QUESITI

GIOVANNI ZICCARDI

Parlamento Europeo, captatore informatico e attività di *hacking* delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche

SOMMARIO: 1. Premessa: lo studio (in corso) della Commissione LIBE del Parlamento Europeo e gli spunti di riflessione. - 2. Il captatore informatico e le attività di *hacking* effettuate dalle Forze dell'Ordine. - 3. La comprensione tecnica degli "*hacking tools*": origini, produttori e caratteristiche. - 4. Un primo punto di dibattito: la segretezza del funzionamento e delle modalità operative di tali strumenti. - 5. Un secondo ambito di discussione: la modularità nell'attivazione delle varie funzioni. - 6. Un terzo argomento: la riproducibilità e la verificabilità delle azioni compiute. - 7. Un quarto tema di confronto: i problemi connessi al codice sorgente. - 8. Alcune considerazioni conclusive.

1. Premessa: lo studio (in corso) della Commissione LIBE del Parlamento Europeo e gli spunti di riflessione.

Nei primi mesi del 2017 la Commissione LIBE ("Libertà civili, Giustizia e Affari Interni") del Parlamento Europeo[1] ha avviato un progetto di studio, denominato "*Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*", mirante a tracciare un quadro ricognitivo il più possibile uniforme per tutti i Paesi europei – oltre ad Australia, Stati Uniti d'America e Israele – con riferimento al cosiddetto "*hacking by law enforcement*", ossia all'utilizzo di strumenti di *hacking* da parte degli investigatori delle Forze dell'Ordine nel corso delle indagini.

Ai generici termini "*trojan*", "*malware*" o "captatore" si è, quindi, preferita l'espressione "*hacking by Law Enforcement*", intendendo per "*hacking*" 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[2]. Nell'ambito investigativo, per "*hacking*" si dovrebbe intendere, a onor del vero, non soltanto la fase iniziale d'inserimento del captatore nel dispositivo preso di mira ("inoculazione"), un momento che può demandare strategie tecniche complesse, ma anche tutte quelle attività di

[1] Le attività della Commissione LIBE si possono seguire al seguente indirizzo: *www.europarl.europa.eu*. Lo studio che dà spunto a questo lavoro è, al momento della redazione del presente saggio, ancora riservato e in una fase embrionale. Sono in corso le prime audizioni di esperti per iniziare a tracciare un quadro comune dell'uso del captatore informatico in Europa muovendo dalle griglie interpretative (e dubbi) che si andranno qui di seguito a illustrare.

[2] Per una comprensione del concetto di "*hacking*" sia consentito il rinvio a ZICCARDI, *Hacker – Il richiamo della libertà*, Venezia, 2010.

"ingegneria sociale"[3] che, tramite l'inganno, permettano di prendere il possesso di un dispositivo remoto, nonché quelle tecniche di OSINT ("*Open Source Intelligence*") che consentano la raccolta utile di informazioni su fonti aperte per cercare di violare, poi, le misure di sicurezza predisposte dal *target*[4].

L'attività di analisi e di confronto della Commissione LIBE è interessata sia all'evidente mutamento in corso del quadro normativo internazionale in questo ambito, sia allo studio di un possibile approccio tecnico, basato su "*best practices*"[5], nella produzione e utilizzo dei captatori informatici: quest'ultimo aspetto è quello che più ci interesserà in questa sede.

Con riferimento al primo comparto di studio, è in corso, come facilmente prevedibile, un'analisi della normativa esistente, delle condizioni in base alle quali simili pratiche investigative sono – o potrebbero essere – permesse (soprattutto in periodi di "emergenza terrorismo"), dei meccanismi di coinvolgimento dell'autorità giudiziaria nelle fasi operative e degli obblighi di autorizzazione e di controllo democratico di tali azioni, oltre a uno studio del rapporto tra mezzi investigativi così invasivi e i diritti fondamentali in un'ottica, evidentemente, di compatibilità con gli stessi e con tutte le garanzie connesse.

Nel secondo momento di riflessione rientrano, invece, gli aspetti più tecnici: i *software* da utilizzare e i loro produttori, le tecniche più comuni adoperate dalle Forze dell'Ordine e dal mondo *hacker*, i *tools* e i metodi attraverso i quali le Forze dell'Ordine potranno attuare pratiche di *hacking*, compreso il modo con cui accederanno a tali mezzi tecnici (se utilizzando esperti *in-house*, o tramite società esterne), il rapporto tra questi strumenti e il mondo della sicurezza informatica e le sue migliori regole[6].

Il primo momento di analisi, più giuridico, è idoneo ad aprire innumerevoli spunti per l'interprete, ed è giusto farne cenno perché costituirà la base per la successiva analisi tecnica. Il giurista si domanda, *in primis*, quali siano le condizioni in base alle quali sarà permessa una simile attività di *hacking* e quale autorità potrà decidere sul punto. Il passo successivo è una riflessione su come saranno documentate procedure così complesse (e su una mole di dati

---

[3] Con riferimento alle più evolute tecniche d'ingegneria sociale e d'inganno in ambito informatico si vedano MITNICK, *L'arte dell'inganno*, Milano, 2013, e ID., *L'arte dell'intrusione*, Milano, 2006.

[4] Con riferimento alle attività di OSINT e, in generale, ad attività d'investigazione e di resistenza/dissidenza elettronica sia consentito il rinvio a ZICCARDI, *Digital Resistance, Liberation Technology and Human Rights*, Berlino, 2012. Per un approccio più tecnico si veda KIDANE MARIAM, RUZZI, SPADA, *OSINT il mondo a portata di click. Breve guida sull'intelligence da fonti aperte*, Roma, 2016.

