CAPTATORI INFORMATICI E DIRITTO ALLA DIFESA
IL CASO EXODUS

di Francesca Palmiotto
(*Dottoranda di Ricerca presso lo* European University Institute)

SOMMARIO: 1. Introduzione 2. Brevi cenni in materia di captatore informatico e la sua novella disciplina 3. La vicenda *Exodus* 3.1 Profili di incompatibilità con la disciplina in materia di captatore informatico 3.2 Le attività consentite mediante captatore informatico: alcune riflessioni 3.3 Un esodo dalla legalità 4. La necessità di controllo e di supervisione: la rivalutazione del ruolo della difesa 4.1 Il diritto al contraddittorio nella formazione della prova a livello nazionale ed europeo 4.2 Diritto alla difesa e opacità algoritmica: le nuove sfide al contradditorio 5. Conclusioni (un aggiornamento)

1. *Exodus* è un *malware* utilizzato come captatore informatico per l'esecuzione di intercettazioni.[1] A marzo 2019 vengono pubblicati i risultati delle analisi condotte da *Security Without Borders* su tale software. In tale report ne viene denunciato l'utilizzo a causa della mancanza di un sistema di filtraggio e verifica dei target,[2] che avrebbe così permesso di intercettare illegalmente diverse centinaia di cittadini italiani.[3] Non solo. *Exodus* era anche in grado di attuare attività non consentite, quali l'accesso al microfono e alla telecamera, l'estrazione di dati dal calendario, dalla rubrica, dalla galleria fotografica e da altre applicazioni installate, perfino la registrazione della geolocalizzazione. Quando un potente algoritmo, quale *Exodus*, viene utilizzato per finalità probatorie nei processi penali si pone il problema di controllabilità giudiziale in funzione di garantire non solo l'attendibilità e la legalità dell'accertamento, ma anche e soprattutto l'esercizio del diritto di difesa dell'imputato, in ossequio al principio del contradditorio nella formazione della prova. Nell'ordinamento italiano, nonostante l'impiego di tali strumenti investigativi sia stato oggetto di recenti interventi normativi[4], il ruolo della difesa in qualità di controllore della legalità del procedimento risulta ancora svilito dalla

[1] Un 'captatore informatico' è un mezzo di ricerca della prova disciplinato dagli artt. 266 ss. del Cpp.

[2] Security Without Borders, *Exodus: Nuovo Spyware per Android Made in Italy*, disponibile in https://securitywithoutborders.org/blog/2019/03/29/exodus-ita.html, 29.3.2019.

[3] Ad oggi si ipotizza siano circa 393 soggetti. Si veda C. Anesi, R. Anigius, P. Petrasso, *Exodus, gli affari dietro il malware di stato che spiava gli italiani*, in www.wired.it, 18.11.2019.

[4] La disciplina del captatore informatico è stata recepita dapprima tramite l. 23.6.2017 n. 103, cd. "Riforma Orlando", e con successivo d. lgs. 29.12.2017 n. 216 in attuazione della delega di cui all'art. 1 co. 82, 83 e 84 lett. *a*, *b*, *c*, *d* ed *e* della suddetta legge. Inoltre, il 31.5.2018 è stato pubblicato il decreto ministeriale contenente i «requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore» (art. 4 del d.m. 20.4.2018). Recentemente, tale disciplina è stata ulteriormente modificata mediante d.l. 30 dicembre 2019 n. 161 conv. in l. dalla l. 28.2.2020 n. 7.

opacità che circonda tali strumenti. Con l'espressione "opacità algoritmica" si indicano quelle situazioni dove è noto l'*output* di un algoritmo, ma non come lo stesso sia stato generato. Di conseguenza, in assenza di informazioni circa il funzionamento di uno strumento informatico, utilizzato per finalità probatorie, la difesa non può contestare la qualità della prova assunta per suo tramite.

Il presente contributo sarà così strutturato. A seguito di una breve ricostruzione della disciplina processuale in materia di captatori informatici alla luce del recente intervento legislativo, *Exodus* sarà utilizzato come caso di studio per avviare una più ampia analisi sulle nuove sfide portate dall'utilizzo di algoritmi nel procedimento penale in materia di trasparenza e supervisione degli strumenti investigativi digitali. In particolare, attenzione sarà posta sul diritto alla difesa, analizzando i profili di (in)compatibilità tra opacità algoritmica e i requisiti imposti dal principio del contradditorio in ambito nazionale ed europeo.

2. Un *malware* è un "*malicious software*" in grado di installarsi in un sistema ad insaputa dell'utente per potervi condurre una serie di attività invasive e dannose. Quando tale strumento è utilizzato nell'ambito di investigazioni penali come mezzo di ricerca della prova, viene denominato "captatore informatico" secondo la terminologia del Codice di Procedura Penale.[5] Con il primo intervento legislativo, composto dalla l. 23.6.2017 n. 103 e dal d.lgs. 29.12.2017 n. 216, il captatore informatico è stato considerato come una *species* del più ampio *genus* delle intercettazioni, e quindi regolato nel Capo IV del Titolo III Libro III agli artt. 266 e ss Cpp. Di recente il legislatore è ulteriormente intervenuto *in subiecta materia* mediante d.l. 30.12.2019 n. 161 conv. in l. dalla l. 28.2.2020 n. 7.

Come risultato di una burrascosa *vacatio legis*, caratterizzata da continue proroghe della entrata in vigore dei provvedimenti,[6] ad oggi la disciplina del captatore informatico può essere ricostruita tenendo conto di due diversi archi temporali:

[5] Il termine "captatore informatico" è stato scelto dal legislatore per indicare l'esecuzione di intercettazioni mediante agenti intrusori con l. 103/2017, anche se tale termine è privo di riscontro nella terminologia tecnico-informatica dove tale strumento viene definito genericamente "*malware*".

[6] L'entrata in vigore delle disposizioni relative al captatore informatico, nonché più in generale alla riformata disciplina in materia di intercettazioni, è stata prorogata innumerevoli volte. Dapprima con d.l. 25.7.2018 n. 91 conv. in l. dalla l. 21.9.2019 n. 108; quindi dalla l. 30.12.2018 n. 45 e successivamente dal d.l. 14.6.2019 n. 53, conv. in l. dalla l. 8.8.2019 n. 77; nonché dal d.l. 161/2019 conv. in l. dalla l. 7/2020. Da ultimo, dal d.l. 30.4.2020 n. 28 il quale all'art. 1 co. 1 e 2 ha prorogato l'entrata in vigore delle disposizioni del d. lgs. 216/2017 e del d.l. 161/2019. In particolare, le disposizioni del d.l. 216/2017 si applicheranno ai procedimenti penali iscritti dopo il 31 agosto 2020, così come le disposizioni dell'art. 2 del d.l. 161/2019 (modificativo, ai nostri interessi, degli artt. 266 co. 2 *bis*; 267 co. 1, 2 *bis*, 4 e 5; 268 co. 2 *bis*, 2 *ter*, 4 e che ha aggiunto i commi 5, 6, 7 e 8; art. 269 co. 1, 1 *bis* e 2, e che ha abrogato gli articoli 268 *bis*, *ter*, *quater* Cpp, nonché modificativo dell'art. 89 n. att. cpp), ad eccezione delle disposizioni di cui al comma 6 che sono di immediata applicazione.

a) Per i procedimenti penali iscritti[7] prima del 31 agosto 2020, si applica la disciplina ante l. 103/2017 e d.lgs. 216/2017 (cd. riforma Orlando) e ante d.l. 161/2019 conv. in l. dalla l. 7/2020 (cd. contro-riforma Bonafede);
b) Per i procedimenti penali iscritti dopo il 31 agosto 2020, si applica la nuova disciplina del d. lgs. 216/2017 come modificata d.l. 161/2019 conv. in l. dalla l. 7/2020;

Fatta questa doverosa precisazione, la novella disciplina del captatore informatico, la quale, lo si ripete, si applicherà a tutti i procedimenti iscritti dopo il 31 agosto 2020, può essere brevemente ricostruita come segue.[8]

È dapprima necessario sottolineare che, nonostante le sterminate attività che un *malware* possa effettuare, il legislatore ha scelto di consentirne l'utilizzo per una sola attività: la registrazione di conversazioni tra presenti, *id est* quale intercettazione ambientale. Attraverso l'inserimento del co. 2 all'art. 266 Cpp, in materia di limiti di ammissibilità, l'intercettazione tra presenti potrà avvenire anche «mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile negli stessi casi previsti dal comma 1».[9] Qualora tali comunicazioni avvengano nei luoghi indicati dall'art. 614 del Cp, ossia nei luoghi domiciliari del

[7] Il cambiamento di dicitura da "operazioni di intercettazione relative a provvedimenti autorizzativi emessi" a "procedimenti penali iscritti" lo si deve all'art. 1 del d.l. 161/2019.

