IL VIRUS TROJAN: UNO STRUMENTO NELLE MANI INCONTROLLABILI DELLA POLIZIA GIUDIZIARIA

Leonardo Filippi

Per scaricare il pdf della sentenza clicca su Cass. Sez. IV, n. 32428 del 24.9.2020

1. La sentenza in commento si contraddistingue per la scarsa sensibilità sul rispetto della libertà domiciliare e della segretezza delle comunicazioni, messe ormai in ulteriore pericolo dal ricorso incontrollabile al *virus trojan*.

La pronuncia, purtroppo, si allinea a quell'indirizzo giurisprudenziale che considera il captatore informatico una semplice diversa modalità di intercettazione, dimenticando la pervasività del *malware*, nonostante la stessa sentenza riporti le parole delle Sezioni unite Scurato sulla forza intrusiva del nuovo congegno[1].

Infatti, diversi sono i profili dell'impiego del captatore informatico presi in considerazione dalla pronuncia, ma tutti risolti all'insegna della salvaguardia dei risultati raccolti, disinteressandosi del modo in cui sono stati conseguiti.

2. Anzitutto, la sentenza affronta il tema della motivazione dei decreti autorizzativi, censurati per non indicare sufficientemente le ragioni per le quali tale modalità di intercettazione mediante *virus trojan*, e quindi particolarmente invasiva, fosse necessaria per lo svolgimento delle investigazioni. La Corte osserva correttamente che l'autorizzazione riguardava un delitto di criminalità organizzata per il quale non deve essere motivata una "assoluta indispensabilità per la prosecuzione delle indagini" ma una semplice "necessità per lo svolgimento". Ma esclude la Corte che sia una formula stereotipata l'assertiva e apodittica affermazione secondo cui tale mezzo tecnico avrebbe costituito "l'unico da cui era possibile trarre notizie sulle direttive emanate dai capi *clan* in stato di detenzione, conoscere le dinamiche interne del sodalizio ed individuare il compito affidato a ciascuno dei sodali all'interno della compagine criminale". Dimentica, però, la Corte che l'autorizzazione riguardava utenze già in corso di intercettazione con modalità "ordinarie" e ciò sta a dimostrare che il ricorso al captatore non era l'unico modo per ottenere le informazioni rilevanti per le indagini, ma una modalità aggiuntiva a quella ordinaria già in corso.
3. In seconda battuta, la sentenza ritiene legittima la sovrapposizione di nuovi decreti autorizzativi di intercettazioni tramite *trojan* ad altri già in corso ed in esecuzione mediante strumenti tradizionali di captazione delle conversazioni telefoniche e tra presenti.

La sentenza motiva la decisione sostenendo, in modo molto formale, che "la disposizione di un diverso decreto di intercettazione sul medesimo bersaglio/dispositivo elettronico colpito dalle investigazioni, motivata dalla necessità di far ricorso, per ragioni investigative, allo strumento di captazione informatica sviluppato tramite *virus trojan*, configura, un nuovo ed autonomo mezzo di ricerca della prova, perfettamente legittimo in presenza del rispetto dei presupposti di legge per la sua autorizzazione, che non presenta interferenze con le intercettazioni telefoniche e/o ambientali già disposte con i mezzi ordinari, pur se l'oggetto sul quale sono stati installati i captatori informatici coincide con quello su cui sono state disposte altre intercettazioni".

La pronuncia ne deduce addirittura un "principio", che sarebbe basato, oltre che sull'analisi del dato normativo, che non prevede preclusioni di sorta per tale ipotesi, su alcune constatazioni della disciplina "di sistema" delle intercettazioni, ricavate dalla giurisprudenza della stessa Corte di cassazione, secondo cui è ben possibile, da parte dell'autorità giudiziaria, oltre che, ovviamente, far cessare l'intercettazione già disposta prima del termine ovvero non prorogarla, anche disporla nuovamente, una volta che sia scaduto per qualsiasi ragione il termine per la proroga, dovendosi in tal caso solo giustificare la nuova intercettazione (identica per obiettivo colpito) secondo gli ordinari criteri previsti dal legislatore come presupposti per l'autorizzazione [2].