[5] Da intendersi, in senso lato, come le migliori regole, a volte – ma non necessariamente – formalizzate, da adottare in un determinato contesto secondo le opinioni della comunità scientifica di riferimento.

[6] Sul punto si veda ZICCARDI, *Internet, controllo e libertà*, Milano, 2015.

elevatissima) e, a livello temporale, quali saranno i termini di durata dell'azione del captatore e le possibili estensioni di tali termini in caso di necessità dell'indagine. Infine, l'attenzione sarà sui reati – in base a quali reati si potrà effettuare una simile attività investigativa –, se ci sarà comunque una qualche forma di tutela della parte più privata, o intima, del soggetto e come le informazioni così raccolte dovranno essere presentate e potranno essere utilizzate in giudizio.
La seconda parte dell'analisi della Commissione, focalizzata sui mezzi tecnici, si concentrerà essenzialmente sull'operatore (chi, in pratica, gestirà i captatori e li controllerà da remoto), sulle modalità di violazione dei sistemi altrui e della impostazione e configurazione di questi *tools*.
Un simile approccio, attento anche al lato tecnico, ci pare ideale per svolgere alcune considerazioni che possono essere utili nell'interpretare un fenomeno così complesso.

2. Il captatore informatico e le attività di *hacking* effettuate dalle Forze dell'Ordine

Il tema del captatore informatico è stato trattato con grande attenzione, negli ultimi cinque anni, da giuristi nazionali e internazionali. Di recente, anche il mondo della politica italiana – con un disegno di legge specifico[7] particolarmente attento al lato informatico – si è mostrato interessato non solo alle questioni giuridiche e processualpenalistiche ma, anche, ai temi tecnici, cercando con difficoltà di inserire, nella tradizionale architettura del codice, nozioni non sempre semplici da comprendere per il giurista.
In questa discussione politica che è ancora allo stato embrionale, e che sta attraversando l'Europa, vi è, accanto all'esigenza, richiamata da più parti, di una riforma sostanziale, una discussione sempre più vivace sulla necessità o meno di un *disciplinare tecnico,* ossia di una serie di regole che prevedano una puntuale regolamentazione informatica e telematica di simili dispositivi.
Si è abbastanza concordi, in sintesi, che per garantire un ingresso del captatore informatico in qualsiasi ordinamento in maniera rispettosa dei diritti di libertà sia assolutamente necessario che detto strumento sia ristretto all'interno di ben precise "griglie" anche da un punto di vista informatico, e non solo processuale. Com'è avvenuto, ad esempio, con la normativa sulla *privacy*, dove accanto alle norme sono stati posti degli allegati tecnici, così appare essenziale, a molti, che la norma sia affiancata da specifiche tecniche, elaborate da

[7] Ci si riferisce al progetto di legge "Quintarelli ed altri" sul tema del captatore informatico, presentato il 31 gennaio 2017 dal Gruppo Civici e Innovatori.

tecnici insieme ai giuristi, che creino un sistema di funzionamento efficace e rispettoso dei diritti. Il tutto non soltanto per meglio specificare gli essenziali aspetti della segretezza, della "certificazione" dei prodotti usati e della loro modularità, ma anche per evitare che si generi la possibilità di *non poter contestare* alcuni accadimenti se non si possono conoscere gli strumenti, o se la procedura di sviluppo degli stessi non è stata corretta.

Si anticipa, sin d'ora, che non si tratteranno in maniera approfondita, in questo breve studio, gli aspetti penalistici e processualpenalistici del captatore informatico: già sono stati sviscerati con grande cura dalla migliore dottrina nazionale e internazionale.

Negli anni passati, infatti, gli studiosi hanno già largamente dibattuto attorno ai cambiamenti portati dall'avvento, nel sistema penale, della fonte di prova digitale[8], al rapporto tra la cosiddetta "sorveglianza *online*" e ispezioni, perquisizioni e sequestro probatorio[9], al diritto di difesa e alle relazioni con il reato di accesso abusivo a un sistema informatico o telematico[10], all'importanza di tradizionali e nuovi diritti con particolare attenzione al quadro sovranazionale[11].

L'analisi è, poi, proseguita attraverso raffinati dibattiti sulle difficoltà d'inquadramento delle perquisizioni online e i conseguenti profili di ammissibilità[12], sul rapporto con il progresso scientifico e la necessità di interpretazioni evolutive[13] e sulle relazioni con l'istituto della perquisizione.

Anche la giurisprudenza nel settore *de quo* è stata compiutamente analizzata: la decisione della Corte costituzionale federale tedesca del 2008 a protezione della vita privata del cittadino[14], il vaglio della Corte di cassazione italiana sul tema dell'intercettazione di "chiunque, ovunque e comunque"[15], la sentenza della Corte costituzionale tedesca del 20 aprile 2016 sulle misure di sorve-

---

[8] Cfr. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, 2016, 5, 118 ss.

[9] Cfr. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in questa Rivista on-line, luglio 2016, 348 ss.

[10] Cfr. TROGU, *Le indagini svolte con l'uso di programmi spia (trojan horses)*, in *La giustizia penale nella "rete"*, a cura di Flor, Falcinelli, Marcolini, Milano, 2014, 67-75.

[11] Cfr. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *Diritto Penale Contemporaneo*, 2010, 1 ss.

[12] Cfr. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Diritto Penale Contemporaneo*, 2014, 329 ss.

[13] Cfr. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cassazione penale*, 2015, 2.

[14] Cfr. MARCOLINI, *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Cassazione penale*, 2010, 7/8.

