puniti con la pena nel massimo pari ad anni XXXXXXXXX[3], il Giudice , su richiesta del Pubblico Ministero, può disporre l'osservazione dei dispositivi e l'acquisizione da remoto dei dati contenuti in un sistema informatico o telematico compresi quelli relativi al traffico telefonico o telematico non altrimenti acquisibili, solo quando vi sono gravi indizi di reato e quando l'osservazione e l'acquisizione da remoto sono assolutamente indispensabili per la prosecuzione delle indagini. Ogni acquisizione deve essere autorizzata dal Pubblico Ministero e convalidata con decreto motivato dal Giudice per le indagini preliminari.
2. Si applicano gli articoli 266 bis commi 1 quater e 1 quinquies, gli articoli 267, 268 e 268-bis, l'art. 269 del codice di procedura penale, in quanto compatibili.
3. Il decreto autorizzativo di cui al comma 1, deve essere notificato alla persona sottoposta alle indagini, alle altre parti nonché, se diversi, ai proprietari e agli utilizzatori dei dispositivi, entro "x" giorni dall'inizio delle attività oppure, ove vi sia fondato motivo di ritenere che dalla notifica possa derivare un grave pregiudizio alle indagini, il Giudice su richiesta del Pubblico Ministero può prorogare tale termine ogni X giorni e fino ad un massimo di diciotto mesi con un provvedimento adeguatamente motivato.

Roma 4 febbraio 2020

Prof. Avv. Stefano Aterno

[3] La scelta della categoria dei reati per i quali sarebbe possibile l'uso del captatore con queste modalità è riservata al Legislatore ma si suggerisce di usare la tecnica della pena nel massimo piuttosto che l'indicazione delle singole fattispecie e si suggerisce di includere in tale novero anche e soprattutto i reati informatici gravi ovvero quelli condotti contro le infrastrutture critiche.