[8] Si tiene a precisare che tale breve ricostruzione è esclusivamente funzionale all'analisi del caso Exodus. Per una approfondita disamina della disciplina si veda in particolare G. Lasagni, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, 7 ottobre 2016; M. Torre, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *DPP* 2015, 1163 s; O. Calavita, *L'odissea del* trojan horse. *Tra potenzialità tecniche e lacune normative*, in *DPenCont* 2018 (11), 45 ss.; L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni*, in *DPenCont* 2018 (1), 59 ss. M. Bontempelli, *Il captatore informatico in attesa della riforma*, in *www.penalecontemporaneo.it*, 20 dicembre 2018; M. Senor, *Trojan di Stato: perché serve una base giuridica adeguata*, 18 aprile 2017, disponibile in www.agendadigitale.eu; R. Orlandi, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *RIDPP* 2018, 544 s. Per una ricostruzione sistematica, v. il contributo di S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino 2018. Per un approfondimento sulle novità introdotte dal d. lgs. 29 dicembre 2017 n. 216 si veda D. Pretti, *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in *DPenCont* 2018, (1), 189 ss. e C. Conti, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *DPenCont* 2017 (3), 78 ss. Per ulteriori approfondimenti si veda G. Giostra e R. Orlandi (a cura di), *Nuove norme in materia di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli, Torino 2018; O. Mazza (a cura di), *Le nuove intercettazioni*, Giappichelli, Torino 2018. Si veda inoltre F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. brasileira dir. proc. pen*. 2017, 485 ss. Più specificamente sulla recente riforma Bonafede si v. inoltre D. Pretti, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, in *SP* 2020, 71 ss; G. Pestelli, *La controriforma delle intercettazioni di cui al d.l. 30 Dicembre 2019 n. 161: Una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, in *SP* 2020, 109 ss.

[9] Art. 266 Cpp di recente modificato in sede di conversione del d. lgs. 161/2019 dalla l. 7/2020 che ha inserito la nuova lettera *f-quinquies* includendo così i delitti commessi avvalendosi delle condizioni previste dall'articolo 416 *bis* Cp ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.

soggetto sottoposto ad indagini, l'utilizzo del captatore è consentito solo «se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa» (art. 266 co. 2 *bis* Cpp). Tuttavia, l'utilizzo di captatore informatico, secondo l'art. 266 co. 2 *bis* Cpp,[10] è sempre consentito, quindi anche nei luoghi domiciliari, «nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficialio degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4».[11] Trattasi, in sintesi, dei delitti di criminalità organizzata e terrorismo di attribuzione del Procuratore della Repubblica distrettuale, nonché dei più gravi reati contro la pubblica amministrazione.

Per procedere ad intercettazione ambientale mediante captatore informatico, il pubblico ministero deve richiedere al Gip l'autorizzazione a disporre le operazioni *ex* art. 267 co. 1 Cpp, la quale deve essere data con decreto motivato. In aggiunta alla sussistenza di gravi indizi di reato e alla indispensabilità della intercettazione per la prosecuzione delle indagini, quando lo strumento prescelto è il captatore, il decreto dovrà anche indicare le ragioni che rendono necessaria tale modalità di captazione. In aggiunta, qualora si proceda per delitti diversi da quelli indicati dall'art. 266 co. 2 *bis* Cpp, il Gip dovrà anche indicare i luoghi e il tempo di attivazione del microfono. In casi di urgenza, il pubblico ministero può disporre, sempre con decreto motivato, l'intercettazione con captatore, ma solamente nei casi più gravi indicati dall'art. 266 co. 2 *bis* Cpp e salva la convalida del Gip entro quarantotto ore (art. 267 co. 2 *bis* Cpp). Presenti i presupposti per l'attività investigativa, l'art. 268 Cpp disciplina l'esecuzione delle operazioni di intercettazione.[12] Le comunicazioni captate vengono registrate e documentate mediante redazione di verbale delle operazioni *ex* art. 268 co. 1 Cpp. Tali attività si svolgono sotto la supervisione del pubblico ministero, anche in funzione di tutela della privacy e reputazione dei soggetti intercettati, specie se terzi estranei al procedimento (art. 268 co. 2 Cpp). Anche al fine di rafforzare il ruolo di supervisore del pubblico ministero, viene previsto che le operazioni siano compiute esclusivamente per mezzo di impianti installati nella Procura della Repubblica. Tuttavia, adottando un approccio consapevole della reale condizione di inidoneità tecnologica delle Procure, è possibile utilizzare altri impianti di pubblico servizio o in dotazione alla polizia giudiziaria (art. 268 co. 3 Cpp). Per lo stesso motivo, tenuto anche conto della complessità tecnica delle operazioni effettuate mediante captatore informatico, l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'art. 348 co. 4 Cpp. Non vi è, tuttavia, alcuna indicazione legislativa in merito alle concrete modalità di installazione del suddetto captatore nel dispositivo bersaglio.

[10] Articolo di recente modificato dall'art. 2 co. 1 lett. *c* del d.l. 161/2019 conv. in l. dalla l. 7/2020.

[11] Tale comma è stato aggiunto dall'art. 4 co. 1 lett. *a* n. 2 del d. lgs. 216/2017, successivamente modificato dall'art. 1 co. 4 lett. *a* della l. 9.1.2019 n. 3 e infine dall'art. 2 co. 1 lett. *c* del d.l. 161/2019 conv. in l. dalla l. 7/2020.

[12] Articolo di recente modificato dall'art. 2 co. 1 lett. *e* del d.l. 161/2019 conv. in l. dalla l. 7/2020.

I verbali, le registrazioni (ossia i dati acquisiti) e la documentazione relativa alle operazioni di captazione vengono conservati in un apposito archivio disciplinato dal seguente articolo 269 Cpp, denominato "archivio digitale" dall'art. 89 *bis* co. 1 norme att. cpp,[13] gestito e tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica.[14] Il Gip e i difensori hanno diritto di accesso all'archivio, nonché all'ascolto delle conversazioni o comunicazioni registrate, successivamente al deposito effettuato ai sensi degli articoli 268 Cpp e 415 *bis* Cpp o nel caso previsto dall'articolo 454 co. 2 bis Cpp (art. 269 co. 1 Cpp).[15] Secondo l'art. 89 co. 3, 4 e 5 norme att. cpp, le comunicazioni intercettate sono trasferite *esclusivamente* e *contestualmente* in tale archivio, previa verifica delle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione. Una volta terminate le operazioni, il captatore deve essere disattivato. Il comma secondo dell'art. 269 Cpp, inoltre, stabilisce che il termine di conservazione dei dati corrisponda al passaggio in giudicato della sentenza,[16] ad eccezione dei casi previsti dall'art. 271 co. 3 Cpp. Quest'ultima norma è di particolare rilevanza per la seguente trattazione, in quanto disciplina i casi di divieti di utilizzazione dei dati captati. Come principio generale, sono inutilizzabili i risultati delle intercettazioni eseguite fuori dai casi consentiti dalla legge o qualora non siano state osservate le disposizioni relative a presupposti e forme del provvedimento (art. 267 Cpp) o sulla esecuzione delle operazioni (art. 268 co. 1 e 3 Cpp). Con particolare riferimento al captatore informatico, il comma 1 *bis* stabilisce l'inutilizzabilità dei dati acquisiti nel corso delle operazioni *preliminari* al suo inserimento, nonché dei dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo.