[15] Cfr. FILIPPI, *Il captatore informatico: l'intercettazione ubicumque al vaglio delle Sezioni unite*, in questa Rivista, 2016, 1, 1 ss.

glianza occulta[16], le nuove frontiere delle intercettazioni così come interpretate dai giudici[17], la categoria più generale dei "programmi spia"[18] e l'evoluzione della giurisprudenza di merito e di legittimità italiana sino alla già citata decisione della Corte di cassazione[19].
Infine, diversi studiosi si sono occupati dei rapporti con la privacy, della *data retention* e della tutela della sfera privata[20]; vi è stato, al contempo, un accorato appello di docenti di diritto, dopo la sentenza delle Sezioni unite del 2016, che auspicava un intervento del legislatore per disciplinare la materia. Si sono, infine, affrontati i temi ancora più specifici dell'uso di captatori nelle intercettazioni tra i presenti[21], le difficoltà interpretative contenute nella già citata decisione delle Sezioni unite[22] e l'apparente "sdoganamento" del cosiddetto "malware di Stato"[23].
Pur in attesa di ulteriori pronunce ed, eventualmente, di una legge sul tema, il quadro ci appare, da un punto di vista giuridico, già denso di spunti di discussione.
L'analisi prevalentemente tecnica è stata, invece, inopportunamente trascurata. Eppure, il tema del captatore, per le sue funzionalità così originali anche da un punto di vista informatico, deve essere compreso integralmente.
Ci si propone allora, in queste riflessioni, di muovere l'analisi, per una volta (e prendendo spunto dallo studio della Commissione LIBE) dal lato tecnico, al fine di cercare di costruire un "ponte", che oggi appare un po' debole, tra una reale comprensione dei pregi e dei limiti del captatore e il suo possibile *status* giuridico.

---

[16] Cfr. VENEGONI, GIORDANO, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *www.penalecontemporaneo.it*.
[17] Cfr. MONTEVERDE, *Le nuove "frontiere" delle intercettazioni, in questa Rivista*, 2014, 3. Si veda anche GAITO, FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *questa Rivista* on-line, luglio 2016, 309 ss.
[18] Cfr. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *questa Rivista* on-line, 2014, 1, 1 ss.
[19] Cfr. PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *questa Rivista* on-line, luglio 2016, 354 ss.; cfr anche ABBAGNALE, *In tema di captatore informatico*, in *questa Rivista*, 2016, 2, 1 ss.
[20] Cfr. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, in *questa Rivista*, 2015, 3, 1 ss.
[21] Cfr. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*.
[22] Cfr. TESTAGUZZA, Exitus acta probat. *"Trojan" di Stato: la composizione di un conflitto*, in *questa Rivista*, 2016, 2, 1 ss.
[23] Cfr. DITARANTO, RUGGIERI, CUPELLI, *Nuove tecniche d'investigazione nell'era digitale: il "malware di Stato"*, in *Ciberpazio e Diritto*, 2017, 1, 113 ss.

L'informatica giuridica è la disciplina ideale per illustrare, all'interno degli ambiti del diritto, il lato tecnico della questione oggetto della nostra attenzione, trascurando inutili tecnicismi e prediligendo una valutazione del problema con un costante riferimento ai diritti fondamentali dell'individuo.
Ci viene in aiuto, in questo percorso, la già citata azione del Parlamento Europeo, interessata anche all'aspetto tecnico, e, in Italia, il già accennato disegno di legge che, indipendentemente dal successo che avrà, o meno, nel complesso *iter* legislativo che lo aspetta, prevede alcune linee guida tecniche molto interessanti.
Dal punto di vista informatico-giuridico occorre a nostro avviso ben comprendere, prima di ragionare con riferimento a un'eventuale politica legislativa, quattro punti precisi:

i) la genetica segretezza delle attività di un captatore ("segreto"),
ii) la modularità della sua azione ("modularità"),
iii) la riproducibilità delle operazioni in altra sede ("riproducibilità"), e
iv) la gestione del prodotto, del suo processo produttivo e del suo codice sorgente ("visibilità" e "certificazione").

Una volta analizzati dal punto di vista informatico-giuridico i quattro punti esposti poco sopra, sarà possibile cercare di trarre alcune conclusioni sul punto della invasività / pericolosità degli strumenti di *hacking* e, infine, della verificabilità del loro operato e di eventuali, possibili contestazioni.

3. La comprensione tecnica degli "*hacking tools*"

L'aspetto preliminare più interessante dello studio della Commissione LIBE del Parlamento Europeo è che il tema degli *hacking tools* è stato senza indugio inserito nel più ampio ambito della *sicurezza informatica*.
Ciò significa, in concreto, che le considerazioni che andremo a fare potranno valere sia per quei captatori venduti, ad esempio, esclusivamente alle Forze dell'Ordine, sia per quegli strumenti in pubblica disponibilità che, comunemente, sono usati in tale ambito per azioni di *hacking*. Vi può essere, in definitiva, una commistione e una interazione tra tecnologie proprietarie (e segrete) e tecnologie comuni (e conosciute).
Un captatore informatico, in senso lato, ha la funzione di prendere il completo controllo di un dispositivo preso di mira (*target*) e di trasmettere tutte le informazioni sulle attività che avvengono in quel dispositivo a un terzo che "ascolta". Il dispositivo può essere un telefono, uno smartphone, un tablet, un computer fisso o portatile, una console per videogiochi, un televisore intelligente, un sistema di controllo meccanico e ogni altro strumento programmabile che sia vulnerabile. Gli smartphone e i computer sono oggi, come noto, i