A riprova della piena legittimità di sovrapposizioni di intercettazioni diverse, la pronuncia richiama la giurisprudenza di legittimità che afferma che il decreto formalmente qualificato "di proroga" dell'intercettazione, intervenuto dopo la scadenza del termine originario o già prorogato, può avere natura di autonomo provvedimento di autorizzazione all'effettuazione delle suddette operazioni, se dotato di autonomo apparato giustificativo, che dia conto della ritenuta sussistenza delle condizioni legittimanti l'intromissione nella altrui sfera di riservatezza[3].

La sentenza conclude che la legittimità di sostituire l'intercettazione di un obiettivo tramite captatore informatico a quella tramite strumenti ordinari, anche sovrapponendole nei tempi e termini di autorizzazione, discende dalla diversa natura dell'attività di intercettazione mediante *trojan* che è più pervasiva, avendo ad oggetto il complesso dei flussi informativi afferenti ad un determinato *target* e ponendosi come finalità quella di arrivare alla percezione e registrazione di conversazioni, messaggi ed informazioni ulteriori rispetto a quelle captate tramite gli strumenti ordinari. E la riprova di tale diversità deriva dalla disciplina normativa in parte differente, che è stata prevista per regolamentare i presupposti normativi per l'autorizzazione delle intercettazioni tramite captatore informatico, secondo le regole procedimentali dettate dal legislatore del 2017.

Ma l'argomentazione non convince perché il fatto che gli strumenti siano diversi non giustifica l'attentato ai medesimi beni della libertà domiciliare e della segretezza delle comunicazioni, che anzi sono doppiamente limitati.

Inoltre, pare evidente che una tale operazione di moltiplicazione di intercettazioni nei confronti dello stesso soggetto non sia consentita perché l'impiego del *virus trojan* è ammesso quando il ricorso ad altri strumenti di intercettazione non è possibile, per cui utilizzare il captatore informatico abbinato alla tradizionale intercettazione significherebbe smentire la motivazione di indispensabilità posta a sostegno del *virus trojan*. Inoltre, tale duplicazione si risolverebbe in una surrettizia elusione dei termini previsti dal legislatore per la durata delle intercettazioni, richiamati in ciascun decreto autorizzativo, che sarebbero sostanzialmente raddoppiati.

4. La sentenza affronta poi due ulteriori questioni.

La prima riguarda la denunciata scarsa precisione dei decreti autorizzativi nell'indicare le modalità con le quali la polizia giudiziaria ha potuto avvalersi del personale della ditta specializzata RCS nelle attività di inserimento del *trojan* e l'incertezza, dovuta a mancanza di adeguata documentazione e verbalizzazione delle operazioni svolte, su quali siano state le modalità attuative dell'intercettazione poste in essere dal personale privato delegato.

La seconda attiene alla mancata indicazione del nominativo di chi ha materialmente eseguito le operazioni di inoculazione del *virus* e dato luogo alla fase primaria e ancora più delicata della stessa installazione del *software* captatore, cioè quella di analisi dei dati relativi al dispositivo da intercettare.

Ma la pronuncia in esame, in riferimento alla mancata indicazione nei verbali di esecuzione delle operazioni di intercettazioni sia delle modalità specifiche con le quali si è installato il *virus trojan* nel dispositivo bersaglio, sia del nominativo del tecnico che ha compiuto tali operazioni, afferma che tali censure peccherebbero di genericità per non essere stato chiarito quale sia l'interesse del ricorrente avuto riguardo a tale aspetto, non essendo stati dedotti vizi o illegittimità sul piano indiziario da parte sua in conseguenza di tali carenze.

Come se l'interesse a tutelare il proprio domicilio e la segretezza delle proprie conversazioni non fosse un motivo degno di interesse e di tutela da parte dell'ordinamento. Tanto più ora che il legislatore ha previsto, nel comma 1-*bis* dell'art. 271 c.p.p., una specifica causa di inutilizzabilità per i "dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico su dispositivo elettronico portatile" e per i "dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo".

5. In particolare, sulla prima questione, la sentenza in commento, segue le indicazioni delle Sezioni unite Scurato per concludere che la disciplina in tema di intercettazioni ambientali è omogenea a quella delle intercettazioni disposte tramite captatore informatico e da tale omogeneità deriverebbe, anzitutto, che le operazioni esecutive di installazione degli strumenti tecnici atti a captare le conversazioni tra presenti dovrebbero ritenersi implicitamente autorizzate ed ammesse con il provvedimento che dispone l'intercettazione; ciò sulla scorta della giurisprudenza che afferma che la collocazione di microspie all'interno di un luogo di privata dimora, costituendo una delle naturali modalità attuative di tale mezzo di ricerca della prova, deve ritenersi implicitamente ammessa nel provvedimento che ha disposto le operazioni di intercettazione, senza la necessità di una specifica autorizzazione[4].