Infine, il recente d.l. 161/2019 conv. in l. dalla l. 7/2020, interviene anche sugli artt. 89 e 89 *bis* norme att. cpp, contenti una disciplina tecnica più dettagliata sulla esecuzione delle intercettazioni. Secondo l'art. 89 co. 1 norme att. cpp, il verbale delle operazioni *ex* art. 268 Cpp, quando si procede a intercettazione mediante captatore, deve indicare anche il tipo di programma impiegato nonché, ove possibile, i luoghi in cui si svolgono le comunicazioni o conversazioni. Le operazioni di "conferimento" (e non più di "trasferimento" come indicato dal d.l. 161/2019) dei dati captati devono avvenire negli impianti della procura della Repubblica e, una volta ultimate, trasferiti da tali server all'archivio digitale di cui all'art. 269 Cpp.[17]

Di estrema importanza è il co. 2 il quale stabilisce che il captatore informatico debba essere conforme ai requisiti tecnici stabiliti con decreto dal Ministero della Giustizia.[18] Lo

[13] Articolo di recente modificato dall'art. 2 co. 1 lett. *f* del d.l. 161/2019 conv. in l. dalla l. 7/2020. Inoltre, gli artt. 268 *bis*, *-ter* e *-quater* in materia di deposito di verbale e registrazioni ed acquisizione al fascicolo delle indagini sono abrogati dall'art. 2 co. 1 lett. *q* del d.l. 161/2019 conv. in l. dalla l. 7/2020.

[14] Si noti, tuttavia, che gli atti ed i verbali ritenuti rilevanti dalle parti, oltre che nell'archivio, possono anche materialmente confluire in copia all'interno del fascicolo delle indagini.

[15] Ultimo periodo aggiunto dalla l. 7/2020.

[16] In ogni caso, qualora i dati siano irrilevanti per il procedimento, gli interessati possono chiederne la distruzione *ex* art. 269 co. 2 Cpp al giudice che ha autorizzato o convalidato l'intercettazione.

[17] Modificato con l. 7/2020.

[18] L'obbligo di conformità con i requisiti tecnici è stato ulteriormente sottolineato in sede di conversione

stesso era già stato previsto del d.lgs. 216/2017, sulla cui base il Ministero della Giustizia aveva emesso il d.m. 20.4.2018, recante all'art. 4 i suddetti requisiti del programma utilizzato come captatore informatico. Secondo l'art. 2 co. 4, 5, 6 del d.l. 161/2019, inoltre, obiettivo del decreto ministeriale è quello di garantire, soprattutto, che tali programmi informatici si limitino all'esecuzione delle operazioni autorizzate.

3. A marzo 2019, *Security Without Borders* pubblica un report sui test condotti su *Exodus*, un *malware* venduto al Ministero degli Interni e ai servizi segreti italiani per essere usato come captatore informatico. Secondo l'inchiesta di Report,[19] *Exodus* sarebbe stato utilizzato da circa il 90 per cento delle Procure italiane per condurre investigazioni informatiche.[20] I risultati delle varie inchieste che si sono susseguite su *Exodus* sono a dir poco sconcertanti.[21] Tale *software* non solo era in grado di controllare moltissime funzionalità del *device* infettato, ma, una volta installata l'applicazione contenente il *malware*, il sistema non verificava se il dispositivo potesse essere legittimamente intercettato o no. In merito, alla data del presente scritto, si ipotizza che quasi quattrocento utenti siano stati intercettati illegalmente.[22] Attualmente gli amministratori delegati e i rappresentati della società eSurv, l'azienda che ha sviluppato tale software, sono coinvolti in una indagine da parte della Procura della Repubblica di Napoli, di Salerno e di Roma. Tra le più recenti ipotesi investigative vi è quella che vedrebbe l'utilizzo di *Exodus* per finalità di dossieraggio e ricatto.[23] I dati acquisiti mediante *Exodus* venivano, infatti, memorizzati all'interno di un unico server Amazon, situato in Oregon. Una volta effettuato il *log in* alla cartella in *cloud*, mediante semplice inserimento di nome utente e password, l'utente poteva avere accesso a *tutte* le intercettazioni effettuate mediante il software, anche relative a procedimenti in corso di altre procure italiane. Secondo quanto ricostruito dalle inchieste giornalistiche, di questi emergono «*screenshot*, brogliacci, registri delle chiamate, rubriche telefoniche e addirittura il grado e il nominativo di alcuni operatori di Polizia giudiziaria, la cui identità era così esposta»[24].

---

mediante la sostituzione del periodo "possono essere impiegati soltanto" del decreto con "devono essere impiegati".

[19] Report, *Infiltrato Speciale*, di Paolo Mondani, puntata del 18.11.2019.

[20] L'utilizzo di *Exodus* come captatore sarebbe inoltre confermato da un documento pubblicato online sul sito della polizia di Stato (disponibile in https://www.poliziadistato.it/statics/21/serv-econ-fin-pagamenti3-1-.pdf), dove eSurv (l'azienda che ipoteticamente avrebbe sviluppato *Exodus*) avrebbe ricevuto un pagamento nel novembre 2016 per l'acquisto di un sistema di intercettazione.

[21] Al tempo del convegno ICONs, non erano ancora chiari i dettagli della vicenda. Risulta doveroso un aggiornamento per il lettore a seguito di una ulteriore inchiesta condotta da Irpi e Wired che hanno svelato inquietanti aspetti legati alla società che ha sviluppato il software. Si veda C. Anesi, R. Anigius, P. Petrasso, *op. cit*.

[22] C. Anesi, R. Anigius, P. Petrasso, *op. cit*.

[23] C. Anesi, R. Anigius, P. Petrasso, *op. cit*.

[24] C. Anesi, R. Anigius, P. Petrasso, *op. cit*.

A seguito di tale grave episodio, nell'aprile 2019 il Garante per la protezione dei dati personali redige una segnalazione rivolta al Parlamento e al Governo[25], al fine di esortare una più ampia riflessione su alcuni possibili miglioramenti della disciplina del captatore informatico. In questo documento, il Garante sottolinea, in particolare, che le caratteristiche innovative dei cd. *malware* siano tali da «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 volta anche alterando i dati acquisiti»[26]. A parere delGarante privacy, la disciplina sul captatore (riferendosi alla riforma Orlando) non è stata in grado di fronteggiare tali difficoltà e di apprestare sufficienti cautele e garanzie per tutelare i diritti individuali. Nei testi definitivamente approvati, infatti, mancherebbe «la previsione di garanzie adeguate per impedire che, in ragione delle loro straordinarie potenzialità intrusive, questi strumenti investigativi, da preziosi ausiliari degli organi inquirenti, degenerino invece in mezzi di sorveglianza massivo o, per converso, in fatti di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio»[27].

3.1. La gravità di tale vicenda può essere meglio compresa attraverso una analisi dei profili di incompatibilità di tale strumento investigativo con gli artt. 266 ss. del codice di procedura penale. Risulta però necessario sottolineare che, dal momento in cui le norme in materia di captatore informatico si applicheranno ai procedimenti iscritti dopo il 31 agosto 2020, l'utilizzo di *Exodus* si inserisce ancora nel panorama normativo ante riforma Orlando e controriforma Bonafede, caratterizzato da pronunce giurisprudenziali, successivamente tendenzialmente recepite dal legislatore. Ciononostante, alla luce della gravità della vicenda,[28] *Exodus* dovrebbe servire, a mio avviso, da test in concreto della adeguatezza delle norme in materia di captatore informatico, soprattutto alla luce del recente intervento normativo. Di seguito, le varie caratteristiche tecniche del software sono descritte e confrontate con le prescrizioni codicistiche.

Inoculazione del malware *in altre applicazioni scaricabili da Google Play Store.* Secondo quanto ricostruito da *Security Without Borders*, *Exodus* era celato in altre applicazioni, apparentemente innocue, disponibili nello *store* di *Android*. Una volta effettuato il *download* di tali applicazioni, il dispositivo veniva così infettato con *Exodus*. In materia di installazione del

[25] *Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*, 30 aprile 2019, in www.garanteprivacy.it.

[26] *Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*, cit.

[27] *Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*, cit.

[28] Denunciata anche dal Garante Privacy in *Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*, cit.

captatore informatico, vi è silenzio normativo circa le specifiche modalità ammissibili. L'unico generico riferimento alla fase di installazione è il disposto dell'art. 268 co. 3 bis Cpp, il quale prescrive che per le operazioni di *avvio* e di cessazione delle registrazioni con captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti, l'ufficiale di polizia giudiziaria possa avvalersi di persone idonee di cui all'articolo 348, co. 4 Cpp. Non vi è dubbio tuttavia che l'occultamento del captatore in applicazioni disponibili nello *store* di Google sia la modalità di installazione meno adeguata per l'esecuzione di intercettazioni mirate, e non a tappeto, quali quelle effettuate dall'autorità giudiziaria.