due obiettivi più interessanti.
In termini più tecnici, il captatore è un *software* che cerca di arrivare a un livello di privilegi tale da poter interagire con l'*hardware* come se fosse l'amministratore di sistema ("*root*") e prendere, quindi, il completo controllo del sistema stesso.
Esistono captatori di tutti i tipi e costi: da *software* che per pochi dollari l'anno consentono ai genitori, ai partner o a semplici curiosi di infettare il dispositivo altrui e ottenere informazioni sulle attività del soggetto preso di mira, sino a *software* di estrema complessità e costi che sono mantenuti segreti e venduti soltanto alle Forze dell'Ordine o a Governi.
Un captatore deve essere "inoculato" nel dispositivo, e questa è una fase molto complessa, dal momento che non è sempre detto che si sia in possesso "fisico" dello strumento. Lo strumento di *hacking* deve poi essere connesso a una rete mobile (per trasmettere a flusso continuo i dati delle attività su quel dispositivo), deve essere invisibile (soprattutto non deve essere rilevato da antivirus o da controlli effettuati sui processi di sistema attivi), non deve rallentare il funzionamento del *target* né aumentare i costi di connessione (per non destare sospetti) e non deve entrare in conflitto con le normali operazioni del dispositivo infetto.
Nella pratica, gran parte dell'investimento per lo sviluppo di un *software* di questo tipo è previsto per mantenere l'*invisibilità*, per renderlo occulto. Il *worm Stuxnet*, che ha attaccato la centrale nucleare di Natanz in Iran danneggiando per diversi mesi le centrifughe e rallentando così il programma nucleare iraniano, era basato su un codice, di origine statunitense-israeliana, che è stato valutato milioni di dollari. Operava, prima di tutto, nascondendosi sui sistemi che attaccava, anche comunicando false informazioni ai tecnici di laboratorio[24].
Un captatore si "pilota", di solito, da un pannello di controllo, che consente numerose opzioni investigative.
Una prima categorizzazione, a nostro avviso, potrebbe raggruppare le attività dei captatori in tre grandi famiglie:

i) operazioni per l'acquisizione delle informazioni scambiate sul dispositivo,

ii) operazioni per il controllo dell'*hardware* del dispositivo, e

iii) operazioni per il controllo dei contenuti (cartelle e file sul dispositivo).

Nella prima categoria rientrano quelle operazioni che acquisiscono tutti i tipi

[24] Con riferimento al caso di *Stuxnet* sia consentito il rinvio a ZICCARDI, *L'odio online*, Milano, 2016.

di informazione che transitano attraverso quel dispositivo: telefonate in entrata e uscita, videoconferenze, *e-mail*, SMS, *chat* di *WhatsApp*, immagini, video, documenti scambiati e pressione dei tasti (per ottenere *password*). Qualsiasi tipo d'informazione digitale, sia già presente, sia in arrivo e in uscita, viene intercettata, acquisita e memorizzata, e il pannello di controllo permette, poi, di disattivare e distruggere il captatore dal dispositivo preso di mira.
Il secondo gruppo di attività tipiche di un captatore permette di prendere il possesso dell'*hardware* e di attivare alcune funzioni – ad esempio il microfono, la telecamera e il GPS – per trasformare il dispositivo in uno strumento capace di fotografare o riprendere l'ambiente circostante, di registrare le conversazioni in prossimità e di localizzare con grande precisione lo spostamento del telefono che, si presume, sia in possesso del soggetto.
Il terzo gruppo di attività permette di modificare lo stato del dispositivo. Posto che il captatore prende il controllo completo del dispositivo, può senza difficoltà cancellare informazioni o inserirne di nuove. Quest'ultimo è l'aspetto, ovviamente, più delicato.
La diffusione di questi strumenti è correlata alla diffusione della crittografia, uno strumento che garantisce una protezione reale del dispositivo e che, tramite un captatore, si può aggirare. Sono, poi, indispensabili per individuare dei dati collocati in servizi di *cloud computing*, dal momento che oggi ci sono sempre meno informazioni sui dispositivi personali e vi è la tendenza a "depositarli" in rete.
Tutti questi tipi di *software* fondano il loro "vantaggio competitivo" non solo sull'esclusività di utilizzo da parte delle Forze dell'Ordine, ma anche sul segreto spesso associato al loro funzionamento. Ciò significa che in molti sanno come funziona in teoria un captatore (o, in pratica, i prodotti più economici e pensati per un'utenza consumer) ma non conoscono esattamente le funzioni di "quel" captatore usato dalle Forze dell'Ordine, soprattutto se lo stesso viene poi modificato o personalizzato. È quindi opportuno avviare il dibattito informatico-giuridico proprio sul punto del segreto.

4. Un primo punto di dibattito: la segretezza del funzionamento e delle modalità operative di tali strumenti.

Il captatore è, per sua natura, un *software* tendenzialmente *segreto*. Segreto nelle sue caratteristiche, segreto nella sua produzione e fornitura, segreto nel codice, segreto nei rapporti commerciali tra aziende e clienti. La segretezza è il valore economico più importante, insieme alla capacità di violare i dispositivi più moderni. In pochi hanno visto realmente come funzioni un captatore, ne conoscono le modalità attraverso le quali memorizza i file e quali possibili-