Tale “principio” sarebbe diretta conseguenza del fatto che le intercettazioni di comunicazioni sono un mezzo di ricerca della prova funzionale al soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost., con il quale il principio di inviolabilità del domicilio previsto dall'art. 14 Cost. e quello di segretezza della corrispondenza e di qualsiasi forma di comunicazione previsto dall'art. 15 Cost. devono coordinarsi, subendo la necessaria compressione[5].

La pronuncia in esame aggiunge che le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni costituiscono “atti materiali rimessi alla contingente valutazione della polizia giudiziaria, non essendo compito del pubblico ministero indicare le modalità dell'intrusione negli ambiti e luoghi privati ove verrà svolta l'intercettazione”; inoltre “l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali”[6].

La giurisprudenza è giunta al punto di ritenere utilizzabili i risultati di intercettazioni acquisite tramite la collocazione di microspie, anziché mediante l'impiego di un *software* spia, così come invece era originariamente disposto nel decreto autorizzativo del giudice; e da tale provvedimento deriva che la modifica delle modalità esecutive delle captazioni, concernendo un aspetto meramente tecnico, può essere autonomamente disposta dal pubblico ministero, non occorrendo un apposito provvedimento da parte del giudice per le indagini preliminari[7]. La sentenza in esame sostiene che l'autorizzazione a disporre le operazioni di intercettazioni “rende superflua l'indicazione delle modalità da seguire nell'espletamento dell'attività materiale e tecnica da parte della polizia giudiziaria, mentre la prova delle operazioni compiute nel luogo e nei tempi indicati dal giudice stesso e dal pubblico ministero è offerta dalla registrazione delle conversazioni intercettate”[8].

In sintesi, la sentenza afferma i seguenti principi di diritto:

- le questioni relative all'installazione degli strumenti tecnici per l'intercettazione -come il *virus trojan* - in relazione all'obiettivo da intercettare non attengono alla fase autorizzativa dell'attività investigativa demandata al giudice per le indagini preliminari, né alla verifica dei presupposti di legittimità delle intercettazioni, bensì alla fase esecutiva, già coperta dall'autorizzazione a disporre le stesse intercettazioni;

- la fase esecutiva è consegnata alle prerogative del pubblico ministero che può delegare la polizia giudiziaria alle operazioni materiali di installazione tecnica degli strumenti (*software*, *hardware*, *trojan*) idonee a dar vita, in concreto, alle intercettazioni e addirittura ci si spinge ad affermare che eventuali modifiche degli strumenti già indicati nel decreto autorizzativo del G.I.P. come quelli da utilizzare per eseguire le captazioni possono essere disposte dallo stesso pubblico ministero;

- le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni, anche tramite *virus trojan*, costituiscono atti materiali rimessi alla contingente valutazione della polizia giudiziaria e l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali.

In altre parole, al giudice non interessa in che modo è stato installato il *virus trojan* perché si tratta della fase esecutiva dell'intercettazione demandata al pubblico ministero, il quale delega la polizia giudiziaria, la quale ha mano libera nell'agire, anche con modalità diverse da quelle indicate dal GIP, e comunque essa potrebbe omettere qualsiasi verbalizzazione delle operazioni compiute perché tale omissione è priva di sanzione processuale.

In altre parole, la libertà domiciliare e la segretezza delle comunicazioni sono affidate all'iniziativa della polizia giudiziaria, la quale ha pieno e incontrollabile potere di utilizzare qualsiasi mezzo per eseguire l'intercettazione e il giudice e il P.M. non vogliono nemmeno sapere come si è proceduto, cioè se in maniera più o meno legittima. E infatti, nel noto "caso Palamara", le cronache giudiziarie riferiscono che, visto che l'indagato rifiutava *mail* e messaggi vari di invito che, sotto mentite spoglie, avrebbero consentito l'accesso del *virus trojan*[9] nel *device*, il P.M., senza nemmeno avvertire il G.I.P. che aveva autorizzato l'intercettazione col captatore informatico senza precisare le modalità di inoculazione, ordinò alla polizia giudiziaria di bloccare le telefonate in uscita dal cellulare, per cui il soggetto, dopo vari ma inutili tentativi di rimediare a quello che appariva un banale guasto dell'apparecchio, ricevette un avviso di invito a resettare il sistema per superare l'inconveniente e quindi, costretto ad aderire all'invito, diede inconsapevolmente accesso al *virus trojan* nel suo dispositivo.

