I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo*

Barbara Indovina

Abstract

Lo scritto analizza il funzionamento dei c.d. captatori informatici recentemente introdotti nell'ordinamento italiano con il d.lgs 216/2017 analizzando, in particolare, la pervasività di tale strumento investigativo.
Il testo prende in considerazione sia l'aspetto prettamente tecnico sia quello giuridico ripercorrendo le diverse pronunce giurisprudenziali che hanno portato il legislatore a inserire i captatori informatici come mezzo di ricerca della prova nel codice di procedura penale.

The article concerns the functioning of the so-called Trojan horse malware, recently regulated in Italy by Law 216/2017 examining, in particular, the pervasiveness of the use of this investigative tool.
The essay analyzes both technical and legal aspects of such use retracing the judgments that led the Italian parliament to regulate Trojan horses in the Italian Criminal Procedure Code under the chapter relating to the gathering of evidence.

Sommario

1. Qualche premessa tecnologica. – 2. I captatori informartici: cosa sono e come funzionano. – 3. L'acquisizione delle informazioni contenute sul dispositivo elettronico. – 4. La nuova disciplina su intercettazioni (e captatori).

Keywords: Prova, Captatori, Trojan horse, Intercettazioni, Riforma Orlando

1. Qualche premessa tecnologica

Una storica sentenza della Corte Suprema Usa del 2014 (*Riley v. California*)[1] ha stabilito che per ottenere una perquisizione su un telefonino, anche in caso di arresto, è necessario un mandato giudiziario *ad hoc* questo perché, si legge: «Ormai il 90% degli americani ne possiede, contengono una trascrizione digitale di ogni aspetto delle loro vite, dai più banali ai più intimi, sono una parte pervasiva e onnipresente della vita quotidiana; un marziano sbarcato sulla terra potrebbe pensare che il telefonino è un pezzo importante

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".
[1] www.documentcloud.org/documents/1208245-riley-v-california.html.

dell'anatomia umana»[2]. E ancora il Giudice relatore John G. Roberts Jr. così argomenta la propria decisione: «perfino la parola telefonino ormai è inadeguata, fuorviante. Li potremmo chiamare videocamere, videoregistratori, agendine personali, calendari, librerie, diari, album, televisioni, mappe, giornali».

Niente di più vero e appropriato.

La tecnologia ormai pervade la nostra quotidianità: strumenti quali computer, smartphone, navigatori GPS, macchine fotografiche digitali trattano e raccolgono innumerevoli dati personali e tracce digitali che consapevolmente o inconsapevolmente rilasciamo quotidianamente.

I moderni smartphone, in particolare, contengono numerosissimi dati e diversi tipi di informazioni tutti allocati su un unico dispositivo: informazioni che prese singolarmente o anche combinate tra loro possono fornire una serie innumerevole di risultati. Basti pensare che su un unico dispositivo conteniamo l'elenco dei nostri contatti, messaggi, registro chiamate, video, dati di navigazione, dati relativi alla geo localizzazione, mail, più tutta una serie di dati raccolti dalle più svariate applicazioni (le c.d. "app").

Dati che spesso, soprattutto se combinati con ulteriori *device* quali, ad esempio, gli Smart watch, possono rilevare anche importanti dati connessi al nostro stato di salute e alle nostre abitudini quotidiane.

È indubbio ritenere che negli ultimi anni gli smartphone e, più in generale, gli strumenti informatici (pc, tablet etc.) siano stati un preziosissimo strumento a fini investigativi: la *digital forensics*[3] è largamente utilizzata a fini investigativi praticamente sempre, in qualsiasi indagine, proprio attesa la quantità di dati contenuti in un singolo device utili a ottenere (a volte fondamentali) indizi e prove.

La Convenzione del Consiglio di Europa sul *cyber crime*, poi ratificata dal legislatore italiano con l. 48/2008, ha introdotto nuove regole processuali applicabili alla ricerca e susseguente acquisizione delle prove elettroniche nel procedimento penale.

Negli ultimi anni, proprio alla luce della pervasività degli strumenti informatici, il dibattito tra privacy e sicurezza è più che mai acceso: le nuove tecnologie consentono una trasmissione e conservazione sempre maggiore di dati personali e questi dati sempre più spesso vengono visti come informazioni necessarie a fini investigativi o, ancor maggiormente, a fini di sicurezza e contrasto e prevenzione alla criminalità.