tà offre affinché gli stessi non siano modificati. Anche una relazione dettagliata delle attività dell'agente si risolve in un elenco di operazioni che mostrano, però, solo la superficie.
La segretezza si origina sin dal primo momento, ossia quando il captatore viene inoculato. Si usano, di solito, metodi quali l'invio di e-mail di phishing o azioni di infezione tramite siti web nel caso non vi sia possibilità di accesso fisico al dispositivo. La segretezza continua anche durante il suo operato, e i risultati non sono spesso verificabili ma occorre prestare fede a un *report* finale sulle attività effettuate.
Posto che molti captatori sono a uso esclusivo delle Forze dell'Ordine, il lato del segreto si unisce a un'indisponibilità, da parte della difesa, dello stesso strumento, che impedisce non solo la possibilità di effettuare dei test ma anche di domandare un confronto tecnico sul *software* stesso, data l'indisponibilità del codice o, ad esempio, la distruzione dell'agente che opera sul computer *target*. Il segreto, infatti, rimane anche al termine dell'operazione, quando il captatore viene eliminato.
Per superare questo alone di segretezza, nel disegno di legge italiano citato si è cercato di "disegnare", da un punto di vista tecnico, come dovrebbe essere il captatore informatico ideale, con le relative modalità operative e con il contorno di centri di controllo e strumenti di garanzia che dovrebbero contribuire a tracciare un quadro più affidabile.
Viene descritto, innanzitutto, un *sistema di gestione*. Tramite tale sistema dovrebbe essere possibile creare nuovi captatori, gestire i captatori già creati e inviati agli obiettivi, gestire in maniera automatica tutte le eventuali comunicazioni a un possibile ente preposto alla conservazione del registro dei captatori, gestire le chiavi crittografiche di comunicazione, verificare che un captatore disponga delle sole funzioni autorizzate e creare il supporto per il deposito del captatore creato nel fascicolo di indagine.
Al primo sistema di gestione si dovrebbe poi affiancare un *modulo captatore*, ossia un *software* che, posizionato nei dispositivi informatici degli obiettivi autorizzati, opera l'acquisizione delle informazioni.
Ai due moduli precedenti si aggiungerebbe, necessariamente, un *sistema di comunicazione*, che potrebbe essere sia "proprio" (ossia il modulo di raccolta dei dati è incorporato nel sistema stesso) sia appoggiato a un sistema esterno, una sorta di centro di controllo autorizzato a ricevere i dati.
Essenziale è, poi, il sistema *d'inoculazione*, che ha lo scopo, si è visto, di installare il captatore sui dispositivi dell'obiettivo autorizzato. Anche questa fase così delicata dovrebbe essere documentata con cura.
Dal punto di vista delle garanzie, la relazione tecnica al disegno di legge sug-

gerisce un sistema di *registrazione*: tutte le operazioni effettuate sul sistema di gestione, dai captatori installati e dagli utenti che accedono ai dati, dovrebbero essere registrate e memorizzate in maniera inalterabile per chiunque, sia gli utilizzatori sia i produttori che hanno sviluppato il *software*. Al fine di fornire tutte le necessarie garanzie, viene suggerito, nel testo, l'uso di firme digitali e di meccanismi di *time-stamping* crittografico unito alla creazione di file di *log* completi e dettagliati.
Proprio sul punto dei file di *log*, visti come ottimali strumenti di controllo, viene delineato un sistema di controllo degli stessi inteso come modulo *software* separato dalla piattaforma, accessibile liberamente e pubblicamente senza autorizzazione alcuna, distribuito dal sito web del produttore del *software*.
Da un punto di vista di politica legislativa, quindi, la natura tecnica del captatore sembra essere inscindibilmente collegata a strumenti di visibilità e di comprensione di cosa si possa definire come captatore e delle sue funzioni primarie.
Già questi primi aspetti dimostrano il rischio della poca conoscibilità di tutte le sue funzioni nel caso il captatore sia mantenuto segreto.
Ulteriori problemi sono creati, però, dal secondo punto, ossia dalla possibilità di un'attivazione modulare dello stesso.

5. Un secondo ambito di discussione: la modularità nell'attivazione delle varie funzioni.

Il secondo punto d'interesse è la cosiddetta *modularità di attivazione*, ossia la possibilità di attivare, "accendere" singole parti del captatore per permettere determinati tipi d'indagine e di acquisizione della fonte di prova con l'effettuazione di operazioni investigative diverse tra loro e, soprattutto, con diversi margini d'invasività.
Non esiste, oggi, strumento d'indagine più potente del captatore se si fa eccezione, forse, per i droni. I moduli attivabili possono consentire un'attività di sorveglianza evoluta, una di sequestro da remoto di documenti, una d'intercettazione di comunicazioni vocali e telematiche, una di controllo ambientale sino a una vera e propria azione di pedinamento via GPS. E più i captatori si evolvono, più si aggiungono "moduli" che aumentano le potenzialità.
La modularità è un aspetto essenziale per cercare di collegare le azioni del captatore alle modalità investigative più "tradizionali" previste nei codici.
In particolare, la discussione verte sulla possibilità di prevedere una specifica attivazione tecnica di ogni singola funzione del captatore in rapporto all'estensione delle richieste d'indagine formulate dall'autorità, evitando al

contempo di attivare *tutti* gli strumenti del captatore nel caso non fossero necessari.
Nel recente disegno di legge italiano che abbiamo citato, ad esempio, si cerca di inquadrare ogni singolo modulo attivabile del captatore nella "griglia" delle categorie giuridiche tradizionali. Un modulo che attivi la possibilità di intercettare il "traffico voce" sarebbe così assimilabile alle intercettazioni telefoniche, l'attività di registrazione di audio e video sarebbe simile alle operazioni d'intercettazione ambientale, l'acquisizione di messaggi di *e-mail* alla intercettazione di corrispondenza, l'uso dei dati di posizionamento per controllare gli spostamenti alla fattispecie del pedinamento, la ricerca di file su dispositivo alla perquisizione, l'acquisizione di file sul dispositivo al sequestro, e così via.
Si potranno attivare e verificare, ci si domanda allora, le singole istanze?
A nostro avviso, un controllo di ogni singola funzione, o istanza, del captatore porterà inevitabilmente a una *burocratizzazione* delle varie operazioni. Si pensi alla necessità di attivare nuove funzioni in corso d'indagine, o in casi di urgenza. Per cui ci pare che l'attivazione modulare di un captatore presenti pregi e difetti. I pregi sono quelli di una possibile *gradualità* nella capacità invasiva e di una limitazione dell'azione a determinati contenuti. Il difetto è che il dato digitale renderà sempre più difficile individuare e separare il tipo d'informazione. Ci sarà una *convergenza* di tutte le informazioni di un soggetto nella categoria del "dato digitale". Si pensi alla difficoltà attuale di distinguere le conversazioni telefoniche da quelle telematiche. Di qui, probabilmente, deriverà la tendenza ad attivare *tutte* le funzioni, subito, per garantire risultati ad ampio spettro o una raccolta dei dati "a strascico"[25].

