IL NUOVO "CAVALLO DI TROIA"

Leonardo Filippi

La nuova disciplina delle intercettazioni, introdotta dalla l. n. 7/2020 consente l'impiego del *virus trojan* per tutti i reati suscettibili di intercettazione, per cui questo invasivo mezzo è divenuto un ordinario strumento di investigazione: ma è veramente paradossale che proprio una legge che si proponeva di tutelare la riservatezza abbia mantenuto un utilizzo così ampio (cioè per ogni reato soggetto ad intercettazione) di un dispositivo che, captando comunque le voci di chiunque si intrattenga con il suo portatore, di qualunque argomento parli e ovunque si trovi, persino negli sconosciuti domicili altrui, è l'antitesi della *privacy*[1].

La insidiosità del captatore informatico deriva anche dal fatto che non limita soltanto la segretezza, ma anche la libertà delle comunicazioni: infatti, si verifica ormai nella prassi che, quando il portatore del dispositivo elettronico portatile non dà l'*imput* 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 suo dispositivo [2].

Ma l'impiego generalizzato del captatore informatico comporta diversi altri gravi inconvenienti. Sono rimasti insoluti, ad esempio, il problema dell'esternalizzazione della gestione delle intercettazioni a società private e la subalternità sinora dimostrata dal ministero della giustizia alle loro logiche tecniche ed economiche. Addirittura la cronaca riferisce di inconvenienti tecnici che potrebbero pregiudicare la genuinità o la completezza delle registrazioni. Risulta infatti che il *software* per la visualizzazione delle intercettazioni telematiche distingue tra progressivi primari (quelli con contenuto) e progressivi secondari (che sono quelli senza contenuto o di base non tipicamente rilevanti), per cui la valutazione sulla rilevanza della comunicazione è lasciata alla macchina, anzichè al giudice e alle parti. In altre parole, al giudice e alle parti sono sottratte alcune comunicazioni che potrebbero essere rilevanti. Inoltre, risulta che il captatore non può registrare continuamente e comunque per un tempo troppo lungo, per evitare un consumo eccessivo della batteria, e in ogni caso esso non sempre può trasferire i dati in tempo reale al *server* per mancanza o scarsa connessione ad *internet* del dispositivo monitorato.

Ma resta ignorato anche il problema della delocalizzazione dei sistemi *cloud* di archiviazione in Paesi non soggetti alla nostra giurisdizione. Per non parlare della consuetudine dei consulenti tecnici del P.M. di non cancellare i dati, una volta terminati gli incarichi conferiti loro dalle Procure, accumulando così enormi ma ignoti archivi, paralleli a quelli blindati presso le procure, e che la cronaca ci ha mostrato come siano stati spesso utilizzati per commercializzare illecitamente conversazioni compromettenti. Tale mercato clandestino rivende e diffonde illegalmente la gran massa delle conversazioni e comunicazioni intercettate, mentre nel processo se ne utilizza la minima parte. Intanto, il legislatore ha perso l'occasione per disciplinare sia le già invalse pratiche di polizia, come il G.P.S., l'"agente segreto attrezzato per il suono", le riprese visive nel domicilio o i "*code catcher*", che negli U.S.A. sono impiegati dalla polizia da almeno venticinque anni per

registrare le informazioni provenienti da tutti i cellulari che si trovano in una certa area[3] e sono da tempo usati anche in Italia tanto che se ne è interessata pure la Corte di cassazione[4], sia le più recenti tecniche d'intercettazione, come l'impiego dei droni per finalità di intercettazione di comunicazioni e di riprese visive.

[1] In generale, sul tema v. M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. contemp.*, 20.12.2018; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, p. 235, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra e R. Orlandi, Torino, 2018; ID., *L'impiego del* trojan horse *informatico nelle indagini* penali, in *Riv. it.sc. giur.*, 2018, 8, p. 329 ss.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista brasileira de direito processual penal*, 2017, p. 483; A.GAITO e S.FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, p. 309 ss.; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017.

[2] Nel noto "caso Palamara", 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 attendibile), 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.

[3] Il *code-catcher* è un apparecchio portatile, delle dimensioni d'una valigetta, che può essere portato a mano, caricato in macchina, installato su un drone o su un aereo e sfruttando alcune vulnerabilità delle reti di comunicazione, in particolare quelle che adoperano lo standard GSM, finge di essere un ponte radio, in modo da indurre i cellulari nei dintorni ad agganciarsi e carpirne i codici identificativi, sia il codice IMSI (*International Mobile Subscriber Identity*) della *Sim card*, sia il codice IMEI (*International Mobile Equipment Identity*) del cellulare. La cattura dei codici del dispositivo è operazione propedeutica a controlli ulteriori, quali l'inoculazione d'un *trojan horse* o un'intercettazione nei confronti di un telefono di cui ancora non si conosce il numero o anche un "pedinamento elettronico" (una volta che il codice identificativo del bersaglio sia stato ottenuto, esso viene inserito nello *Stingray*, che a questo punto è in grado di seguirne gli spostamenti) : v. in proposito A.CAMON, *Il cacciatore di IMSI*, in *Arch. Pen,*, 2020, n. 1 .

[4] Cass., sez. IV, 12 giugno 2018, Chirico e altro, n. 41385, in *CED* 273929.