# VITA DIGITALE A RISCHIO:

## I CAPTATORI INFORMATICI TRA PERICOLI PER I DIRITTI UMANI E RIDUZIONISMO GIURIDICO

*PROF. AVV. ROBERTO DE VITA, AVV. ANTONIO LAUDISA*


*Il rapporto tra diritti dell'individuo e potere investigativo coinvolge i nuovi e potentissimi strumenti a cui anche lo Stato fa ricorso. Il Trojan ne è l'esempio più concreto ed attuale.*

L'era digitale impone, ormai in maniera sempre più frequente, una rivalutazione degli equilibri tra libertà fondamentali dell'individuo ed interesse dello Stato all'accertamento ed alla prevenzione dei reati.

Siamo immersi in realtà interconnesse e circondati da dispositivi dotati di tecnologia smart, attraverso cui dialoghiamo, ci muoviamo, comunichiamo, ricordiamo. I dati qui contenuti rappresentano un patrimonio informativo sconfinato, su cui sempre più spesso impattano le Forze dell'ordine e l'Autorità giudiziaria,

per perseguire gli autori di condotte criminose o, addirittura, per prevenirne la commissione.

Il rapporto tra diritti dell'individuo e potere investigativo coinvolge anche i nuovi e potentissimi strumenti a cui lo Stato fa ricorso, che – secondo la puntuale definizione della Commissione LIBE del Parlamento europeo – rientrano nel concetto di "hacking by law enforcement" [1].

Nello studio pubblicato a marzo del 2017, la Commissione LIBE dichiara che l'uso di "hacking techniques" da parte delle "law enforcement agencies" si sta evolvendo in maniera organica per vincere la sfida del "going dark" [2]: termine particolarmente evocativo (cui fa esplicito riferimento la stessa FBI [3]), descrive la crescente difficoltà delle Forze di polizia di avere legalmente accesso e di esaminare tanto le informazioni "a riposo" [4] contenute sui dispostivi quanto alle informazioni "in movimento" tra sistemi di comunicazione [5].

L'oscurità in cui rischiano di brancolare le Forze di polizia e l'Autorità giudiziaria deriva, principalmente, dai sistemi di crittografia ("encryption"): i numerosi e diffusi protocolli di sicurezza delle "technology companies" garantiscono, infatti, la protezione e la riservatezza delle comunicazioni tra individui, impedendo l'accesso a soggetti terzi.

**"L'uso di hacking techniques da parte delle law enforcement agencies si sta evolvendo per vincere la sfida del c.d. going dark"**

***COMMISSIONE LIBE***

Tra questi sistemi rientra sicuramente la cosiddetta "end-to-end encryption" (E2EE), utilizzata attualmente dalle principali app di messaggistica istantanea (citandone una per tutte, Whatsapp, che applica di default tale tecnologia sia ai messaggi che alle chiamate) per codificare le informazioni spedite dal mittente e renderle leggibili soltanto dal dispositivo del soggetto ricevente.

Tramite un sistema di chiavi pubbliche e private, il protocollo di crittografia end-to-end riduce al minimo, di fatto, la probabilità che tanto hackers privati quanto Forze di polizia o Governi possano avere accesso al contenuto delle informazioni che gli utenti si scambiano, così cifrate.

A tal proposito, secondo un'indiscrezione di pochi giorni addietro rilanciata dal sito statunitense "TheNextWeb.com", anche Facebook starebbe sviluppando e testando la

stessa tecnologia per la propria app Messenger, sebbene allo stato solo nella modalità “Secret Conversation” [6]. Infatti, già da marzo 2019, Mark Zuckerberg aveva annunciato il suo piano di voler uniformare le comunicazioni tra Whatsapp, Messenger ed Instagram, garantendo la privacy e la sicurezza degli utenti tramite la E2EE.