È sempre più difficile bilanciare questi aspetti così compenetrati: il caso Apple/FBI[4] ha portato all'attenzione internazionale proprio il difficile equilibrio tra sicurezza, investigazioni e tutela della privacy degli utenti; e soprattutto si è iniziato a parlare di

[2] *Such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.*

[3] La *digital forensics* è una branca delle scienze forensi che attiene al reperimento, recupero e analisi investigativa del materiale digitale utile a fini investigativi allocato in dispositivi digitali.

[4] Nel febbraio del 2016 l'FBI ha chiesto ad Apple di poter accedere al contenuto del cellulare di uno degli attentatori della strage di San Bernardino del dicembre 2015 mediante una *backdoor* ovvero una "porta di accesso" che fosse in grado di aggirare le tecniche di cifratura poste a tutela di ogni *device* Apple.

crittografia[5] e tecniche di cifratura, argomento fino a quel punto ignorato anche da gran parte degli addetti ai lavori.
Solo pochi anni prima lo scandalo Datagate/Prism aveva fatto emergere il problema della sorveglianza globale delle comunicazioni e dei dati tramite internet e fornitori di servizi elettronici.
I sistemi operativi degli smartphone di ultima generazione hanno previsto (da una data versione in poi) dei sistemi di cifratura così che il loro contenuto diventi ineleggibile da chi non è in possesso della password di sblocco.
Non solo smartphone ma anche alcune app quali, ad esempio, il più diffuso sistema di messaggistica istantanea "Whatsapp[6]", hanno introdotto sistemi di cifratura (*end to end*) volti a garantire la segretezza delle comunicazioni: comunicazioni non solo effettuate via messaggistica testuale ma anche relative alla telefonia e video chiamate.
La cifratura *end to end* è stata via via implementata da pressoché tutte le piattaforme di messaggistica e comunicazione: dapprima Whatsapp, poi Facebook messenger, poi Allo di Google ed è notizia di questi ultimi giorni che anche Skype ha implementato tale tecnologia: mentre in alcune piattaforme prevedono di default il sistema di cifratura (Whatsapp e Signal, ad esempio), in altre piattaforme è l'utente che decide di iniziare una conversazione cifrata (ad esempio in Telegram o Messenger "chat o conversazione segreta").
Le moderne comunicazioni elettroniche, quindi, a differenza di ciò che succedeva un tempo con le comunicazioni telefoniche e di messaggistica istantanea, mediante l'utilizzo di tecniche di cifratura sono, allo stato, inintelligibili qualora intercettate nel loro flusso: da questa doverosa premessa tecnologica è necessario partire per comprendere l'importanza dei nuovi strumenti di captazione che vengono inseriti direttamente nei dispositivi a valle, quindi, del processo di criptazione dei dati in entrata e uscita.

2. I captatori informartici: cosa sono e come funzionano

I captatori informatici sono dei software definiti quali virus (termine usato volgarmente per indicare dei *malicious software-malware*) atteso il loro scopo intrusivo e volto a carpire informazioni nel dispositivo ove vengono rilasciati (iniettati): da tale accezione i più autorevoli esperti hanno coniato il nome di "trojan di stato".
La tipologia di malware è infatti quella definita come "*trojan horse*": come il celeberrimo "cavallo di troia" tali malware si nascondono all'interno di altri programmi apparentemente innocui e vanno a infettare la macchina bersaglio.
Il captatore informatico non viene individuato dai sistemi antivirus dei *device* ove viene allocato in quanto utilizza delle tecniche di inoculazione e/o mascheramento, ossia un pacchetto offensivo in grado di infettare vari tipi di *device* e sistemi di escalation dei

[5] La crittografia (dall'unione di due parole greche: κρυπτός [kryptós] che significa "nascosto", e γραφία [graphía] che significa "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo (da Wikipedia).

[6] www.whatsapp.com/security/?l=it

privilegi, tipici di un *rootkit*, in grado altresì di eludere i sistemi di rilevamento e dare all'intrusore accesso da remoto al contenuto del dispositivo.

Tali software quindi si comportano come programmi di *backdoor* (come abbiamo accennato sopra in relazione al caso Apple/FBI), ossia rendono possibile connettersi in modalità remota al dispositivo "infetto".