Mancanza di una "target validation procedure".[29] Il termine *target validation procedure* si riferisce alla procedura di validazione del target in grado di assicurare, attraverso le informazioni ottenute dal *device*, se il dispositivo potesse essere legittimamente infettato o no. Tuttavia, secondo i test condotti da *Security Without Border* – nonostante la raccolta di dati dal dispositivo, quali codice IMEI e numero di telefono, avvenisse – la effettiva validazione del target non sarebbe stata mai effettuata. Inoltre, se si considera anche la circostanza sopra esposta in merito alle modalità di installazione del software (non già attraverso mirati interventi da parte degli operatori, ma anche mediante l'occultamento di *Exodus* in diverse applicazioni presenti nello *store* Google), si comprende la grave portata della mancanza di tale verifica. Di conseguenza, *Exodus* esponeva chiunque scaricasse tali applicazioni ad una intercettazione illegale, condotta sanzionata penalmente dall'art. 615 *ter* Cp. Secondo l'inchiesta di *Wired*, tale circostanza non era frutto di un errore, ma di una precisa scelta della società eSurv. Le informazioni raccolte, infatti, venivano raggruppate in due cartelle: demo e volontari. Quest'ultimi sarebbero stati i soggetti che avrebbero installato *Exodus* per caso e che probabilmente servivano per testarne l'operatività su dispositivi diversi per modello o sistema operativo.[30] Superfluo sottolineare come siffatta attività di intercettazione fosse del tutto illegale, nonché contraria all'essenza stessa degli atti di indagine preliminari i quali devono, per loro stessa natura, essere *ad personam*, specifici e supportati dall'esistenza di una notizia di reato.[31] Ed è in questo che si distingue uno stato di sorveglianza da uno stato di diritto.

In particolare, secondo l'art. 267 co. 1 Cpp è necessaria l'autorizzazione del Gip, data con decreto motivato, il quale verifica la presenza delle condizioni previste dall'art. 266 Cpp

[29] Security Without Borders, *Exodus: Nuovo Spyware per Android Made in Italy*, cit.

[30] C. Anesi, R. Anigius, P. Petrasso, *op. cit*.
Inoltre, nella stessa inchiesta si riporta che, sulla base delle dichiarazioni di un dipendente della eSurv, tale pratica sarebbe stata permessa sulla base di garanzie funzionali. Tali garanzie funzionali sono, secondo Wired, quelle previste dalla legge 3.8.2007 n. 124 per esonerare i servizi segreti e i privati, "*qualora la loro attività sia indispensabile e avvenga in concorso con il personale delle Agenzie*" da responsabilità penali durante l'attività istituzionale.

[31] La notizia di reato, da un punto di vista funzionale, è il presupposto per l'avvio di un procedimento penale, in difetto del quale pubblico ministero e polizia giudiziaria non possono compiere atti d'indagine preliminare. Si veda in tal senso B. Lavarini, *La notizia di reato,* in *Le indagini preliminari e l'udienza preliminare*, a cura di D. Negri, V, in *Trattato teorico pratico di diritto processuale penale*, diretto da G. Illuminati e L. Giuliani, Torino 2017, 2.

dei gravi indizi di reato e della indispensabilità della intercettazione per la prosecuzione delle indagini. Il decreto, inoltre, deve indicare le ragioni che rendono necessario l'uso del captatore informatico come modalità per lo svolgimento delle indagini. Nel d.l. 161/2019, il tema della installazione riceve leggermente più attenzione, laddove modifica l'art. 89 co. 2 norme att. cpp il quale ora dispone che ai fini della installazione debbano essere impiegati solo programmi conformi ai requisiti tecnici stabiliti con decreto dal Ministero della giustizia. Tuttavia, le specifiche modalità di installazione non vengono indicate. Tale omissione è, a mio avviso, particolarmente preoccupante se si pensa al fatto che la sola attività di installazione di un *malware* in un dispositivo costituisca *per se* una compromissione dei diritti individuali, in particolare una violazione del cd. domicilio informatico,[32] nonché una condotta penalmente rilevante ai sensi dell'art. 615 *ter* Cp.

Mancanza di un sistema di disinstallazione del software. Secondo il report di *Security Without Borders*, i dispositivi da loro utilizzati per i test non sono mai stati disinfettati da remoto dagli operatori. Di nuovo, non solo tale circostanza è più genericamente contraria alla essenza stessa delle attività investigative, le quale non possono chiaramente protrarsi *ad libitum*, ma anche specificamente in violazione delle norme che prevedono una durata limitata per l'esecuzione di intercettazioni. In particolare, secondo l'art. 267 co. 3 Cpp, la durata massima delle intercettazioni non può superare i 15 giorni, prorogabili dal giudice con decreto motivato di ulteriori 15 giorni. Inoltre, l'art. 89 co. 5 norme att. cpp (sostitutivo del precedente comma 2 *quinquies*) dispone che al termine della registrazione il captatore informatico venga disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante.

Scarsissimo livello di sicurezza. Il *malware* non solo di fatto esponeva il dispositivo infettato all'attacco di terzi, ma tutti i dati intercettati mediante *Exodus* venivano conservati in un unico *database*, accessibile da qualsiasi dispositivo e *browser*, semplicemente con nome utente e password, senza neanche la presenza di un secondo livello di verifica (ad esempio attraverso inserimento di un codice inviato per SMS). Di conseguenza, chi era a conoscenza delle chiavi avrebbe potuto accedere a informazioni «scottanti per attività di dossieraggio».[33] Secondo l'art. 4 del d.m. 20.4.2018, emanato ai sensi del d.lgs. 216/2017, i programmi informatici funzionali all'esecuzione di intercettazioni mediante captatore sono elaborati in modo da

[32] Per un approfondimento si veda il mio contributo in questa rivista, F. Palmiotto, *Le indagini informatiche e la tutela della riservatezza informatica*, in www.lalegislazionepenale.eu 2019 laddove si afferma che per poter effettuare una corretta analisi degli strumenti investigativi digitali– che sia in grado di proporre soluzioni adeguate alle sfide portate dall'evoluzione tecnologica – risulta fondamentale adottare un approccio unitario e non atomistico e, per quanto possibile, aderente al principio di neutralità tecnica. Il focus deve essere posto non tanto sulla singola tecnologia e sulle singole attività che consente di effettuare, quanto sul bene giuridico da tutelare, individuando tutti i casi in cui questo possa essere potenzialmente leso e prestando maggiori cautele nei casi in cui un terzo estraneo al procedimento possa essere coinvolto. Di conseguenza, ogni fase tecnica di attività investigative di *hacking* dovrebbe essere regolata in quanto lesiva di diversi diritti fondamentali".

[33] C. Anesi, R. Anigius, P. Petrasso, *op. cit*.

assicurare integrità, *sicurezza* e autenticità dei dati captati. Inoltre, l'art. 2 co. 3 del d.lgs. 161/2019, stabilisce che con decreto del Ministro della giustizia saranno stabiliti i requisiti tecnici dei programmi funzionali all'esecuzione di intercettazioni mediante captatore informatico. Tali requisiti, secondo il comma 4, sono stabiliti secondo misure idonee di affidabilità e *sicurezza*, garantendo che tali programmi si limitino alla esecuzione delle operazioni autorizzate.

Trasferimento dei dati su un cloud *Amazon.* I dati intercettati da *Exodus* (ben 80 *terabyte*) venivano trasferiti su un unico server Amazon situato in Oregon (USA). Diego Fasano, ex amministratore delegato della società eSurv, intervistato da Report ha giustificato così la scelta di inviare i dati prima in *cloud* e poi ai server della Procura: «Una cautela che prendevamo noi e che era fondamentale era di mettere in mezzo tra il telefonino che aveva il virus e la procura dei server intermedi. Questa in gergo si chiama catena di anonimizzazione. Perché? Perché questo impediva nel caso in cui l'indagato si fosse accorto del virus, un informatico prendeva il virus e vedeva l'indirizzo IP a cui mandava i dati. Se non ci fossero stati questi server di mezzo avrebbe visto direttamente il server della procura». La legge, tuttavia, dispone che il trasferimento delle registrazioni sia effettuato esclusivamente verso gli impianti della Procura della Repubblica così da garantire originalità e integrità delle registrazioni, senza server intermediari, tantomeno situati all'estero. Tale disposizione è stata confermata dal recente intervento legislativo con il nuovo art. 89 co. 3 norme att. cpp, il quale prevede che le comunicazioni intercettate mediante captatore informatico siano conferite esclusivamente negli impianti della Procura della Repubblica. Inoltre, l'aspetto più critico è che in tale *server* venivano conservati *tutti* i dati captati da *Exodus*.