***“Le backdoors sono intenzionali vulnerabilità che l’autore del sistema dovrebbe introdurre nel proprio protocollo di crittografia per consentire l’accesso in determinati casi”***

Il dibattito sul tema è particolarmente acceso a livello internazionale e vede contrapposte due principali posizioni: da un lato, quella dei Governi nazionali, preoccupati dal rischio che siano principalmente le organizzazioni criminali e terroristiche a beneficiare di questa generalizzata impermeabilità delle comunicazioni; dall’altro quella delle tech companies, che non vogliono rinunciare alla garanzia di riservatezza e tutela da qualsiasi intromissione esterna promessa ai propri utenti.

In particolare, tiene banco il tema delle cosiddette “backdoors”: si tratta di intenzionali vulnerabilità che l’autore del sistema dovrebbe introdurre nel proprio protocollo di crittografia, fornendone poi la chiave alla forza pubblica così da consentire di accedere, legalmente, ai dati cifrati a fine di indagine e prevenzione di crimini particolarmente gravi.

All’inizio di ottobre, è stata diffusa dalla stampa estera [7] una lettera aperta con cui alcuni esponenti dei governi di Stati Uniti, Regno Unito ed Australia avrebbero chiesto a Facebook di non andare avanti con il piano di implementazione della E2EE sui propri servizi di messaggistica senza assicurare che non ci siano diminuzioni di sicurezza per l’utente e, soprattutto, «senza includere uno strumento per un accesso legittimo ai contenuti delle comunicazioni per proteggere i cittadini» [8].

Il riferimento è proprio alla backdoor, spesso proposta dalle law enforcement agencies quale misura di compromesso: in altri termini, la sicurezza delle comunicazioni è sì garantita a tutti gli utenti, eccezion fatta per un’unica “entrata sul retro” di cui ha la chiave solo l’autorità pubblica, che potrà utilizzarla nei casi di necessità per garantire la sicurezza di utenti e cittadini stessi.

Tuttavia, esiste un primo dubbio logico e giuridico a cui sottoporre tale misura: in un mondo interconnesso, refrattario ai limiti della sovranità nazionale, chi stabilisce quando, come e per quali motivi possa essere necessario – e quindi legittimo – l'utilizzo della backdoor? Appare difficile coniugare l'uso di uno strumento così invasivo con princìpi che non abbiano una forte diffusione ed approvazione, ma che anzi molto spesso sono legati al bilanciamento tra potere dello Stato e diritti fondamentali dell'individuo.

E ciò tanto più quando, in assenza di confini fisici, le nostre democrazie sono esposte alle ingerenze di paesi stranieri: la crittografia, infatti, non può essere solo percepita come un ostacolo all'attività investigativa o all'attività di Intelligence, ma anche come un imprescindibile strumento di difesa per la democrazia e per il diritto di libera manifestazione del pensiero.

D'altra parte, esiste anche un dubbio scientifico e tecnologico sulla sicurezza di tale strumento: secondo gli esperti di sicurezza, è infatti impossibile garantire un accesso limitato alle comunicazioni criptate senza indebolire complessivamente la funzionalità della tecnologia e, quindi, la privacy degli utenti.

Una diatriba, dunque, che non sembra di facile e prossima risoluzione.

Anche per tale ragione, il crescente rischio del going dark ha da tempo imposto alle law enforcement agencies di fare ricorso a differenti tecniche di hacking, sia per bypassare la crittografia sia per conseguire migliori risultati investigativi, che prescindano dalle tradizionali tecniche, come ad esempio le intercettazioni "classiche".

Sebbene gli Stati siano restii ad utilizzare tale terminologia (i.e. tecniche di hacking), si tratta proprio di questo: sfruttare ogni possibile vulnerabilità di un sistema informatico, sia essa tecnica, di sistema e/o umana per accedere ai dati e alle comunicazioni dei soggetti su cui si indaga [9]. Nel concetto di hacking rientra infatti «qualsiasi attività tecnica che richieda specifiche e avanzate competenze e che sia finalizzata a superare le misure di protezione (e prendere il controllo) di un sistema informatico altrui» [10].