I captatori vengono iniettati sfruttando una vulnerabilità all'interno del sistema operativo bersaglio non conosciuta nemmeno agli sviluppatori del programma definita comunemente "0-day"[7], talvolta, unitamente a tecniche di *social engineering*[8] che utilizzano metodi di comunicazione e di persuasione al fine di ottenere o compromettere informazioni personali riguardanti individui o società, tramite un vero e proprio studio di ogni soggetto da intercettare.

Il captatore viene generalmente inoculato con diverse modalità:

- mediante posta elettronica: il malware appare come un allegato apparentemente innocuo di posta elettronica;
- mediante web: il virus è trasmesso tramite un download effettuato dall'utente da una pagina web;
- mediante trasferimento fisico tramite CD-ROM o un'unità USB da collegare all'apparecchio da infettare;
- mediante infezione dall'esterno attraverso connessione dal provider di telecomunicazioni, falsi update o siti civetta, oppure tramite *IMSI Catcher*, anche portatili, che permettono alle forze dell'ordine di portare attacchi di tipo "*man-in-the-middle*" (MTM)

Una volta inoculato all'interno del sistema il captatore può assumere diverse forme e svolgere diverse attività e funzioni, tra le quali:

- raccogliere email, SMS, cronologia telefonica e lista dei contatti;
- intercettare ciò che viene digitato sulla tastiera (*keylogger*);
- visualizzare la cronologia delle ricerche web e "catturare" le schermate visualizzate sul dispositivo;
- registrare le telefonate effettuate anche mediante applicazioni o programmi (Skype etc.);
- usare i telefoni per intercettazioni di tipo ambientale con attivazione del microfono;
- mettere in funzione la foto-videocamera di telefoni o computer;
- sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati.

Le operazioni svolte dal captatore rientrano, quindi, per loro natura in quelle attività di "intercettazioni di comunicazioni" ricollegabili alla disciplina di cui agli artt. 266 ss. c.p.p., alla luce dell'interpretazione offerta dalle Sezioni Unite della Corte di cassazione[9] relativamente alle operazioni con carattere occulto e clandestino, avvenute anche

[7] Il termine "*zero-day*" viene utilizzato perché il programmatore del codice vittima dell'attacco ha zero giorni per poter correggere il prodotto dopo che questo viene attaccato sfruttando una sua vulnerabilità intrinseca.

[8] Nel campo della sicurezza informatica le tecniche di ingegneria sociale permettono lo studio del comportamento individuale di una persona al fine di carpire informazioni utili.

[9] Cass. pen., sez. un., 28 maggio 2003, n. 36747, in *Guida al diritto*, 2003, 42 ss.

tramite tecnologia informatica o telematica.

3. L'acquisizione delle informazioni contenute sul dispositivo elettronico

La cifratura delle moderne comunicazioni elettroniche richiede che l'acquisizione delle informazioni contenute sul *device* avvenga mediante l'acquisizione diretta del supporto informatico non cifrato (*rectius* mediante sequestro), o tramite intercettazione a monte dei flussi di comunicazione attraverso software in grado di captarli.
Come sopra evidenziato gli smartphone di ultima generazione sono cifrati mediante codice di accesso e/o codice biometrico (impronta digitale o altro dato biometrico come ad esempio l'ultimo modello della Apple iPhone X, il riconoscimento facciale dell'utente).
Un aspetto interessante fino ad ora mai preso in considerazione dal nostro legislatore, a differenza di altri legislatori come ad esempio quello statunitense, è che non vi è alcun obbligo da parte dell'indagato di rivelare il proprio codice di accesso o le proprie password di de-criptazione; l'indagato ha sempre la facoltà di non rispondere e/o di non dire il vero.
Non solo: le password di accesso dello smartphone se digitate erroneamente per diversi tentativi possono portare alla disabilitazione del telefono con perdita dei dati in esso allocati.
Un sequestro può, quindi, risultare vano attesa la complessità e, talvolta, l'impossibilità di recuperare informazioni custodite all'interno del computer o nello smartphone dell'indagato.
L'utilizzo dei captatori informatici è una tecnica investigativa che potenzialmente può ovviare a tale problema di acquisizione materiale mediante sequestro di un supporto che poi risulta essere non intellegibile e sta diventando l'unico strumento utile per acquisire gran parte del traffico dati che transita mediante IP.
Ancor più quando si consideri l'utilizzo ormai massivo di sistemi di *cloud computing* che garantiscono la fruizione on-line di tecnologie e risorse informatiche con servizi come quelli di archiviazione con conseguente pressoché totale assenza di dati allocati su di un singolo dispositivo.
Sia che il dispositivo venga sequestrato che si agisca mediante captatori è indubbio che gli investigatori vengano a conoscenza di una serie di informazioni (soprattutto se si considerano gli smartphone) che spaziano dalla corrispondenza (e-mail), agli SMS, ai dati di spostamento e geolocalizzazione, al registro chiamate, ai dati bancari, ai documenti.
Dati che vengono acquisiti, quindi, o con sequestro del dispositivo o mediante intercettazione con inoculazione e attivazione del captatore informatico.
Se è vero che mediante captatore informatico vi è una attività di intercettazione di una molteplicità di dati (da qui le grandi preoccupazioni relative ad una corretta regolamentazione legislativa di tali programmi) è pur vero che la stessa cosa può dirsi relativamente al sequestro di un *device*: mediante sequestro dello smartphone (conoscendone la password di sblocco) è possibile accedere a una infinità di dati ivi stanziati.
Tuttavia è innegabile che anche mediante captatore è possibile prendere cognizione di