Funzionalità diverse dalla sola attivazione del microfono. Tra le varie attività che potevano essere effettuate con *Exodus* si annoverano l'accesso al microfono e alla telecamera, l'estrazione di dati dal calendario, dalla rubrica, dalla galleria fotografica e anche da altre applicazioni installate, registrazione della posizione tramite GPS, delle chiamate effettuate, dei messaggi vocali inviati. Questo è sicuramente uno degli aspetti più delicati della vicenda *Exodus*. Lungi dal ripercorrere il dibattito dottrinale sul tema,[34] in tale breve lavoro si vuole piuttosto invitare ad una riflessione sul tema della tipicità delle attività investigative.

3.2. In generale, un captatore informatico nient'altro è che uno strumento mediante il quale determinate attività investigative possono essere condotte; non solo intercettazioni dunque, ma anche *inter alia* le cd. perquisizioni *online,* che permetterebbero la raccolta di dati presenti nel dispositivo in tempo reale, o le videoriprese, mediante attivazione della telecamera del dispositivo. Alla luce del fatto che *Exodus* consentisse, ai chi ne avesse il controllo, di effettuare tutte queste operazioni, si tratta ora di distinguere tra quali fossero consentite e quali no. Partendo dalle disposizioni del codice, secondo l'art. 266 co. 2 Cpp la sola intercettazione di comunicazioni fra presenti può essere eseguita «anche mediante l'inserimento di

[34] Si veda in materia l'autorevole contributo di F. Caprioli, *op. cit.,* 485 ss.

un captatore informatico su un dispositivo elettronico portatile», che si realizza tecnicamente mediante l'attivazione del microfono del dispositivo. Benché discutibile la scelta di limitare l'uso del captatore ad una sola attività, quella di intercettazione ambientale, peraltro non oggetto di richieste da parte degli organi inquirenti, è da rifiutare, a mio parere, una interpretazione che vedrebbe la possibilità di usare i *malware* per condure *altre* attività investigative. Tale convincimento deriva da due considerazioni.

La prima si riferisce al rispetto della riserva di legge, quale principio fondante dell'ordinamento giuridico, dettata dagli artt. 13, 14 e 15 Cost. Tutte le attività probatorie che ledono il diritto alla libertà personale, all'intimità domiciliare, nonché alla libertà e alla segretezza delle comunicazioni, devono essere previste tassativamente dalla legge. Allo stesso modo, l'art. 8 della Convenzione Europea dei diritti dell'uomo prevede che ogni ingerenza nella vita privata e familiare di un individuo, del suo domicilio e corrispondenza debba essere previsto dalla legge (oltre che costituire una misura necessaria in una società democratica). Si noti inoltre che, secondo la Corte EDU, la nozione di vita privata è ampia e non rigidamente interpretata. Può dunque l'utilizzo di un captatore informatico incidere su tali diritti? Certamente sì.[35] I beni giuridici che possono essere lesi da questi strumenti sono plurimi. Richiamando le fasi di cui si compone il procedimento cd. di *computer intrusion*, proprio dell'installazione di *malware*,[36] nella prima fase, cd. di perlustrazione, è la sfera di riservatezza del soggetto passivo del captatore informatico che viene lesa, proprio perché gli inquirenti procedono ad una raccolta di informazioni utili, talvolta anche personali e riservate, per poter passare all'attacco. Nella fase di attacco e di trincea la condotta rilevante è l'accesso al sistema. I beni giuridici coinvolti possono essere ricondotti al diritto individuale alla riservatezza informatica e soprattutto all'integrità e alla sicurezza dei sistemi informatici che, in questo caso, vengono gravemente compromessi. L'ultima fase è quella cd. di abuso, dove sono tipicamente svolte tutte le operazioni-obiettivo dell'attacco, utilizzando le diverse funzionalità del *malware* per compiere le più disparate azioni investigative. Si arriva così alla fase più invasiva e plurioffensiva. Infatti, i *malware* possono, in ordine di invasività:

- effettuare una copia delle unità di memoria per poi trasmetterla in tempo reale o ad intervalli stabiliti; in questo caso è evidente l'intrusione nella riservatezza informatica sia del soggetto *target,* che di soggetti terzi estranei che possono aver utilizzato il dispositivo compromesso o a cui i dati copiati possono riferirsi;
- decriptare i dati cifrati, avendo così l'accesso a dati particolarmente sensibili o comunque riservati, per cui si era reso necessario il ricorso a tale misura di sicurezza; in questo caso oltre alla riservatezza informatica viene coinvolto anche il diritto costituzionale alla segretezza delle comunicazioni rese possibili tramite l'utilizzo di dispositivi tecnologici e della rete;

[35] Tale tema è anche approfondito in F. Palmiotto, *La prova e l'indagine informatica*, cit.

[36] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*[3], Waltham 2011.

- captare il flusso informativo proveniente dalle periferiche consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo, digitato attraverso la tastiera, detto attraverso il microfono, o visto tramite la *webcam* del sistema *target* controllato; in questo caso, oltre a risultare violata la riservatezza informatica e la segretezza delle comunicazioni, c'è il rischio concreto che, mediante l'attivazione della telecamera e/o del microfono si possa violare il domicilio fisico.

Inoltre, in tutte le attività svolte in fase di abuso, l'aver infettato il dispositivo implica che tutti i soggetti che utilizzino tale supporto siano passibili di monitoraggio[37]. Si aggiunga inoltre che la sola condotta di installazione del software è sufficiente a costituire reato *ex* art. 615 *ter* Cp. Di conseguenza, il perimetro della condotta legittima deve essere specificamente tracciato *con legge ordinaria*, che intervenga a stabilire con precisione in quali casi e con quali modalità e garanzie tali diritti possano essere violati.

Per rispettare la riserva di legge non basta, a parere di chi scrive, che una attività investigativa, ma attuata con strumenti diversi dal captatore, sia disciplinata nel codice. Si pensi, ad esempio, alle intercettazioni di comunicazioni. Prima dell'intervento del 2017, le intercettazioni di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione erano disciplinate *ex* art. 266 Cpp, mentre le intercettazioni di comunicazioni informatiche o telematiche dal seguente art. 266 *bis* Cpp. Se si volesse adottare una interpretazione meno rigida del principio di riserva di legge, si potrebbe sostenere che essendo disciplinata l'attività di intercettazione di comunicazioni o conversazioni (telefoniche o telematiche), allora anche quelle effettuate mediante captatore informatico avrebbero potuto trovare base legislativa negli art. 266 e 266 *bis* Cpp. Siffatta soluzione è stata tuttavia confutata dall'intervento legislativo del 2017, laddove il legislatore ha comunque deciso di regolamentare le intercettazioni effettuate con captatore mediante l'aggiunta dei commi 2 e 2 *bis* all'art. 266 Cpp. Un captatore informatico, infatti, benché sia uno strumento mediante il quale determinate attività possono essere espletate, si differisce da tradizionali metodi investigativi per due fondamentali caratteristiche: il suo carattere occulto e la sua natura cd. attiva. Con quest'ultimo termine si far riferimento al fatto che un *malware* consente all'operatore di avere il controllo di tutto il sistema, sia captando ciò che viene effettuato mediante tale dispositivo, sia potendolo alterare (ad esempio, facendo telefonate, mandando SMS o messaggi in *chat*, accedere ed inviare posta elettronica, scattare foto, inserendo o modificando *files*). Tali caratteristiche rendono, a mio avviso, inadeguate le tradizionali norme in materia di mezzi di ricerca della prova, pensate con riferimento a strumenti analogici o tradizionali di investigazione.[38] Punto di partenza

[37] L'utilizzo del sistema da parte di più soggetti può avvenire non solo mediante account diversi, ma anche in modo "promiscuo". Per un approfondimento v. S. Marcolini, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche),* in *CP* 2010, 336 ss.

[38] Simili considerazione avevano informato la proposta di legge Quintarelli, la quale partiva proprio da una considerazione fondamentale: analizzate le caratteristiche tecniche dello strumento, si rendeva necessaria una

imprescindibile è dunque il rispetto della riserva di legge, come richiesto dagli artt. 14 e 15 Cost. e dall'art. 8 CEDU.