Tra le tecniche maggiormente utilizzate rientra il ricorso agli ormai noti captatori informatici: che siano chiamati trojan, virus spia o intrusori, l'inoculazione di questo malware – anche e soprattutto da remoto – all'interno di un

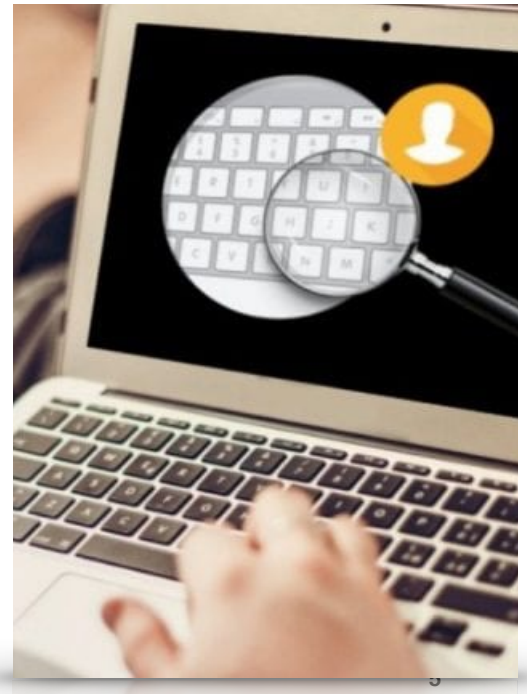
dispositivo bersaglio permette agli autori dell'attacco di prendere possesso del device infettato. In questo modo, quindi, l'accesso ai dati non avviene "dall'esterno" – laddove, quindi, incontrerebbe il limite della crittografia – ma si realizza, a tutti gli effetti, "dall'interno": infatti, poiché non si intercetta il messaggio in transito bensì il messaggio sul dispositivo mittente o sul dispositivo destinatario, non è necessaria la decodifica.

***"Il captatore informatico è un malware che clandestinamente e silenziosamente più introdursi da remoto in qualsiasi dispositivo connesso alla rete"***

Il captatore informatico altro non è che un software (per la precisione, un malware [11]) che, clandestinamente e silenziosamente, può introdursi da remoto in qualsiasi tipo di dispositivo informatico, purché connesso alla Rete: smartphone, laptop, Pc, Smart Tv, automobili, assistenti vocali [12], dispositivi wearable per l'health care, console per i videogames.

Ma come funziona un captatore? Possiamo distinguere due "moduli" principali del software malevolo: un client, con cui è possibile gestire da remoto le attività che si faranno compiere al target, ed un server, che è invece il programma che viola le difese del bersaglio e si introduce all'interno dello stesso [13]. Quest'ultimo, una volta introdotto all'interno del dispositivo da colpire, inizierà a dialogare con l'hardware come se fosse l'amministratore di sistema, scalando i privilegi necessari e prendendo di fatto l'intero controllo del sistema stesso.

L'attività più complessa nell'introduzione del captatore è sicuramente rappresentata dall'installazione del server, poiché – in assenza della materiale disponibilità del dispositivo da infettare – quest'ultima deve avvenire con la necessaria, ancorché inconsapevole, collaborazione del proprietario del dispositivo. Egli, ignaro di tutto, procede all'aggiornamento automatico di un'applicazione, apre una mail che funge da esca, scarica un contenuto grafico ricevuto tramite una "catena di Sant'Antonio", oppure effettua il download di tool disponibili sugli stores: così, di fatto, viene aperta la strada all'introduzione del captatore.



Alla vastità di dispositivi attaccabili dai virus spia, corrisponde un altrettanto ampio range di attività che gli stessi possono compiere sui sistemi infettati: attivazione del microfono e della videocamera; tracking del segnale GPS del

dispositivo; screenshot e screencast dello schermo, keylogger (ossia possibilità di "tracciare" la pressione dei tasti digitati sulla tastiera del dispositivo, così da carpire, ad esempio, le password digitate), visualizzazione di tutti gli scambi di messaggi, informazioni e file tramite le app di messaggistica istantanea; per giungere alla quasi "banale" perquisizione della memoria fisica dei dispositivi.