tutta una serie di dati che sono allocati sul dispositivo ai quali si ha accesso e di cui si può disporre l'acquisizione (dati GPS, vecchie conversazioni e chat, mail).
I nuovi strumenti tecnologici hanno messo a dura prova legislazione e giurisprudenza nell'adattare vecchi strumenti a nuovi problemi e tecnologie: il captatore può svolgere le più disparate attività e a ciascuna di esse possono ricondursi diverse attività investigative riconducibili a pressoché tutti i mezzi di ricerca probatoria disciplinati dal codice di procedura penale.
Numerosi sono stati gli interventi giurisprudenziali volti a fare luce su diverse problematiche afferenti proprio la qualificazione delle diverse attività del captatore in relazione, innanzitutto, alla definizione di cosa sia una attività di intercettazione, alla tipologia di dati presenti su un singolo supporto (equiparabili o meno ad analoghi strumenti analogici) e al loro utilizzo probatorio come ad esempio in tema di pedinamento elettronico (mediante attivazione di GPS) o sequestro di corrispondenza telematica (e-mail) o SMS e chat.
Un captatore può effettuare intercettazioni telematiche (carpire il traffico in entrata e uscita), intercettazioni ambientali (mediante l'attivazione del microfono), effettuare videoriprese, tracciare il movimento mediante GPS; e lo fa mediante una intrusione in un domicilio informatico (tutelato dalla Costituzione come tutelata è la riservatezza dei dati ai sensi dell'art. 8 CEDU).
Una attività tipica del captatore informatico è, infatti, quella di consentire la geolocalizzazione con conseguente possibilità di monitoraggio via GPS dei movimenti del dispositivo intercettato: la giurisprudenza di legittimità sul punto ha caratterizzato tale attività come un mero pedinamento (digitale), e quindi atto atipico di indagine che non rientra nel novero delle intercettazioni.
Il dibattito su tali aspetti tecnologici e giuridici non è ancora sopito anche perché dalle diverse soluzioni interpretative dipendono gravi conseguenze relative anche all'utilizzabilità dei dati acquisiti nella fase investigativa: e nuove problematiche si presentano di continuo.
Pochi giorni dopo la Sentenza Scurato la pronuncia della Corte di cassazione sul caso Occhionero-Eyepyramid, andando oltre i limiti delineati dalla sentenza delle Sezioni unite, ha analizzato un caso di captatore installato su un pc fisso che svolgeva attività di intercettazione telematica (*ex* art. 266-*bis* c.p.p.) e che acquisiva, altresì, screenshot dello schermo del PC controllato qualificando tale ultima attività come atto di perquisizione/ispezione.
Perquisizione occulta, peraltro, e sfornita di tutte le garanzie difensive previste.
E ancora, una delle prime pronunce di legittimità relativa all'utilizzo dei captatori informatici è stata la sentenza "Virruso[10]" relativamente a un captatore in grado, semplicemente, di prelevare e copiare alcuni documenti memorizzati sull'hard disk dell'apparecchio in uso all'indagato: il P.M. titolare delle indagini aveva disposto tale attività ai sensi dell'art. 234 c.p.p. come acquisizione documentale e la Suprema Corte aveva ricondotto le risultanze investigative nell'alveo delle prove atipiche perché l'attività del Pubblico Ministero aveva avuto ad oggetto non un flusso di comunicazioni, ma «una relazione operativa tra microprocessore e video del sistema elettronico», ossia un'attività confi-