La mia seconda considerazione fa riferimento alla *voluntas legis*. Il legislatore è intervento in due momenti, nel 2017 e nel 2019, esercitando dunque la riserva di legge di cui *supra*. In tali interventi, il legislatore non ha solo scelto di disciplinare il captatore quale modalità speciale di intercettazione ambientale, ma ha anche deciso che questo sia il suo unico uso, avendone espressamente regolamentato solo uno. Tale decisione si evince anche dalla Relazione Illustrativa al d.lgs. 216/2017, laddove si legge: «il delegante (riferendosi alla L. 103/2017) ha inteso regolamentare uno solo degli usi del captatore informatico, quale modalità specifica di esecuzione di intercettazioni tra presenti. E ha ad oggetto esclusivamente dispositivi». Si aggiunge inoltre che nonostante il fatto che un *malware* consenta l'esecuzione di un «complesso di operazioni (alcune delle quali già praticate ove consentite dalla legislazione vigente) che la tecnologia consente dì effettuare, ma che il delegante non ha inteso regolare, limitando l'ambito dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inoculazione di dispositivo portatile (smartphone, tablet ecc.) e non anche di dispositivi fissi». Lo si ripete, benché discutibile (soprattutto il riferimento ai soli dispositivi portatili), *sic est*. Inoltre, ad ulteriore supporto di tale interpretazione, si aggiunga che, nonostante il recente intervento legislativo, non ne è stato esteso l'uso per nessun'altra tipologia di attività investigativa. L'impostazione minimalista e riduttiva della riforma Orlando è stata dunque confermata nella contro-riforma Bonafede,[39] aggiungendo inoltre enfasi sui requisiti tecnici dei programmi informatici al fine di garantire *inter alia* che questi si limitino «all'esecuzione delle operazioni autorizzate» (art. 2 co. 4 d.l. 161/2019).

3.3 Da come si evince dalla tabella *infra* (pag. 15), numerosi sono i profili di incompatibilità di *Exodus* con le regole in materia di captatore informatico. *Exodus* agiva indiscriminatamente, senza specifici target, compiendo attività illecite (quali la memorizzazione di dati dal dispositivo), trasferendo successivamente questa mole di byte in un *cloud* in Oregon, nella totale assenza di misure di sicurezza idonee. Nella mia ricerca,[40] mi riferisco a questi casi con

modifica al codice di procedura penale poiché nessun istituto ad allora esistente era adattabile ai captatori. Nella relazione alla proposta si legge: «L'art. 266 *bis* c.p.p. non è sufficiente in quanto lo strumento di osservazione e di acquisizione da remoto non si limita a intercettare un flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi, ma consente un monitoraggio molto più penetrante, anche su dati non oggetto di comunicazione da parte dell'utente e registrati in memoria (e quindi non ascrivibili fra i flussi di comunicazioni)».

[39] Si veda in tal senso anche G. Pestelli, *cit*, 150.

[40] Per un approfondimento, v. F. Palmiotto, *The impact of Algorithmic Transparency on Fair Trial Rights in Criminal Proceedings*, in *Algorithmic Governance and Governance of Algorithms*, in M. Ebers, M. Cantero Gamito (eds.), Springer 2020; F. Palmiotto, *Algorithmic Opacity as a Challenge to the Rights of the Defence*, blog post for Robotics & AI Law Society, September 2019, available here https://ai-laws.org/en/2019/09/algorithmic-opacity-challenge-to-rights-of-the-defense/.

il termine "*legal miscode*" che va ad indicare quei casi in cui il design di un *software* viola norme specifiche e/o principi fondanti l'ordinamento giuridico. Di recente, molti studi e ricerche si stanno concentrando sul problema del cd. "*Algorithmic Bias*".[41] In ambito di giustizia penale, ad esempio, COMPAS ci ha dimostrato come un *software* possa condurre a risultati discriminatori sulla base del colore della pelle, del genere o della classe sociale.[42] A mio parere, la sfida che l'utilizzo di tali *software* pone non riguarda solo ed esclusivamente il pericolo di risultati inaccurati o invalidi, ma anche illegali. *Legal miscode* è il termine che utilizzo per identificare questi casi. Questo può essere generato, ad esempio, da dati usati come *input* illegalmente ottenuti o dall'utilizzo di criteri illegittimi per raggiungere una decisione, quali il colore della pelle. La vicenda *Exodus* ci aiuta a chiarire questo concetto: il modo in cui il *software* è stato progettato è contrario alla novella disciplina in materia di captatore. Di conseguenza, l'illegalità del suo design non potrà che riversarsi sulla legittimità della prova acquisita per suo tramite, una volta vigenti tali disposizioni.[43]

[41] Si segnala in materia l'eccellente contributo di S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer 2020.

[42] Per un approfondimento sul caso COMPAS si veda S. Quattrocolo, *op. cit.*

[43] A livello processuale, la prova acquisita può dunque essere viziata da invalidità (nullità o inutilizzabilità). Nel caso specifico del captatore, ad esempio, l'art. 271 Cpp elenca i casi di divieti di utilizzazione dei dati acquisiti in violazione delle disposizioni di cui agli artt. 267 e 268 co. 1 e 2 Cpp, nonché tutti i dati acquisiti al di fuori dei limiti di tempo e luogo indicati nel decreto autorizzativo.

Funzionalità *Exodus*	**Normativa Riforma Orlando** *L. 103/2017* *D.lgs. 216/2017*	**Normativa Riforma Bonafede** *D.l. 161/2019* *conv. in L. dalla l. 7/2020*
Exodus camuffato e caricato su *Google Play Store*	Nulla in merito di installazione (se non il generico disposto dell'art. 268 co. 3 *bis* Cpp)	Art. 89 co. 2 ss. disp. att. dispone che ai fini della installazione debbano essere impiegati solo programmi conformi ai requisiti tecnici stabiliti con decreto dal Ministero della giustizia.
Mancanza di una "*target validation procedure*"	Generale incompatibilità con il principio di riserva di giurisdizione Incompatibilità con l'art. 267 co. 1 Cpp che richiede l'autorizzazione del Gip, data con decreto motivato, per procedere ad intercettazione mediante captatore informatico	*Idem*
Mancanza di un sistema di disinstallazione del *software*	Incompatibilità con l'art. 267 co. 3 Cpp che stabilisce che la durata massima delle intercettazioni non può superare i 15 giorni, prorogabili dal giudice con decreto motivato di ulteriori 15 giorni	*Idem*
	Inoltre l'art. 89 co. 2 *quinquies* disp. att. c.p.p. dispone che al termine della registrazione il captatore informatico venga disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante	Nuovo articolo 89 co. 5 disp. att. Cpp il quale ha identico contenuto al precedente comma 2 *quinquies* dis. Att. Cpp.

Scarsissimo livello di sicurezza	L'art. 4 del d.m 20.4.2018 detta i requisiti dei programmi informatici funzionali all'esecuzione di intercettazioni in modo da assicurare integrità, sicurezza e autenticità dei dati captati	L'art. 2 co. 3 del Decreto Legislativo 31 dicembre 2019 n. 161, rinvia nuovamente al decreto del Ministro della giustizia per stabilire i requisiti tecnici dei programmi informatici. Tali requisiti, secondo il comma 4, sono stabiliti secondo misure idonee di affidabilità e sicurezza, garantendo che tali programmi si limitino alla esecuzione delle operazioni autorizzate.
Funzionalità diverse dalla sola attivazione del microfono	Secondo l'art. 266 co. 2 Cpp la sola intercettazione di comunicazioni fra presenti può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile, che si realizza tecnicamente mediante l'attivazione del microfono del dispositivo.	L'impostazione minimalista e riduttiva della riforma Orlando è stata confermata nella contro-riforma Bonafede
Trasferimento di tutti i dati intercettati da *Exodus* (ben 80 terabyte) su un unico server Amazon Cloud situato in Oregon	L'art. 89 co. 2 *ter* disp. att. c.p.p. prevede che il trasferimento delle registrazioni sia effettuato esclusivamente verso gli impianti della Procura della Repubblica così da garantire originalità e integrità delle registrazioni	Nuovo articolo 89 co. 3 disp. att. prevede che le comunicazioni intercettate mediante captatore informatico siano conferite esclusivamente negli impianti della Procura della Repubblica.