Due sono le macro-categorie di attività investigativa: le attività di online search, che prevedono la copia totale o parziale dai dati contenuti sul dispositivo target; le attività di online surveillance, che prevedono la captazione del flusso di informazioni che transita tra le periferiche (microfono, webcam, tastiera, ecc.) ed il processore del dispositivo, tutto recepito in tempo reale dal sistema di controllo remoto [14].

Sostanzialmente, tramite il cosiddetto RCS (Remote Control System) il malware prende possesso di ciò che infetta e dispone di tutto quanto lo stesso faccia, contenga, comunichi. In altre parole, consente un livello di intrusione nella vita degli individui ben più pervasivo di quello teorizzato dai fautori della più cupa letteratura distopica.

Nel nostro Paese, l'Autorità giudiziaria e la Polizia giudiziaria già da tempo si servono dei cosiddetti "captatori informatici" a fini investigativi: dal caso Bisignani alla recente vicenda che ha coinvolto parte della magistratura romana, la cronaca giudiziaria e politica del nostro Paese è piena di riferimenti alle applicazioni di tale sistema.

D'altronde, gli utilizzi "giudiziari" del captatore non sono gli unici: è soprattutto l'Intelligence a doversi necessariamente servire di questo mezzo straordinario, che consente un'azione preventiva più che mai effettiva.

Di conseguenza, già dagli anni Dieci del XXI secolo è emerso nel dibattito giuridico nazionale ed internazionale il tema dei cosiddetti "Trojan di Stato", affrontato anche in Italia prima a livello giurisprudenziale e poi, ancorché solo parzialmente, a livello legislativo. Tuttavia, è fuorviante parlare di "Trojan di Stato" poiché, attualmente, il nostro Paese non dispone di una propria tecnologia, sviluppata in via autonoma o gestita in via diretta ed esclusiva, ma si serve di software prodotti da privati, anche stranieri.

***"Oggi è fuorviante parlare di Trojan di Stato poiché il Paese non dispone di una tecnologia sviluppata e gestita in via autonoma ma si serve di software prodotti da privati "***

Le recenti vicende giudiziarie hanno ridato vigore ad una discussione mai sopita: fino a che punto è ammissibile l'uso degli intrusori e quali sono le attività consentite? Quali sono i pericoli per i diritti degli individui? Ma, soprattutto, qual è il rapporto tra limite normativo e limite tecnico?

Di fronte al potenziale di invasività dei captatori, l'attuale

legislazione italiana ha limitato il proprio intervento normativo ad uno specifico e circoscritto utilizzo dello strumento: il D. Lgs. 216/2017, infatti, disciplina una nuova forma di intercettazione tra presenti, ossia quella «che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile». In altre parole, dal punto di vista legislativo, ci si è preoccupati di regolamentare in maniera puntuale l'impiego del captatore informatico per registrare le conversazioni cosiddette "ambientali", ascoltate grazie all'attivazione del microfono del dispositivo infettato.

La riforma ha raccolto alcuni degli auspici dell'ormai celebre sentenza a Sezioni Unite della Corte di Cassazione (che si era trovata ad affrontare l'"affaire" captatori con riferimento alle intercettazioni ambientali "itineranti") [15]: ed infatti, l'uso del captatore a fini di intercettazione ambientale rivoluziona la concezione di intercettazione tra presenti, non più associata ad un luogo specifico in cui installare la microspia, ma legata ad un dispositivo mobile, che il soggetto intercettato porta con sé nei luoghi più diversi.

Tra questi rientrano anche i luoghi in cui è preclusa, salvo particolari eccezioni, l'attività captativa "ambientale": si tratta dei luoghi di privato domicilio, tutelati dalla garanzia costituzionale di inviolabilità di cui all'art. 14 della Costituzione.

È così che la nuova legge introduce la sostanziale utilizzabilità dei captatori ai fini predetti tanto per i reati comuni, quanto per i più gravi reati di criminalità organizzata e terrorismo: tuttavia, solo rispetto a questi ultimi è consentito un uso ubiquitario del mezzo di ricerca della prova [16], mentre negli altri casi è previsto che il giudice debba specificamente indicare, nel provvedimento autorizzativo, tempi e luoghi di attivazione del microfono, escludendo quelli di "privata dimora" ex art. 614 c.p. [17].