[10] Cass. pen, sez. V, 14 ottobre 2009, n. 16556, *CED* 246954.

nata esclusivamente all'interno del dispositivo acquisita poi come mero documento.
Alla luce della più recente giurisprudenza come quella appena citata, tutto ciò che è contenuto in uno smartphone e non sottoposto a captazione di flusso (intercettazione) è teoricamente visualizzabile e, quindi, acquisibile come mero documento (informatico): nel codice di procedura penale non esiste la definizione di cosa sia un documento informatico ma è obbligatorio il rimando a l'unica giuridicamente fondata ovvero quella prevista dal Codice dell'Amministrazione Digitale (d.lgs. 82/2005 e successive modificazioni) secondo cui è documento informatico «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».
Così anche sms e chat ritenute non meritevoli della tutela costituzionale e processuale relativa alla corrispondenza (art. 15 Cost e artt. 254 ss. c.p.p.) atteso che la più recente giurisprudenza sul punto[11] ha stabilito che «Non è applicabile la disciplina dettata dall'art. 254 cod. proc. pen. in tema di sequestro di corrispondenza, bensì quella prevista dall'art. 234 stesso codice, concernente i documenti, con riferimento a messaggi WhatsApp e SMS rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi, non costituendo il diretto obiettivo del vincolo, non rientrano neppure nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito».
Tale orientamento è stato confermato da altra, recentissima, sentenza[12] secondo cui «I dati informatici acquisiti dalla memoria del telefono in uso all'indagata (sms, messaggi whatsApp, messaggi di posta elettronica "scaricati" e/o conservati nella memoria dell'apparecchio cellulare) hanno natura di documenti ai sensi dell'art. 234 c.p.p. La relativa attività acquisitiva non soggiace né alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni telefoniche. Secondo l'insegnamento della Corte di legittimità non è applicabile la disciplina dettata dall'art. 254 c.p.p., con riferimento a messaggi WhatsApp e SMS rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi non rientrano nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito (Sez. 3, n. 928 del 25/11/2015, dep. 2016, *Giorgi*, Rv. 265991). Non è configurabile neppure un'attività di intercettazione, che postula, per sua natura, la captazione di un flusso di comunicazioni in corso, mentre nel caso di specie ci si è limitati ad acquisire ex post il dato, conservato in memoria, che quei flussi documenta».

4. La nuova disciplina su intercettazioni (e captatori)

Negli ultimi anni sono stati diverse le proposte volte a normare una così difficile materia come quella dei captatori informatici: innanzi tutto il d.l. 18 febbraio 2015, n. 7 "Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione

[11] Cass. pen., sez. III, 25 novembre 2015, n. 928, *CED* 265991.

[12] Cass. pen., sez. V, 16 gennaio 2018, n. 1822, in *Processo Penale e Giustizia.*

alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione", convertito successivamente con la l. 43/2015. che inizialmente prevedeva la modifica dell'art. 266-*bis* c.p.p. prevedendo di poter eseguire intercettazioni informatiche anche «attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico».

Una proposta scarna, insufficiente che aveva destato numerose perplessità negli addetti ai lavori e che fu stralciata in sede di conversione della legge.

Tentativi simili furono effettuati rispettivamente dalle proposte di legge C. 3470 del 2 dicembre 2015 e C. 3762 del 20 aprile 2016.

Quest'ultima, in particolare, promossa dal deputato Stefano Quintarelli dal titolo «Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali»[13], è stata redatta dopo un lavoro di quasi due anni che ha coinvolto un gruppo di esperti "giuridici e tecnologici" e poi sottoposto a consultazione pubblica.

Tale proposta di legge prevedeva:

- una definizione ben precisa dei reati per i quali sarebbe stato possibile l'uso dei captatori;
- la previsione che la richiesta di poter utilizzare un captatore a fini intercettivi dovesse essere redatta dal Pubblico Ministero e convalidata da un giudice, il quale avrebbe disposto quindi «l'osservazione dei dispositivi installati e l'acquisizione da remoto dei dati contenuti», aggiungendo inoltre che il decreto autorizzativo dovesse essere notificato all'indagato entro 40 giorni dall'inizio dell'attività captativa del trojan;
- l'introduzione dell'art. 254-*ter* c.p.p., come nuovo mezzo di ricerca della prova denominato «osservazione e acquisizione da remoto»;
- la necessità dell'esecuzione materiale delle operazioni di intercettazione solo tramite la polizia giudiziaria e non tramite soggetti terzi;
- il necessario possesso, da parte dei captatori informatici, di determinati requisiti, «requisiti stabiliti con regolamento del Ministro della Giustizia, di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali», prevedendo in particolare un sistema di omologazione dei captatori affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e, allo stesso tempo, la creazione di un Registro Nazionale dei Captatori informatici prevedendo altresì il diritto per la difesa dell'imputato di ottenere la documentazione relativa a tutte le operazioni effettuate con il captatore informatico, dalla sua installazione fino alla sua rimozione, garantendo anche la verifica del codice sorgente per escludere manipolazioni.

La riforma attuata dalla l. 23 giugno 2017, n. 103 (Riforma Orlando) "Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario" ha previsto un apposito punto della delega all'art. 1, c. 84, lett. *e)* relativo ai criteri direttivi da seguire nel «disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili».

L'attuazione del predetto punto è stata inserita nell'art. 4 del d.lgs. 216 del 29 dicembre

[13] www.civicieinnovatori.it/wp-content/uploads/2017/02/2017.01.31-09_20-Conf.-stampa.pdf

2017; nella relazione illustrativa dello schema del decreto legislativo viene posto l'accento sulla novità di tale strumento investigativo e si evidenzia la pervasività di detto strumento: «l'utilizzo del cosiddetto "trojan" – o, appunto, captatore informatico –, pur ampiamente praticato nella realtà investigativa, non è stato in precedenza oggetto di alcuna regolamentazione a livello normativo. Come noto, si tratta di un malware occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva, il quale consente in ogni momento all'attaccante di captare tutto il traffico dati (sia in entrata che in uscita), di attivare da remoto il microfono e la telecamera registrandone le attività, di "perquisire" gli hard disk e di fare copia integrale del loro contenuto, di intercettare tutto quanto digitato sulla tastiera, di fotografare le immagini ed i documenti visualizzati».

Il *focus* del legislatore è incentrato, innanzi tutto, sul luogo ove le intercettazioni a mezzo captatore possono essere effettuate, limitandosi a codificare la giurisprudenza della Corte di legittimità[14].

Il nuovo art. 266 c.p.p., rubricato "Limiti di ammissibilità", prevede che l'attivazione del dispositivo è sempre consentita nel caso si proceda per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater* c.p. mentre, fuori da tali casi, nei luoghi di cui all'art. 614 c.p. soltanto qualora vi sia il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

Difformemente dalla decisione delle Sezioni unite n. 26889 del 2016 che considerava una definizione estensiva di reato associativo andando a comprendere qualsiasi forma di associazione a delinquere, il legislatore del 2017 ha previsto i limiti di cui all'art. 51 commi 3-*bis* e 3-*quater*.

Il nuovo testo dell'art. 266 c.p.p., c. 2, quanto ai requisiti di ammissibilità, prevede che nei medesimi casi di cui al c. 1 «è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

Il c. 2-*bis* del medesimo art. 266 c.p.p. disciplina poi che «l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater».

Una prima perplessità è sulla locuzione "dispositivo elettronico portatile" che si presterà sicuramente per la propria ambiguità a interpretazioni difformi e che chiude le porte a qualsiasi tipo di attività captativa su dispositivi che portatili non sono: il legislatore segue il solco tracciato dalle Sezioni unite della Cassazione (Scurato) sul tema delle operazioni di intercettazioni "tra presenti" da svolgersi nei luoghi di privata dimora, effettuate proprio a mezzo di captatore informatico installato su un dispositivo portatile con attivazione del microfono trascurando tutti gli altri possibili utilizzi del trojan a fini investigativi.

Il *focus* del legislatore avrebbe dovuto essere un altro, come nella accennata proposta

[14] E. Jannuzzi- A. Regi, *Riforma Orlando e captatori informatici: il difficile compito del Legislatore nel riuscire a stare al passo con la tecnologia*, in www.medialaws.eu, 23 ottobre 2017.