6. Un terzo argomento: la riproducibilità e la verificabilità delle azioni compiute.

Una volta risolte le questioni della segretezza delle funzioni e della possibile modularità dell'utilizzo degli strumenti di indagine, occorre affrontare necessariamente il problema tecnico della *riproducibilità* o, comunque, della *verificabilità* delle azioni compiute da un investigatore.
Questo è l'aspetto probabilmente più spinoso, da un punto di vista tecnico. Si deve muovere dalla premessa che, nella maggior parte dei casi, ciò che viene svolto da un captatore o da uno strumento di *hacking* non è riproducibile *esattamente*, sia perché il sistema attaccato è originale, sia perché lo stesso

[25] Modalità di raccolta dei dati degli individui effettuate "a strascico" ed effettuate dalla CIA e dalla NSA sono ben descritte in GREENWALD, *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, Milano, 2014.

viene modificato ma anche i *software* utilizzati possono modificarsi durante l'attività.
In sintesi: è quasi impossibile ricreare un ambiente identico nel quale replicare l'azione investigativa (una sorta di ambiente di *test*) e non è facile entrare in possesso dello stesso, identico programma nella stessa versione, soprattutto se è personalizzata. Senza contare che occorrono competenze tecniche specifiche e una certa abitudine investigativa per usare simili strumenti. I captatori stessi, poi, possono adottare tecniche di polimorfismo (mutano man mano che operano per adattarsi al sistema che devono attaccare) o offuscamento (non appaiono nella loro completezza, operano travisati) per migliorare le proprie capacità di occultamento nei confronti dei *software* antivirus e *anti-malware*. In conclusione: la versione "di partenza" del captatore può essere differente rispetto a quella che si trova installata sul sistema preso di mira.
La possibilità concreta, quindi, anche se si fosse in possesso di un captatore identico a quello utilizzato, di replicare l'azione effettuata, è tendenzialmente negata.
Differente è, invece, la possibilità di richiedere la *verificabilità* delle azioni compiute, ossia poter contare su descrizioni dettagliate delle azioni e del comportamento del captatore.
Su tale punto diventa fondamentale la modalità di raccolta dei dati una volta che viene installato il captatore nel sistema *target*, ossia un tipo di raccolta che memorizzi i dati dell'investigazione con le dovute garanzie. Si pensi, ad esempio, alla possibilità di verificare chiaramente l'identità dell'agente operante, alla tenuta di un registro non solo delle attività effettuate dall'operatore ma anche di quelle generate autonomamente dal *software* per ognuno dei suoi moduli attivati, alla creazione di un supporto inalterabile contenente la copia dei file di log relativi a tutte le operazioni svolte, alla generazione di un secondo supporto contenente tutto il materiale acquisito durante l'indagine, sino a una descrizione dettagliata di come siano avvenute le procedure di disinstallazione del captatore (e la verificabilità di cosa è successo, se il sistema è cambiato).
In questa fase, come è intuibile, sono essenziali i dati contenuti nei file di log e la loro corretta comprensione.
La verificabilità potrebbe essere, infine, anche sul *tipo* di captatore utilizzato, nel caso si sia stabilito per legge l'uso di "captatori certificati".
Da un punto di vista di disciplinare tecnico, e di politica legislativa, occorrerà predisporre un sistema accurato di verifica *ex post* delle azioni di un sistema che *geneticamente* è pensato per occultare, mascherare, ingannare con le sue azioni, che muta nel tempo e che non solo può essere "pilotato" da un essere

umano ma può anche agire in maniera autonoma e rimanere silente per lunghi periodi.
Se può essere impossibile, si diceva, replicare esattamente l'azione di simili strumenti di *hacking*, occorrerebbe in definitiva concentrare l'attenzione (almeno) sulla verificabilità di ogni operazione che hanno effettuato.

7. Un quarto tema di confronto: i problemi connessi al codice sorgente.

Il tema del codice sorgente alla base del *software* captatore e degli strumenti di *hacking* utilizzati si presenta come un argomento cruciale e, purtroppo, di non facile soluzione. Si tratta della tappa conclusiva del percorso costellato di "dubbi tecnici" che si è voluto tratteggiare. Tutti dubbi che dovrebbero, in prospettiva, essere risolti.
Il codice sorgente, con riferimento a un *software* di qualsiasi tipo, è l'insieme di tutte quelle istruzioni, "listati", righe di codice, scelte di programmazione e commenti che costituisce il suo DNA, la sua "ricetta"[26]. In estrema sintesi: per comprendere come operi un *software*, occorre avere l'accesso al suo codice sorgente e poterlo leggere (o farlo leggere a esperti di fiducia). Al contrario, si definisce un *software* "proprietario" un programma che si può solo installare ed eseguire ma del quale non è possibile conoscere il codice che vi sta alla base e, così, comprenderne il funzionamento e le scelte fatte dai programmatori. "Ci si fida", in poche parole, del risultato, senza poter conoscere la procedura e senza poter individuare, ad esempio, funzioni nascoste. L'idea di codice sorgente aperto, o a disposizione della collettività, è collegata all'idea di una possibilità di "scrutinio pubblico" delle funzioni di quel programma, anche in un'ottica di sicurezza. Se il codice è visibile, ci sarà la possibilità, per chiunque dotato di competenze di programmazione, di ricostruire le modalità operative di quel programma.
In un prodotto così delicato come uno strumento investigativo, il conoscere il codice sorgente, per verificarne il funzionamento può assumere un'importanza essenziale. Non è una novità, un simile approccio: il dibattito è stato sollevato, ad esempio, negli Stati Uniti d'America con riferimento al voto elettronico (il poter vedere il *software* delle macchine utilizzate nelle tornate elettorali elettroniche)[27]. I problemi pratici sono gli stessi: sono strumenti che puntano sulla segretezza, sulla protezione del valore industriale e sulla originalità.