I casi di applicazione del captatore sono stati poi ampliati dalla Legge "Spazzacorrotti", che ha previsto l'indiscriminata utilizzabilità dello strumento anche per alcuni reati contro la pubblica amministrazione [18].

A complicare ulteriormente le cose, c'è il fatto che il cosiddetto "Decreto Intercettazioni" non sia ancora completamente applicabile; la riforma, infatti, è stata prorogata per la terza volta ed acquisterà piena efficacia dal 1° gennaio 2020 [19].

*“In assenza di una valutazione globale sulle potenzialità tecniche del captatore si sta di fatto realizzando una atomizzazione delle sue funzionalità, attraverso categorie tradizionali ed analogiche ”*

Pertanto, confrontandosi con uno strumento complesso, pervasivo e potenzialmente ubiquitario, la legislazione si è esclusivamente preoccupata di regolamentare le attività che lo stesso può realizzare. Anzi, una sola attività: l’attivazione del microfono a fini di intercettazione “tra presenti”.

In assenza di una valutazione globale sulle potenzialità tecniche dello strumento, si sta di fatto realizzando una “atomizzazione” delle funzionalità del captatore (uso del microfono per intercettazione, copia dei dati da remoto per la perquisizione, ecc.), cercando di incasellare ognuna di esse in tradizionali categorie processuali e mezzi di ricerca della prova di carattere “analogico”.

In ragione di tali presupposti, le principali carenze normative si concentrano proprio sull’analisi e conseguente disciplina del funzionamento tecnico dello strumento: su questo aspetto, il decreto ministeriale del 20 aprile 2018 [20], che mirava a disciplinare gli aspetti “tecnici” relativi alla riforma delle intercettazioni, non è andato esente da critiche, poiché privo di indicazioni puntuali e tendente all’impiego di formule generiche.

L’eccessiva astrattezza del citato comparto normativo (che più dovrebbe avvicinarsi ad un disciplinare tecnico) si può sintetizzare in un dato esemplificativo: l’art. 4 del decreto – norma deputata a stabilire i requisiti tecnici dei programmi informatici – da un lato richiede che i software impiegati siano periodicamente adeguati agli standard più recenti di funzionalità ed operatività tecnica, dall’altro non prevede nessun sistema di controllo, inteso quale fase di verifica ed approvazione dei programmi utilizzati [21].

Nell’aprile del 2019, è stata l’Autorità Garante per la protezione dei dati personali a criticare il contenuto del citato decreto ministeriale (oltre che, più in generale, l’intera predisposizione della riforma): con una lettera rivolta ai Presidenti di Camera e Senato, al Presidente del Consiglio dei Ministri ed al Ministro della Giustizia, l’Autorità ha rimarcato una serie di criticità dell’attuale riforma sui captatori informatici, rese ancor più preoccupanti dalla nota vicenda “Exodus” (all’epoca appena esplosa) [22].

Il Garante ha evidenziato innanzitutto come «alcuni agenti intrusori sarebbero, infatti, in grado non solo di "concentrare", in un unico atto, una pluralità di strumenti investigativi (perquisizioni del contenuto del pc, pedinamenti con il sistema satellitare, intercettazioni di ogni tipo, acquisizioni di tabulati) ma anche, in talune ipotesi, di eliminare le tracce delle operazioni effettuate, a volte anche alterando i dati acquisiti».

Tre i rischi principali denunciati: in primo luogo, il pericolo della sorveglianza massiva.

In assenza di regole puntuali e appositi divieti, non esiste un argine effettivo con cui impedire che il malware sia liberamente disponibile, ad esempio, sugli stores online per il download di applicazioni: tale criticità parrebbe essere emersa in maniera dirompente nel caso “Exodus”, dove, la disponibilità “aperta” sugli stores di app contententi il virus spia e liberamente scaricabili da tutti i soggetti (in assenza di filtri necessari a limitarne l’acquisizione) non restringeva l’inoculazione al soggetto (e quindi al dispositivo) nei cui confronti eseguire l’attività, ma esponeva un numero indiscriminato di utenti.