di riforma Quintarelli, al fine di normare e disciplinare uno strumento così invasivo considerandone tutte le potenziali implicazioni.
Ed è indubbio ritenere che la giurisprudenza di legittimità, se pur attraverso poche pronunce, ha negli ultimi anni approfondito la tematica dei captatori informatici comprendendo molto meglio l'ampiezza del problema rispetto al più recente legislatore, passando da una loro qualificazione come fonti prove atipiche a un tentativo di fornir loro una definizione e una copertura normativa quali mezzi di ricerca della prova.
Il legislatore, invece, nonostante il fermento giurisprudenziale dello scorso anno con le sentenze Scurato e Occhionero, non ha fornito una adeguata copertura normativa alle diverse tipologie di attività svolte dai captatori come avrebbe potuto e dovuto fare.
I software captatori sono utilizzati da più di un decennio a fini investigativi e da ancor più tempo a fini di *surveillance* e spionaggio: a parere di chi scrive i tempi erano maturi per definire e normare per lo meno le più utilizzate attività del software-spia fornendo diversi livelli di pervasività dello strumento in relazione alla tipologia di reato e alla sua gravità alla luce del principio di proporzionalità.
La più attenta dottrina[15] e le associazioni forensi ben avevano illustrato la criticità del ricondurre uno strumento così invasivo e tecnico (non si dimentichi che ci si muove all'interno dell'alveo della prova scientifica) nell'area delle prove atipiche ma così, allo stato, sarà, con conseguente lesione dei diritti difensivi in capo all'indagato.
Al P.M. è concesso, peraltro, di procedere con decreto motivato nei casi di urgenze demandando tale attività di captazione (avvio e cessazione) anche a persone idonee di cui all'art. 348, c. 4, c.p.p.: molto diverso da quella riforma Quintarelli che prevedeva l'esclusione di tale ultima possibilità proprio attesa la grande pervasività dello strumento e l'opportunità che i dati carpiti dallo stesso fossero in possesso unicamente delle autorità inquirenti.
Non sono stati pochi, negli ultimi anni, i casi di attività di intercettazioni illecite o *data breach* di società fornitrici per le Procure di software spia: sarebbe stato, quindi, opportuno, impedire l'accesso a tali dati a persone estranee all'apparato investigativo.
La riforma in esame appare, allo stato, una opportunità persa di regolare compiutamente tutte le diverse possibilità offerte dalle nuove tecnologie dettando regole chiare e univoche.
Sarà compito esclusivo del Ministero della Giustizia emanare il relativo disciplinare tecnico relativo alla tipologia dei captatori da utilizzare: i disciplinari tecnici nella normazione di materie relative all'informatica giuridica sono una parte fondamentale.
Vedremo se saranno ascoltati tutti i tecnici, consulenti ed esperti che da anni studiano questi programmi e ne conoscono tutte le enormi potenzialità e relativi pericoli e che richiedono, oltre all'emanazione di un disciplinare tecnico, un sistema esterno di verifica, certificazione e trust delle operazioni effettuate[16]: ad una prima lettura della norma il riferimento esclusivo al Ministero della Giustizia sembra escludere tale possibilità.
Per ora nel testo del decreto appaiono solo scarni riferimenti (con la modifica dell'art.

---

[15] G. Lasagni, *L'uso dei captatori informatici (trojans) nelle intercettazioni "tra presenti"*, in *Diritto Penale Contemporaneo*, 7 ottobre 2016.

[16] G. Ziccardi, *Parlamento Europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Archivio Penale*, 1, 2017, 234 ss.

89 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale) al tipo di software utilizzato e al luogo ove lo stesso verrà attivato senza nessun riferimento alla progettazione e alla conformità dello stesso («Quando si procede ad intercettazione delle comunicazioni e conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, il verbale indica il tipo di programma impiegato e i luoghi in cui si svolgono le comunicazioni o conversazioni»).
Nessun accenno appare poi riconducibile direttamente alla conservazione dei relativi file di log: le nuove norme prevedono che « le comunicazioni intercettate sono trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente verso gli impianti della procura della Repubblica. Durante il trasferimento dei dati sono operati controlli costanti di integrità, in modo da assicurare l'integrale corrispondenza tra quanto intercettato e quanto trasmesso e registrato».
Vedremo nel disciplinare tecnico come questi aspetti verranno normati certo è che si parla di requisiti tecnici e non di certificazioni od omologazioni.
Ad ogni modo, allo stato, non vi è alcun accenno a un possibile diritto della difesa di ottenere la documentazione relativa a tutte le operazioni effettuate con il captatore informatico, dalla sua installazione fino alla sua rimozione, garantendo anche la verifica del codice sorgente per escludere manipolazioni.
Staremo a vedere.