---

[26] Un giurista che ben spiega la natura e l'importanza del codice informatico è LESSIG, *Cultura libera*, Milano, 2007.
[27] Si veda, sul punto, il pluripremiato documentario investigativo "*Hacking Democracy*" del 2006 dove vengono illustrate attività di *hacking* su macchine per il voto elettronico.

Il captatore è un *software* che, già per sua natura, deve funzionare in maniera nascosta, surrettizia e personalizzata. Il diffondere il codice sorgente permetterebbe *in primis* di conoscerne il funzionamento e, quindi, di poter approntare contromisure volte a eluderlo o a riutilizzarlo, ad esempio, nei confronti degli stessi investigatori. Una seconda possibilità di garanzia, più tenue, sarebbe quella di non rendere *sempre* disponibile il codice sorgente, ma di farlo solo "all'occorrenza", ad esempio depositandolo presso un notaio o un'autorità in vista di un successivo accesso/controllo nel caso ce ne fosse bisogno. Anche questo non è una soluzione accettata pacificamente dai produttori. Negli Stati Uniti d'America la società *Diebold* si è rifiutata di depositare in molti Stati il codice sorgente delle sue macchine per il voto elettronico.
Le proposte, con riferimento al codice sorgente e alla visibilità della "natura" del captatore, potrebbero essere le più diverse.
Il deposito del codice sorgente e della documentazione tecnica potrebbe, ad esempio, avvenire presso un ente scelto dal produttore stesso, che dia garanzia di protezione del segreto industriale.
Oppure, si potrebbe pensare di consentire l'utilizzo solo di *software* che in precedenza abbia dovuto affrontare un percorso di certificazione che ne verifichi il funzionamento e l'assenza di operazioni nascoste. In questo caso, però, ci si scontrerebbe con la natura stessa di alcuni programmi che mutano durante l'azione o sono pesantemente personalizzati e non più standard, ossia diversi da quelli eventualmente valutati da un certificatore terzo.

8. Alcune considerazioni conclusive

Una corretta, e puntuale, percezione dei multiformi aspetti tecnici alla base della progettazione, dello sviluppo, della commercializzazione e dell'utilizzazione di strumenti di *hacking* a uso dalle Forze dell'Ordine – compresi i cosiddetti "captatori informatici" – è oggi essenziale per evidenziare, sin dalle radici, i problemi di politica legislativa e di tutela dei diritti che sono coinvolti nella regolamentazione di questo delicato, e innovativo, aspetto delle attività investigative[28]. Mai come in questo ambito il lato informatico appare legato a doppio filo alle categorie giuridiche "tradizionali", già previste nei codici, e ai diritti di difesa e di libertà. Nell'analisi che abbiamo condotto, seppur sommariamente, poco sopra, si è cercato di evidenziare alcuni principi che non dovrebbero essere soltanto "regole di buon senso" ma che avran-

[28] Per un quadro – con approccio giornalistico – molto curato della situazione attuale delle cosiddette "guerre dell'informazione", compresi i *malware*, gli *zero day* e il caso della società *Hacking Team* e di altri produttori di captatori informatici si veda FREDIANI, *Guerre di rete*, Roma-Bari, 2017.

no, a nostro avviso, un impatto importante nel quadro giuridico che si sta disegnando in tutta Europa con riferimento all'utilizzo quotidiano di simili strumenti.

La prima considerazione, avviandoci alle conclusioni, è che un *software* che abbia la funzione di fornire, durante le indagini, all'autorità un gran numero di dati (anche) sensibili di un individuo, debba essere in qualche modo, *verificato a priori*, e *verificabile a posteriori*, in ogni sua funzione. Tali dati, infatti, sono estratti da quel complesso di comunicazioni, interazioni ed esercizio della vita sociale che ogni individuo conduce offline e online[29], con il rischio che non vi sia distinzione tra ambito privato e professionale, tra ciò che sia afferente all'indagine e ciò che non lo sia, tra dati che riguardino l'indagato o, al contrario, altre persone che con lo stesso si relazionino per i motivi più vari.

Il captatore e gli strumenti di *hacking* possono superare senza difficoltà le tradizionali categorie "vita privata" e "vita professionale", dati "esistenti" e dati "cancellati", comunicazioni "cifrate" e comunicazioni "in chiaro", soggetti terzi all'indagine e soggetti, invece, coinvolti nel caso: tutte categorie, queste, che hanno sempre cercato di tracciare dei "confini" ben precisi non soltanto con riferimento a un'indagine ma anche alla stessa vita privata, e alla tutela della *privacy*, del soggetto indagato.

Siamo in presenza, già si è detto, di uno strumento caratterizzato da un'invasività che è in grado di "travolgere" ogni barriera, e di carpire qualsiasi tipo d'informazione. Di più: sono strumenti appositamente pensati per aggirare tutti quei sistemi di protezione delle comunicazioni, ad esempio la crittografia, che potrebbero creare problemi nell'acquisizione dei dati.

Essenziale è, quindi, comprendere innanzitutto il "peso" di un simile strumento e le sue capacità invasive; l'unico modo per farlo (non sempre possibile) è quello di vederlo in azione, di studiarne il funzionamento, di conoscerne gli aspetti tecnici, di poterlo sperimentare in ambienti di test, o "asettici", per osservarne i comportamenti.