4. Dalla scoperta di *Exodus*, l'attenzione si è focalizzata sulla mancanza di adeguati disciplinari tecnici in forma di decreti ministeriali,[44] che indichino dettagliatamente le caratteristiche tecniche dell'intrusore informatico, nonché sulla necessità di garantire sufficienti controlli su tali *software* e sulla intera filiera investigativa. Prima della contro-riforma, agli albori dello scandalo *Exodus*, vi era chi proponeva un controllo indipendente da parte di un terzo soggetto o chi suggeriva un ulteriore intervento normativo che andasse a regolamentare con

[44] Soprattutto alla luce della imbarazzante vaghezza del d.m. 20.4.2018.

maggiore precisione le varie fasi tra cui, in particolare, quella della disattivazione del malware.[45] Secondo Giovanni Ziccardi, «fino a quando tutta l'attività rimane chiusa in aziende o nei locali della procura o in aziende correlate alle procure e viene portato in processo l'esito, ma non c'è la possibilità di controllare traccia per traccia, momento per momento tutto quello che è stato fatto, secondo me non si può ritenere che sia una attività corretta, o meglio, *si va sulla fiducia*».[46] Tuttavia, la vicenda *Exodus* ci ha proprio insegnato che di tali sistemi e di chi li produce non è possibile fidarsi. A mio avviso, in aggiunta a tali auspicabili soluzioni, vi è un soggetto che viene spesso trascurato e il cui ruolo in qualità di supervisore ha una importanza centrale nel procedimento penale: la difesa. Questa "fiducia" di cui Ziccardi parla circa la correttezza, legalità e validità della prova assunta mediante strumenti informatici è un concetto diametralmente opposto al principio del contraddittorio nella formazione della prova e questa necessità di controllo sul funzionamento di questi software è per la difesa, un diritto.

4.1 Senza pretese di esaustività, a livello nazionale l'imprescindibile rapporto tra il principio del giusto processo e quello del contradditorio è delineato nei vari commi dell'art. 111 della Costituzione. In particolare, si evidenzia la statuizione al comma terzo secondo cui la legge deve assicurare che «la persona accusata di un reato…abbia la facoltà, davanti al giudice, di interrogare o far interrogare le persone che rendono dichiarazioni a suo carico». Il cd. "diritto al confronto" ivi sancito, nonostante la formula "facoltativa" che si distingue rispetto a quella usata nell'art. 6 Cedu, si realizza nella forma di contraddittorio specifico nel quarto comma il quale statuisce che «La colpevolezza dell'imputato non può essere provata sulla base di dichiarazioni rese da chi, per libera scelta, si è sempre volontariamente sottratto all'interrogatorio da parte dell'imputato o del suo difensore». Il diritto al confronto è una prerogativa dell'imputato, distinto dal diritto alla controprova, che si configura come espressione «di un diritto di difesa attivo nella fase di assunzione del procedimento probatorio e non piegato ad una forma di intervento, circoscritto nei tempi e passivo nei modi, ad atti unilaterali dell'autorità».[47]

A livello sovranazionale, di estrema importanza sono gli artt. 6 Cedu e 47 Carta dei diritti fondamentali dell'Unione Europea i quali sanciscono il diritto all'equo processo. L'art. 6 co. 3 lett. *d* Cedu, in particolare afferma che «ogni accusato ha il diritto di…esaminare o far esaminare i testimoni a carico e ottenere la convocazione e l'esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico». Secondo la giurisprudenza della Corte, con particolare riferimento al caso *Al-Khawaja e Tahery contro Regno Unito*, il diritto al confronto *ex* art. 6 co. 3 lett. *d* non solo impone che l'imputato debba essere in grado di contestare l'attendibilità

[45] Come suggerito dalla dottoressa Dolci della Procura Milano, intervistata per Report, *Infiltrato Speciale*, di Paolo Mondani, puntata del 18.11.2019.
[46] G. Ziccardi, *Consulenza tecnica*, in M. Gutheil e Q. Liger, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, studio per il Comitato LIBE del Parlamento Europeo, 2017, 56.
[47] N. Galantini, *Giusto processo e garanzia costituzionale del contraddittorio nella formazione della prova*, in www.penalecontemporaneo.it, 2011.

e la credibilità delle prove a suo carico, ma anche di verificarne la veridicità e l'affidabilità. È importante inoltre precisare che la Corte Edu da sempre adotti una interpretazione autonoma ed estensiva del termine "testimone". Nel caso *Georgios Papageorgiou contro Grecia*, ad esempio, la Corte ha esaminato ai sensi dell'art. 6 co. 3 lett. *d* la questione dell'accesso da parte dell'imputato a documenti in originale e a computer files rilevanti per le accuse mosse al ricorrente. Infine, benché tale diritto ricopra un ruolo fondamentale nell'assicurare un equo processo, non è assoluto e come tale può subire delle limitazioni. Similmente al disposto costituzionale italiano, secondo il quale la formazione della prova può non avvenire in contraddittorio per consenso dell'imputato o per accertata impossibilità di natura oggettiva o per effetto di provata condotta illecita *ex* art. 111 co. 5 Cost., anche il cd. *right to confrontation* può essere soggetto a deroghe, nella presenza di due circostanze cumulative: 1) l'assenza (del testimone) deve essere giustificata e 2) devono essere presenti sufficienti fattori di contro-bilanciamento se la condanna è fondata esclusivamente o ad un grado decisivo su elementi di prova assunti in assenza di contraddittorio.

4.2 In che modo si rapportano questi diritti con una prova digitale quale quella assunta mediante captatore informatico? Queste tipologie di prove si definiscono "algoritmiche" in quanto è l'algoritmo ad essere usato come mezzo di acquisizione della prova. Di conseguenza, la qualità della prova digitale presentata dipenderà strettamente dalla qualità del *software* usato per acquisirla e dalle tecniche forensi adottate.[48] La presenza di errori nel design e/o nell'uso di tali strumenti influirà direttamente sul loro output, *id est* sulla qualità della prova. L'esigenza della difesa di controllare la presenza di tali errori è fondamentale per verificare la legalità, validità ed accuratezza della prova digitale assunta. In questi casi, dunque, per poter correttamente esercitare il diritto al confronto, la difesa deve poter conoscere il *software* e come è stato concretamente utilizzato. Questo prescinde, a mio avviso, dalle concrete regole di esclusione della prova e/o di ammissibilità della prova, specifiche di ogni sistema giuridico: prima di escludere o dichiarare inammissibile una prova, la difesa deve poter essere messa nella condizione di lamentare la potenziale violazione di legge. Inoltre, anche se una prova fosse dichiarata ammissibile, la difesa deve comunque verificarne la qualità. Esattamente come previsto in materia di prova testimoniale per la quale, una volta ammessa a processo, la difesa ha la possibilità di condurre l'esame incrociato per verificare l'attendibilità del teste, allo stesso modo una prova algoritmica deve poter essere contestata, anche se dichiarata ammissibile. Dunque, per poter esercitare il diritto al contraddittorio, la difesa deve poter aver accesso alle informazioni riguardanti l'algoritmo mediante il quale la prova è stata assunta.

4.3 Tuttavia, le barriere che si pongono tra l'accesso alle informazioni e la loro comprensibilità pongono un problema inedito per il diritto al contraddittorio. In che modo può la difesa esercitare tale diritto se gli strumenti informatici rimangono occultati e le informazioni circa il loro funzionamento nascoste? Quando gli algoritmi vengono utilizzati nei procedimenti penali per finalità probatorie, spesso la difesa deve confrontarsi con i problemi derivanti dalla

[48] Sul tema del diritto alla difesa e al giusto processo si veda S. Quattrocolo, *op. cit.*

cosiddetta opacità algoritmica. Con questo termine si indicano in letteratura quelle situazioni dove è noto l'*output* di un algoritmo (*id est* la prova) ma non come sia stato generato. È uno stato di "non conoscenza".[49] L'opacità algoritmica, inoltre, può riferirsi a due diverse tipologie di barriere: 1) all'accesso alle informazioni e/o 2) alla comprensibilità delle stesse. In particolare, l'accesso alle informazioni può essere impedito dal diritto d'autore e altre forme di protezioni proprietarie, da segreti o da situazioni di totale assenza di trasparenza, come nel caso *Exodus*. Quanto alla possibilità di comprendere le informazioni, rileva in particolare modo la mancanza di competenza tecnica del difensore o, più in generale, la scarsa comprensibilità del sistema stesso. Si pensi ai sistemi di Intelligenza Artificiale, in cui neanche il programmatore è in grado di spiegare con precisione in che modo la macchina sia giunta al risultato finale. Tali considerazioni si applicano, in generale, a tutte le prove algoritmiche, *id est* generate da un sistema algoritmico.