Quindi alla pericolosità insita nel *virus trojan* si aggiunge l'ulteriore insidia delle modalità di inserimento, che sono sconosciute al giudice e al P.M. e incontrollabili dalla difesa.

6. In riferimento all'altra questione riguardante la mancata indicazione del nome dell'ausiliario che ha provveduto all'installazione del *virus* informatico per l'intercettazione, la Corte iscrive correttamente il difetto nella categoria dell'omessa documentazione delle operazioni svolte dalla polizia giudiziaria delegata dal pubblico ministero all'esecuzione delle operazioni autorizzate e che però non dà luogo ad inutilizzabilità o nullità dei risultati delle intercettazioni, alla stessa stregua di quanto si è affermato da una parte soltanto della giurisprudenza in un ambito parallelo ma omogeneo: quello della mancata indicazione delle generalità degli ausiliari utilizzati per la traduzione delle intercettazioni di conversazioni che si svolgano in lingua straniera[10].
7. Un'ultima questione affrontata dalla sentenza riguarda i rischi derivanti dal servirsi per l'installazione del *trojan* di personale proveniente da ditte private. La sentenza annotata richiama la giurisprudenza di legittimità che ha già chiarito come, in tema di intercettazioni telefoniche, la previsione dell'art. 267

c.p.p., secondo cui «il pubblico ministero procede alle operazioni personalmente ovvero avvalendosi di un ufficiale di polizia giudiziaria», si riferirebbe unicamente alle operazioni previste dal precedente art. 266, ossia alle intercettazioni di conversazioni o comunicazioni telefoniche o di altre forme di telecomunicazioni, con la conseguenza che qualsiasi altra «operazione» diversa, ancorché correlata, dalle suddette non rientrerebbe nella previsione normativa evocata e legittimamente, dunque, potrebbe essere svolta da personale civile[11].

In altre parole, quando serve a sorreggere la conclusione prescelta l'operazione di intercettazione mediante *virus trojan* diventa "diversa" da quella telefonica o di altre forme di telecomunicazioni.

Ma la sentenza contraddice se stessa, giacchè poco prima aveva affermato che "la disciplina in tema di intercettazioni ambientali è omogenea a quella delle intercettazioni disposte tramite captatore informatico" per poi contraddirsi e sostenere che l'operazione di intercettazione mediante *virus trojan* sarebbe "diversa" da quelle telefoniche e di altre forme di telecomunicazioni.

Insomma, la Corte di cassazione, che dovrebbe censurare la manifesta illogicità della motivazione, ci offre una motivazione manifestamente illogica !

8. In conclusione, ci troviamo di fronte ad una pronuncia molto deludente, che, in nome dell'efficienza del processo, sacrifica la libertà domiciliare e la segretezza delle comunicazioni, la cui limitazione è in definitiva affidata all'iniziativa, incontrollabile e priva di sanzioni, della polizia giudiziaria. Non resta che sperare che rimanga una pronuncia isolata e non apra la strada ad un nuovo illiberale indirizzo giurisprudenziale.

[1] Le Sezioni unite Scurato avevano definito il *virus trojan*"*Uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente: - di captare tutto il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia web mail, che outlook); - di attivare il microfono e, dunque, di apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi; - di mettere in funzione la web camera, permettendo di carpire le immagini; - di perquisire l'hard disk e di fare copia, totale o parziale, delle unità di memoria del sistema informatica preso di mira; - di decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (keylogger) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (screenshot); - di sfuggire agli antivirus in commercio. I dati raccolti sono trasmessi, per mezzo della rete internet, in tempo reale o ad intervalli prestabiliti ad altro sistema informatico in uso agli investigatori."* (Sez. un., c.c. 28.4.2016, (dep. 1.7. 2016), Scurato, n. 26889/2016).

[2] Si citano in tal senso Sez. VI, 16.6.2005, Ciaramitaro, n. 28521, Rv. 231957, in un caso di decreto di intercettazione d'urgenza e relativa convalida, che la Corte ha ritenuto legittima in luogo del decreto di proroga di cui sia scaduto il termine, atteso che il presupposto è comunque costituito dalla permanenza dei gravi indizi di reato e dall'assoluta indispensabilità dell'intercettazione ai fini della prosecuzione delle indagini (sostenendo che tale evenienza determina, in concreto, una maggiore garanzia per l'indagato, rispetto al decreto di proroga dell'intercettazione).