L'esercizio del diritto di difesa dovrebbe, poi, comprendere la possibilità di ricevere in ogni momento una *descrizione accurata* delle attività svolte dal captatore o da altri strumenti di *hacking* e la certezza che non vi siano state alterazioni della scena del crimine – ad esempio: non siano state immesse nuove informazioni, o cancellati dei dati favorevoli all'indagato – sia da parte degli investigatori sia da parte di terzi, sfruttando le funzioni del captatore

[29] Con riferimento alla presenza dell'individuo in rete e all'insieme delle comunicazioni messe in circolazione quotidianamente, sino a creare nuovi "corpi elettronici", e alla necessità di una protezione sempre più estesa della "sfera elettronica" dell'individuo, si veda RODOTÀ, *Il mondo nella rete*, Roma-Bari, 2015.

stesso.
Le descrizioni accurate delle azioni, e la certezza che non siano avvenute alterazioni, si possono raggiungere soltanto grazie alla tecnologia, utilizzando sistemi di reportistica, di generazione e di custodia dei file di log che siano in grado di documentare in ogni momento l'attività di raccolta delle informazioni e la relativa catena di custodia che si viene a creare. Ci sembra essenziale che una tale attività sia generata dal sistema stesso ma sia, al contempo, sotto il "dominio" di un soggetto terzo che sia l'unico autorizzato a gestire simili preziose informazioni. Si pensi, per fare un esempio nell'ambito della normativa sulla protezione dei dati, alle regole previste per il controllo delle attività degli amministratori di sistema[30] e al classico principio del *Quis custodiet ipsos custodes*.
Circa, invece, le idee di creare *registri elettronici* (che, ad esempio, elenchino tutte le richieste di attività legittime di captazione), di avviare processi di certificazione, di apporre "bollini" al *software* e di obbligare al deposito del codice sorgente, al fine di garantire una trasparenza di tutti i prodotti utilizzati, ci paiono non certo idee peregrine, ma di difficile attuazione nella pratica e di dubbia applicabilità ai singoli casi.
Ci sembra, in particolare, per alcuni versi insuperabile il requisito del *segreto* richiesto dai grandi produttori di captatori, visto l'enorme valore di alcuni prodotti sul mercato internazionale, e l'ovvia importanza che le modalità di attacco, di azione e, soprattutto, di offuscamento dell'azione stessa debbano rimanere occulte per non minare la natura stessa di simili prodotti. Si pensi alle quotazioni attuali, per fare un esempio lineare, degli *zero day*[31] e agli interessi commerciali e politici che ruotano attorno a questo settore (molti dei captatori usati durante le indagini giudiziarie sono simili, nelle funzioni, a quelli usati da Stati autoritari per controllare e perseguire giornalisti, dissidenti e avversari politici, come è successo nel caso della morte di Giulio Regeni).
L'approccio ricognitivo di studio della Commissione LIBE del Parlamento Europeo, e lo spirito alla base del disegno di legge italiano citato, hanno avuto il merito di aprire un nuovo fronte di consapevolezza e di dibattito che ci appare molto interessante. La domanda che appare, sullo sfondo, è la seguente:

[30] Ci si riferisce al provvedimento del 27 novembre 2008 del Garante per la Protezione dei Dati Personali italiano intitolato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
[31] Uno *zero day* è un programma che sfrutta, per accedere a un sistema altrui, una vulnerabilità non ancora nota al produttore e alla comunità tecnica e scientifica. Sono tipi di *malware* che, a seconda dell'obiettivo che potrebbero colpire – un sistema di controllo industriale, ad esempio, o uno smartphone di diffusione mondiale – hanno una quotazione, al "mercato nero", che può arrivare sino a diverse centinaia di migliaia di euro.

come si può arrivare a conciliare la complessità tecnica di simili strumenti con un quadro giuridico che dovrà, necessariamente, disciplinare, prima o poi, il *più potente* mezzo di investigazione e di ricerca della fonte di prova mai esistito?

Ci sembra, per concludere, che un *disciplinare tecnico*, o un insieme strutturato di regole e migliori pratiche informatiche, unito a un sistema *esterno* di verifica, certificazione e trust delle operazioni effettuate con i captatori, debbano essere ormai parti essenziali di una possibile riforma normativa.

Pare di percepire una necessità sempre più sentita che, accanto a una riforma giuridica che sia attenta alle esigenze processuali, di "parità delle armi" nel processo, di tutela dei diritti dell'indagato e della sua *privacy* vi sia anche, parallelamente, la necessità di un urgente processo di elaborazione di *regole tecniche* che stabiliscano, insieme alle regole di diritto, le basi per un quadro globale di garanzia[32].

In un sistema così oscuro, multiforme e complesso, la migliore tecnologia informatica potrebbe, in definitiva, venire in aiuto al giurista non solo al fine di chiarire i dettagli della procedura/azione investigativa ("che cosa avviene realmente quando si utilizzano simili strumenti") ma anche per segnalare *automaticamente* attività, o situazioni, che potrebbero generare elementi di futura, possibile contestazione o che potrebbero essere portate avanti senza rispettare le regole e le garanzie procedurali.

[32] Ciò è già avvenuto, in parte, con la ben nota Legge 48/2008, che ha introdotto nel nostro ordinamento i principi della Convenzione di Budapest sul *cybercrime* relativi alla *digital forensics* e alle *best practices* nell'acquisizione della fonte di prova digitale. Cfr., sul punto, VACIAGO, *Digital evidence, I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012. Per l'analisi delle origini di questo momento di transizione e di nuova percezione dell'importanza del dato digitale anche in ambito processualpenalistico sia consentito il rinvio a LUPÁRIA, ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007.