Secondo aspetto allarmante concerne la conservazione dei dati: in attesa dell’attuazione del cosiddetto “Archivio riservato delle intercettazioni” presso le Procure, il ricorso a “sistemi cloud per l’archiviazione” in server delocalizzati in Stati extra Ue (sempre citato in relazione al caso Exodus) genera un’importante violazione sia dei diritti degli interessati, che della stessa «efficacia e segretezza dell’azione investigativa».

Ed infatti, l’attuale necessaria dipendenza da sistemi di terze parti non consente un governo diretto e certo da parte dell’Autorità pubblica delle modalità di data storage: pertanto, il rischio che la riservatezza degli individui sia esposta, anche e soprattutto in contesti al di fuori dell’orbita europea, è più che mai concreto.

E tale timore è destinato ad aumentare, se si esce dal confine dell’attività giudiziaria in senso stretto: infatti l’accertamento giudiziario consente potenzialmente all’individuo, prima o poi, di sapere di essere stato intercettato e, quindi, di poter quantomeno conoscere che tipo di attività sia stata eseguita.

Se, invece, volgiamo lo sguardo all’attività di prevenzione, lo scenario si fa più inquietante: pur in presenza di norme “interne” che impongono la distruzione degli esiti di intercettazioni preventive (art. 226 commi 3 e 3 bis disp. att.), noi non avremo mai la garanzia della loro eliminazione, se le stesse sono transitate (e magari ancora risiedono) in server collocati all’estero.

Pertanto, ognuno di noi corre il rischio che i risultati di captazioni *ante delictum* tramite trojan, anche se eliminate dall’autorità pubblica, rimangano comunque in circolazione. E

questo in assenza di qualsiasi tipo di controllo o anche astratta consapevolezza in capo a chi sia stato intercettato.

Ma l'aspetto più preoccupante riguarda la verificabilità delle attività che il trojan può compiere a seguito dell'avvenuta inoculazione, ad oggi non sufficientemente garantita: lo sconfinato potenziale degli intrusori, infatti, non esclude in potenza che lo stesso strumento venga utilizzato per eliminare contenuti presenti sul dispositivo, per simulare conversazioni o scambi di informazioni, oppure, più in generale, per "creare" materiale ad hoc.

È il rischio della "junk science", che dovrebbe essere combattuto perseguendo la completezza e la veridicità del materiale investigativo raccolto sul "sistema ospite": in che modo? Ad esempio, garantendo esplicitamente la tracciabilità effettiva delle operazioni eseguite, tramite i file di log e l'univoca riconducibilità degli stessi ai singoli operatori intervenuti nell'attività.

Certo, non tutti hanno ritenuto effettivo il rischio di "contraffazione" del dato raccolto dal trojan: poiché, infatti, l'attività del malware dovrebbe comunque fornire il medesimo risultato dell'intercettazione tradizionale (comunicazioni a voce tra individui), si potrebbe sempre ricorrere, durante il processo, agli strumenti tradizionali (perizia e trascrizione delle intercettazioni) per verificare l'attendibilità del materiale "audio" raccolto [23].

Questa considerazione consente di introdurre un ulteriore tema di riflessione: sebbene non ancora completamente in vigore, l'attuale normativa ha fornito una disciplina in tema di captatori utilizzati a fini di intercettazione. E cosa accade per tutti gli altri utilizzi? Ad esempio, può essere utilizzato il captatore per le perquisizioni online da remoto?

***"L'aspetto più preoccupante riguarda la verificabilità delle attività che il trojan può compiere a seguito dell'avvenuta inoculazione, ad oggi non sufficientemente garantita "***

Ebbene, in assenza di norme in materia, l'attuale indirizzo della Corte Suprema di Cassazione [24] riconosce l'utilizzabilità di questa nuova tecnica investigativa, tramite l'istituto della "prova atipica": da un lato, essa non rientra in attività di intercettazione (poiché si tratta di un flusso unidirezionale di dati), dall'altro non rientra nella tradizionale attività di perquisizione, che prevede la partecipazione consapevole del soggetto sottoposto all'atto invasivo della propria sfera strettamente personale.