[3] Così Sez. V, 17.7.2015 (dep. 2016), Ambroggio, n. 4572, Rv. 265746.

[4] In tal senso cfr. Sez. VI, 31.1.2011, Di Maggio, n. 14547, Rv. 250032; Sez. I, 9.12.2003 (dep. 2004), Rigato, n. 24539, Rv. 230097.

[5] Così Sez. II, 18.2.2013, Badagliacca, n. 21644, Rv. 255541; Sez. I, 2.10.2007, Biondo, n. 38716, Rv. 238108; Sez. IV, 28.9.2005, Cornetto, n. 47331, Rv. 232777; Sez. VI, 10.11.1997, Greco, n. 4397, Rv.210062.

[6] Sez. VI, del 23.6.2017, Nobile, n. 39403, Rv. 270941; Sez. VI,25.9.2012, Adamo, n. 41514 Rv. 253805.

[7] Sez. VI, 8.3.2018, Romeo, n. 45486, Rv. 274934.

[8] Si cita, sul tema, in motivazione, - oltre che Sez. II, 18.2.2013, Badagliacca, n. 21644, Rv. 255541; Sez. I, 2.10.2007, Biondo, n. 38716, Rv. 238108; Sez. IV, 28.9.2005, Cornetto, n. 47331, Rv. 232777 - anche Sez. VI, 13.6.2017, Romeo, n. 36874.

[9] Di solito la polizia giudiziaria fa pervenire al dispositivo portatile un *link* contenuto in un SMS inviato da un contatto frequente o in un allegato ad una *mail* che pare inoffensiva, rispondendo ai quali si apre la porta al *virus trojan*.

[10] Secondo una certa giurisprudenza, l'omessa indicazione, nel verbale di esecuzione delle intercettazioni, delle generalità dell'interprete di lingua straniera che abbia proceduto all'ascolto, traduzione e trascrizione delle conversazioni, non è causa di inutilizzabilità dei risultati di tali operazioni, essendo tale sanzione prevista solo per i casi tassativamente indicati dall'art. 271 c. p. p. (Sez. V, 16.1.2020, Polak, n. 7030, Rv. 278659; Sez. V, 19.1.2018, Kochev, n. 15472, Rv. 272683; Sez. VI, 10.11.2017 (dep. 2018), Feretti e altri, n.

5197, Rv. 272151; Sez. VI, 23.3.2017, Lleshaj, n. 31285, Rv. 270570; Sez. III, 19.1.2017, Mifsud, n. 24305, Rv. 269985; Sez. V, 15.4.2015, Silagadze, n. 25549, Rv. 268024; Sez. VI, 4.6.2008, El Arbaoui, n. 24141, Rv. 240372; Sez. VI, 12.7.2007, Barbu, n. 30783, Rv. 237088).Anche le Sezioni Unite che con la pronuncia 26.6.2008, Carli, n. 36359, Rv. 240395, in motivazione, hanno chiarito come la violazione delle disposizioni sulla redazione del verbale poste dall'art. 89 disp. att. c.p p. non comporta l'inutilizzabilità dei risultati dell'intercettazione, ostandovi il principio di tassatività che governa la sanzione processuale, e, dunque, l'assenza di riferimenti in tal senso nell'art. 271 c. p. p. Secondo altro indirizzo giurisprudenziale l'omessa indicazione, nel verbale di esecuzione delle intercettazioni, delle generalità dell'interprete di lingua straniera che abbia proceduto all'ascolto, traduzione e trascrizione delle conversazioni, rende invece inutilizzabili i risultati di tali operazioni :Sez. III, 12.11.2013, Muka, n. 49331, Rv. 257291; Sez. III, 4.11.2015 (dep. 2016), Serban, n. 28216, Rv. 267448; Sez. III, 4.11.2015 (dep. 2016), Burcea, n. 31454, Rv. 267738.

[11] Cfr. in tal senso Sez. IV, 1.12.2016 (dep. 2017), Agnotelli, n. 3307, Rv. 269012; Sez. III, 7.1.2014, Vita, n. 11116, Rv. 259744, nonché Sez. VI, del 23/6/2017, Nobile, n. 39403 cit., in motivazione.