MA DAVVERO SI PUÒ RICORRERE A MANOVRE FRAUDOLENTE PER INTERCETTARE COL VIRUS TROJAN ?

Leonardo Filippi

1. Si era già messa in luce la pervasività del *virus trojan*, un micidiale strumento itinerante che può essere impiegato per compiere ispezioni, perquisizioni, sequestri, intercettazioni sonore e visive e localizzazione personale, come riconosciuto anche dalle Sezioni unite Scurato[1] E si è anche già evidenziata la pericolosità del nuovo strumento che emerge anche dall'interpretazione che proviene dalla Corte di cassazione, la quale consente l'intercettazione, tramite *virus trojan*, sul medesimo dispositivo già sotto intercettazione tradizionale, ritenendo che le questioni relative all'installazione del *virus trojan* non attengano 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. In questo modo la giurisprudenza consegna la fase esecutiva dell'intercettazione alle prerogative del pubblico ministero, il quale delega la polizia giudiziaria alle operazioni materiali di installazione tecnica degli strumenti (*software*, *hardware*, *trojan*) idonee a dar vita, in concreto, alle intercettazioni; ed è sempre il P.M. a disporre anche le eventuali modifiche degli strumenti già indicati nel decreto autorizzativo del G.I.P. da utilizzare per eseguire le captazioni. Così come è *ius receptum* che le operazioni di collocazione e disinstallazione del *virus trojan* costituiscono atti materiali rimessi alla contingente valutazione della polizia giudiziaria e l'omessa documentazione delle operazioni svolte non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali[2]. In altre parole, non occorre nemmeno verbalizzare come la polizia giudiziaria ha installato il *virus trojan*, che quindi è una modalità ignota e incontrollabile nelle mani della polizia giudiziaria.

2. Ma anche su altri fronti emerge prepotentemente la insidiosità del captatore informatico.

Il *virus trojan* infatti non limita soltanto la segretezza, ma pure la libertà di autodeterminazione della persona da intercettare. Ormai di regola nella prassi si verifica che, quando il portatore del dispositivo elettronico portatile non dà l'*input* che consente l'accesso al *malware* (ad es. non accetta l'aggiornamento proposto come "cavallo di Troia), il P.M. ricorre ad ulteriori e più insidiosi stratagemmi, non previsti dalla legge, quali, ad esempio, di bloccare le telefonate in uscita dal cellulare per costringere l'ignaro soggetto ad operazioni che comportano l'accesso del *virus trojan* nel dispositivo, come accaduto nel noto "caso Palamara"[3].

Si è perciò dubitato della legittimità dell'impiego del *trojan horse*, quale conseguenza della modalità "subdola" di acquisizione della prova attraverso l'induzione del soggetto intercettato alla "autoinstallazione" del virus, con costi a carico del destinatario e in violazione del principio di autodeterminazione di cui all'art. 188 c.p.p. Ed in effetti, già la denominazione di "cavallo di Troia" dovrebbe far capire che si tratta di una manovra fraudolenta.

Infatti, mentre per le tradizionali forme di intercettazione non è mai necessaria una collaborazione della persona da monitorare, per il *trojan*, salvo i rari casi in cui si riesca ad avere la disponibilità fisica

dell'apparecchio per il tempo necessario all'installazione del *virus*, si deve sempre ricorrere ad una "trappola" per inoculare il *malware* sull'apparecchio portatile, senza alcun consenso da parte del titolare del dispositivo controllato ed anzi con la sua inconsapevole collaborazione. Di solito si invia al *device* da monitorare una *mail* o altro messaggio, apparentemente inoffensivo, aprendo il quale si scarica il *virus* senza averne alcuna consapevolezza. Inoltre, le modalità di questa "trappola" non sono indicate dalla legge, con conseguente limitazione talvolta anche della libertà domiciliare in plateale violazione della riserva di legge; di conseguenza, tali stratagemmi sfuggono alle prescrizioni ed al controllo sia del P.M. sia del G.I.P. e sono lasciate all'estemporanea iniziativa della polizia giudiziaria. In fondo, "trappole" del genere sono sempre state praticate: si pensi all'espediente cui ricorre la polizia giudiziaria, per sistemare le microspie, di entrare a casa del sospettato, sotto le mentite spoglie di un operaio del gas o della società elettrica o di accedere all'abitacolo della vettura con i doppioni delle chiavi.

Ma la Corte di cassazione esclude ora che il captatore informatico possa inquadrarsi tra "i metodi o le tecniche" idonee ad influire sulla libertà di determinazione del soggetto, come tali vietati dall'art. 188 c. p. p., sostenendosi che il captatore informatico "non esercita alcuna pressione sulla libertà fisica e morale della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità"[4].

In realtà, il captatore viene inconsapevolmente auto-installato dal soggetto controllato, che viene indotto a farlo con artifici e raggiri: gli si fa credere che è un'operazione che serve a ripristinare o a migliorare la funzionalità del suo *device* quando, invece, si tratta di un modo subdolo per spingerlo a compiere un atto che, a sua insaputa, inocula il *virus trojan* nel suo dispositivo e quindi consente l'intercettazione. In questo caso, a nostro parere, il pubblico ministero viene meno ad suo dovere di lealtà processuale e viola il principio di autodeterminazione garantito dall'art. 188 c.p.p. a chiunque, e *in primis* all'indagato. Come noto, tale disposizione vieta l'utilizzazione, neppure con il consenso della persona interessata, di "metodi o tecniche idonei ad influire sulla libertà di autodeterminazione", e il divieto non riguarda soltanto il contenuto della dichiarazione, ma anche qualsiasi costrizione, fisica o psichica, ad un *facere* [5].