Infatti, ancorché in assenza di un "appiglio" normativo, la disciplina processuale italiana riconosce la possibilità di ricorre a strumenti investigativi "nuovi" per l'accertamento dei fatti: tuttavia, numerosi studiosi

contestano questa scelta, evidenziando che un simile strumento di ricerca della prova è, per sua natura, lesivo di alcuni diritti fondamentali dell'individuo, tra cui rientra il cosiddetto "domicilio informatico" ex art. 14 Cost. o addirittura un più generale diritto alla "libertà informatica", declinato come sviluppo della personalità dell'individuo [25].

Riconoscendo infatti la rilevanza costituzionale dei beni giuridici che si sottopongono a compressione tramite il ricorso a tali attività investigative, si dovrebbe garantire una disciplina "forte" del nuovo strumento, che dovrà essere necessariamente sottoposto ad una riserva di legge (e quindi dovrebbe essere puntualmente disciplinato a livello legislativo) e di giurisdizione (e, quindi, il suo utilizzo dovrebbe essere sempre autorizzato da un giudice).

Nonostante il fervente dibattito giuridico, c'è comunque la possibilità che il captatore venga impiegato per attività investigative escluse da precisi perimetri normativi, come segnalato per le perquisizioni online.

Questa situazione accresce la necessità di ripensare l'approccio giuridico e normativo allo strumento dei trojan: fino ad oggi, la legislazione nazionale ha ritenuto di poter bilanciare il rapporto tra potere investigativo dello Stato e diritti dell'individuo, disciplinando le singole funzionalità tecniche azionabili tramite il captatore.

In realtà, un corretto processo di bilanciamento dovrebbe muovere dall'analisi tecnica dello strumento, in quanto fortemente limitativo delle libertà fondamentali di ognuno non tanto e non solo per il risultato che fornisce, ma per le modalità con cui ambisce a tale risultato.

Infatti, non si può pensare di regolamentare uno strumento così pervasivo solo in relazione ai risultati giudiziari e di intelligence ottenibili grazie alle sue funzionalità, rischiando di precipitare nel riduzionismo giuridico che circoscrive la valutazione della norma alla sola sua efficacia, trascurandone giustizia e validità.

Il funzionamento del captatore (sin dalla sua attività di "attacco intrusivo") impatta sui diritti fondamentali e sulla riservatezza degli individui: il monito lanciato dall'Autorità Garante ha rinvigorito ulteriormente le tesi dei principali studiosi di "digital forensic", i quali, praticamente da sempre, sostengono che il tema dei captatori sia "intrinsecamente tecnico" [26].

L'argine più sicuro per i nostri diritti è costituito da regole puntuali ed effettive che forniscano una disciplina globale dello strumento, che non sia parcellizzata rispetto ai suoi risultati e che trovi nel bilanciamento costituzionale il criterio guida e limite.

Lo strumento andrebbe quindi innanzitutto regolamentato nei suoi aspetti di funzionamento tecnico e, solo successivamente, inserito in un quadro normativo che introduca dei limiti giuridici rispetto al suo utilizzo ed ai risultati della sua attività.

Tuttavia, l'approccio finora utilizzato è stato esattamente quello contrario.