Con particolare riferimento alla disciplina del captatore informatico, tuttavia, tali preoccupazioni si aggravano non solo a causa della elevata invasività di siffatto strumento, ma anche per la scarsa attenzione prestata alle esigenze difensive, nonostante l'ultima occasione di riforma.[50] A ben vedere, poche sono le disposizioni che garantiscono alla difesa accesso alle informazioni necessarie per controllare la qualità dei dati acquisiti mediante captatore. Di interesse è l'art. 89 norme att. cpp il quale al primo comma prevede che, quando si procede ad intercettazione mediante captatore, «il verbale indica il *tipo di programma* impiegato». Tuttavia, tale riferimento potrebbe essere troppo generico per poter giustificare, *inter alia*, l'accesso a informazioni più dettagliate sul software, solitamente protette da segreto commerciale. Sempre con riferimento al verbale delle operazioni, l'art. 268 Cpp prevede che siano annotate le operazioni e trascritte, anche sommariamente, il contenuto delle operazioni intercettate. Nulla viene stabilito riguardo all'annotazione a verbale delle informazioni riguardanti il software utilizzato. Inoltre, al comma 6, ai difensori viene sì data facoltà di esaminare gli atti e di ascoltare le registrazioni, ma non di ottenere ulteriori informazioni sul software, né di esaminarne, ad esempio, il codice sorgente.

Le garanzie difensive sono così modellate dando diritto di accesso e di copia (art. 268 co. 8 Cpp e art. 89 *bis* co. 4 norme att. cpp) con riferimento all'*output* (ossia le registrazioni delle comunicazioni) o ad atti ad esso relativi (i verbali delle operazioni in cui non sono però annotate informazioni sul software se non il "tipo di programma impiegato"), ma non al *software* che lo ha generato. Ciò non toglie, a mio avviso, che la difesa possa fondare una richiesta di accesso ad informazioni sul *software* in forza della generale garanzia costituzionale (e sovranazionale) del diritto al contradditorio. La presenza di più specifiche disposizioni sarebbe

[49] J. Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, in *Big Data & Society*, 2016.

[50] Già prima della riforma Bonafede, in dottrina molti commentatori avevano denunciato il previgente sistema di selezione delle intercettazioni rilevanti, ritenuto manifestamente incostituzionale. Si veda *inter alia* G. Pestelli, *op. cit.*, 116.

comunque auspicabile, soprattutto dal momento in cui, come riportato da Ziccardi, «l'utilizzo di tecniche e strumenti di *hacking*, nonché la prova assunta per loro tramite, non viene contestata in corte perché molti professionisti non possiedono l'adeguata conoscenza e formazione».[51]

4.4 Riprendiamo il caso *Exodus*. Ipotizziamo che una prova digitale assunta mediante questo *malware* sia stata presentata in un processo penale senza, come avviene nella pratica, fornire ulteriori dettagli. Le informazioni che abbiamo su *Exodus* le dobbiamo ad un lungo lavoro di ricerca e di inchiesta da parte di *Security Without Borders*, Report, la Repubblica, *Wired*, *Motherboard* e altri. In che modo la difesa avrebbe potuto raccogliere le stesse informazioni e giungere agli stessi risultati? Non credo che questo sarebbe stato possibile, quantomeno nell'ambito di un procedimento penale. Paradossalmente, i vari strati di opacità e segretezza che caratterizzano questo caso e le numerose barriere alle informazioni e alla loro intelligibilità, non avrebbero manco permesso alla difesa di sapere che tipo di *software* fosse stato utilizzato, il nome dell'azienda che lo ha sviluppato, le sue caratteristiche tecniche. Né ad oggi, secondo quanto dichiarato da *Wired*, ai giornalisti è accessibile il numero preciso delle procure che si siano affidate alla compagnia sviluppatrice di *Exodus* per servizi di intercettazione.[52]

L'opacità così creata influisce sul diritto al contraddittorio che, in mancanza di specifiche garanzie in grado di garantire accesso e comprensibilità delle informazioni, non consente alla difesa di contestare *de facto* le prove informatiche assunte mediante algoritmi. Senza conoscere l'oggetto del proprio scrutinio, non è possibile contestarne l'affidabilità, l'accuratezza e la legalità. Tuttavia, conoscere il *software* e il suo funzionamento, non significa, si badi bene, solo ed esclusivamente accesso ad il codice sorgente. È una sfida maggiore le cui soluzioni procedurali possono essere molteplici quali, ad esempio, risposte scritte sul funzionamento della macchina, esame incrociato di chi ha utilizzato il *software*, accesso alla documentazione necessaria sul funzionamento del *software*, testimonianze dei programmatori di *software* che eseguono analisi forensi, possibilità di partecipazione all'assunzione della prova. O ancora, quelle proposte dal disegno di legge Quintarelli,[53] tra cui *inter alia*:

- l'istituzione di un sistema di omologazione dei captatori;
- il diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dall'installazione fino alla loro rimozione, e di verificare tecnicamente che i captatori in uso siano certificati, fino a consentire l'ispezione del codice sorgente, previamente depositato presso un ente da determinare, e gli accertamenti tecnici informatici volti a verificare l'assenza di manipolazioni;

[51] M. Gutheil e Q. Liger, *op. cit.*, 56.
[52] C. Anesi, R. Anigius, P. Petrasso, *op. cit*.
[53] Proposta di legge Quintarelli e altri, *Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi,* 31.1.2017 n. 4260.

- la possibilità per la difesa, con tutte le garanzie del caso e con gli obblighi di riservatezza e di segreto, di verificare gratuitamente la presenza del captatore utilizzato in un registro nazionale dei captatori, gestito dall'ente di omologazione, fino alla più radicale opzione di imporre un obbligo per i produttori di fornire pubblicamente e gratuitamente gli strumenti software necessari per l'analisi dell'allegato al fascicolo contenente la registrazione delle operazioni.

In assenza di specifiche garanzie procedurali, che garantiscano una supervisione da parte della difesa, l'opacità che circonda questo tipo di software rappresenta un ostacolo e una possibile violazione del principio del contraddittorio della prova. L'auspicio è dunque quello di rivalorizzazione del ruolo, finora trascurato, di controllo svolto dalla difesa sulle prove digitali e l'abbandono della presunzione quasi assoluta di affidabilità e oggettività degli strumenti informatici.

5. Durante il mio intervento al convengo "Nuove tecnologie e futuro del diritto pubblico" organizzato da ICON-s, concludevo con un auspicio. Quello della rivalorizzazione del ruolo, finora trascurato, di controllo svolto dalla difesa sulle prove digitali. Ironia della sorte, qualche mese dopo la conferenza, il legislatore ha avuto l'occasione di esaudire queste speranze e, tuttavia, poco sembra essere cambiato dalla disciplina previgente. È grave, a mio avviso, che lo scandalo *Exodus* abbia insegnato così poco. Ed è ancora più paradossale pensare al fatto che tutti i dati delle intercettazioni effettuate con tale *software* confluissero indiscriminatamente e senza misure di sicurezza in un unico *cloud* se si pensa al fatto che la linea di ispirazione della riforma Orlando fosse proprio l'intento di tutelare la riservatezza dei soggetti coinvolti nelle indagini.[54] Sarebbe riduttivo e semplicistico, tuttavia, affidarsi esclusivamente all'intervento di un legislatore illuminato. L'avvento delle nuove tecnologie come strumenti investigativi ha dimostrato, a mio avviso, che non solo è necessario l'adeguamento di norme pensate per strumenti tradizionali analogici, ma anche di personale formato ed istruito al loro uso, nonché la necessità di un sistema di controlli e supervisione per identificare errori ed abusi. E la difesa deve poter giocare un ruolo maggiore in tale sistema.

[54] Tale obiettivo veniva perseguito mediante l'introduzione di una serie di misure miranti a bloccare la conoscibilità delle comunicazioni riguardanti terzi estranei al procedimento, sanzionandone la diffusione penalmente e limitando *ab origine* la verbalizzazione.