A mio parere, non è ammissibile che lo Stato, al fine di reprimere le condotte illecite dei criminali, scenda al loro livello, ingannando l'indagato per indurlo a consentire inconsapevolmente l'accesso al "cavallo di Troia".

E siccome l'impiego di tali fraudolente manovre è diventata ormai la regola, il problema non può essere più ignorato.

3. Così come non può essere più ignorato il problema, ancora più grave, dei tempi di accensione e spegnimento del microfono, che è lasciato all'insindacabile opinione della polizia giudiziaria, la quale

quindi è libera di scegliere le conversazioni ed i soggetti da intercettare oppure da tenere fuori delle indagini, come è emerso, ancora una volta, nel caso Palamara[6].

E' vero, infatti, che l'art. 267, comma 1, c.p.p. prescrive che, se si procede per delitti diversi da quelli di cui all'art. 51, commi 3-*bis* e 3-*quater* c.p.p. e dai delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la reclusione non inferiore nel massimo a cinque anni, il decreto di autorizzazione del G.I.P. deve indicare "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono". Ma proprio tale generica e indiretta determinazione lascia spazio alle scelte, non necessariamente documentate e quindi incontrollabili, della polizia giudiziaria. Abbiamo infatti visto come la giurisprudenza affermi che l'omessa documentazione delle operazioni di intercettazione non dia luogo ad alcuna nullità o inutilizzabilità dei relativi risultati, per cui, non solo la polizia giudiziaria può non verbalizzare come ha installato il *virus trojan*, ma può anche omettere di indicare quando, dove e perchè ha attivato o disattivato il microfono, che quindi è un altro aspetto dell'esecuzione della captazione che può restare sconosciuto e quindi insindacabile.

Per leggere la sentenza clicca su SENTENZA

[1] Le Sezioni unite Scurato avevano precisato che "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] Cass., sez. V, 24.9.2020, Marzano, n. 32428, in questa Rivista, 30.11.2020, con nota dello scrivente, *Il virus trojan: uno strumento nelle mani incontrollabili della polizia giudiziaria.*

[3] 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* (di solito viene inviato un *link* contenuto in un SMS inviato da un contatto frequente o in un allegato ad una mail che pare inoffensiva), 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, 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.

[4] Cass., sez. V, 30.9.2020 (dep. 11.1.2021), Palazzo, n. 31604. V. pure Cass., sez. I, 18.12.2013 (dep. 30.1.2014), Cinà, n. 4429, Rv.258310, che dichiara inutilizzabile l'intercettazione delle dichiarazioni indotte in una persona dall'adozione di metodi o tecniche idonei a influire sulla sua capacità di autodeterminazione, posto che il divieto dell'art. 188, comma 1, c. p. p. investe l'oggetto della prova e non è circoscritto al contesto formale delle sole prove dichiarative (fattispecie nella quale le conversazioni indizianti erano state registrate in un ufficio di polizia, dove il locutore era stato sottoposto a minacce e violenze dal personale di polizia giudiziaria. V. invece Cass. 8.4.1994, Giannola, che dichiara utilizzabile la registrazione di una conversazione telefonica eseguita da uno degli stessi interlocutori, non rientrando tra le intercettazioni, e comunque il fatto che venga registrata all'insaputa dell'altro non costituisce offesa alla libertà di autodeterminazione dell'ignaro interlocutore che ha comunicato in piena libertà.

[5] P. FERRUA, *La prova penale*, Torino, 2015, p. 103 ss. ritiene "inammissibile una costrizione del soggetto ad atti che richiedano un comportamento collaborativo, un *facere*"; il divieto non coinvolge, invece, gli atti in cui, per la loro stessa natura, "la persona intervenga come corpo, come oggetto di ispezione, di prelievo o di riconoscimento; atti che implicano un atteggiamento passivo di chi vi è sottoposto, che si sostanziano in un *pàtere*. In questi casi l'esecuzione coatta dell'atto non è a priori inammissibile, purchè sia prevista e regolata dalla legge come richiede l'art. 13 comma 2 Cost.". In senso contrario, pare R. APRATI, ne *Il Foro it.,*16.1.2021, che ritiene che l'art. 188 tuteli soltanto l'oggetto della prova, ovverosia le dichiarazioni o i comportamenti, i quali devono essere frutto di una scelta del soggetto che li realizza, per cui esulerebbe dalla sfera dell'art. 188 c.p.p. tutto ciò che non attiene a tale specifico aspetto, come la circostanza che il sistema di registrazione sia involontariamente e inconsapevolmente istallato dallo stesso soggetto poi registrato.

[6] Nel "caso Palamara" è emerso che la polizia giudiziaria ha interrotto la registrazione nelle occasioni in cui il magistrato intercettato doveva incontrarsi con l'allora Procuratore della Repubblica di Roma.