*Prof. Avv. Roberto De Vita*

*Avv. Antonio Laudisa*

# RIFERIMENTI

[1] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices – Study for the LIBE Committee – 2017.
[2] IACP Summit Report. Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence – 2015, "Going Dark is a term used "to describe [the] decreasing ability [of law enforcement agencies] to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks".
[3] https://www.fbi.gov/services/operational-technology/going-dark
[4] Ibidem, "data at rest—court-ordered access to data stored on devices, like e-mail, text messages, photos, and videos".
[5] Ibidem, "data in motion, such as phone calls, e-mail, text messages, and chat sessions".
[6] https://thenextweb.com/facebook/2019/10/31/facebook-is-testing-end-to-end-encryption-for-secret-messenger-calls/
[7] https://www.buzzfeednews.com/article/ryanmac/bill-barr-facebook-letter-halt-encryption
[8] https://www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption
[9] Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices – Study for the LIBE Committee – 2017.
[10] G. Ziccardi, Parlamento Europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche, Archivio Penale n. 1/2017; G. Ziccardi, Hacker – Il richiamo della libertà, Marsilio, 2010.
[11] Secondo il Cambridge Dictionary il malware è un "software that is designed to damage the information on other people's computers and prevent the computers from working normally". https://dictionary.cambridge.org/dictionary/english/malware.
[12] La SRLabs (società tedesca che si occupa di sicurezza informatica e che fornisce consulenza alle aziende) ha dimostrato come attraverso le app (sviluppate da terze parti) di estensione delle skills degli smart speakers (in particolare di Amazon Echo e Google Home) si possano eludere abbastanza agevolmente gli ordinari sistemi di tutela della privacy e controllo. Così, dopo aver chiesto al nostro assistente vocale il nostro oroscopo oppure di dirci un numero a caso, continuiamo ad essere ascoltati. Infatti, nonostante ci siamo preoccupati di dare il comando "stop", il microfono rimane attivo, carpendo le nostre comunicazioni. https://srlabs.de/bites/smart-spies/, https://www.ilpost.it/2019/10/22/assistenti-vocali-sicurezza/
[13] O. Calavita, L'Odissea del Trojan Horse. Tra potenzialità tecniche e lacune normative, Diritto Penale Contemporaneo, n. 11/2018, p. 51.
[14] M. Griffo, Una proposta costituzionalmente orientata per arginare lo strapotere del captatore, Diritto Penale Contemporaneo, n. 2/2018; M. Torre, Il captatore informatico, Giuffrè, 2017.
[15] Cass. SS. UU. n. 26889 del 1 Luglio 2016, "Scurato".
[16] Come previsto dal comma 2 bis dell'art. 266 c.p., introdotto dal D. Lgs. n. 216 del 2017.
[17] Ai sensi dell'art. 266, comma 2 c.p., l'intercettazione nei luoghi ex art. 614 c.p. "è consentita solo se vi sia fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa".
[18] Si tratta dei delitti commessi dal pubblico ufficiale e puniti con una pena massima superiore ai 5 anni di reclusione; cfr. comma 2 bis dell'art. 266 c.p., modificato nella seconda parte dalla Legge n. 3 del 2019.
[19] Art. 9, comma 2 del D.L. n. 53 del 2019, "Rifissazione e proroga di termini in materia di protezione di dati personali e di intercettazioni"
20] Art. 7 del D. Lgs. 216 del 2017: "Con decreto del Ministro della giustizia, da emanare entro trenta giorni dalla data di entrata in vigore del presente decreto, sono stabiliti i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante inserimento di captatore informatico su dispositivo elettronico portatile".
[21] M. Torre, D.M. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico, Diritto penale e processo n. 10/2018, p. 1255 ss.
[22] Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, 30 Aprile 2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9107773
[23] M. Torre, D.M. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico, Diritto penale e processo n. 10/2018, p. 1255 ss.
[24] Cass. Sez. V n. 16556 del 14.10.2009; Cass. Sez. V n. 48370 del 30.05.2017.
[25] Per una panoramica sul tema, M. Griffo, Perquisizione informatica…e dintorni, Giurisprudenza penale web n. 5/2019. M. Bontempelli, Il captatore informatico in attesa della riforma, Diritto Penale Contemporaneo, 20 Dicembre 2018.
[26] R. Brighi, Funzionamento e potenzialità investigative del malware, Nuove norme in tema di intercettazioni, Giappichelli, 2018, p. 211ss.; Ziccardi, Il captatore informatico nella Riforma Orlando: alcune riflessioni informatico-giuridiche, Archivio penale, 2018, Speciale Riforme.