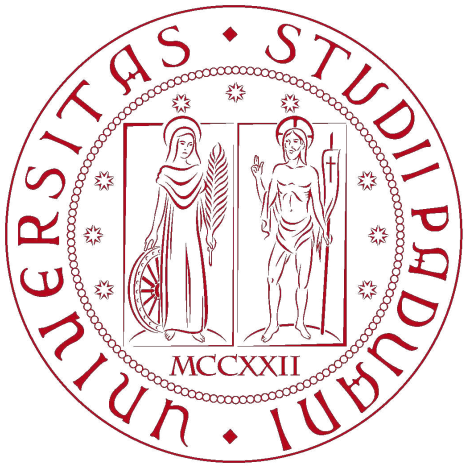

UNIVERSITÀ DEGLI STUDI DI PADOVA

Università degli Studi di Padova

Dipartimento di Diritto Pubblico,
Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia
a.a. 2022/2023

IL CAPTATORE INFORMATICO "ATIPICO"

Relatore: Professore Massimo Bolognari

Studente: Tobia Gaddi

Indice

1. Le indagini penali digitali e il captatore informatico

1. Verso una digitalizzazione delle indagini penali

L'avvento di internet e la diffusione ormai capillare nella vita quotidiana delle *Information and Communications Technologies*-ICT[1] hanno rivoluzionato il sistema delle indagini penali, rendendo necessario un ripensamento profondo delle norme e dei principi che le caratterizzano. Infatti, le indagini previste dal *Codice di Procedura Penale* del 1988 erano state concepite in un mondo pre-digitale, fondato sulla materialità degli elementi di prova, risultando oggi inadeguate e inefficaci.

La rivoluzione digitale, tuttora in corso, ha profondamente trasformato questa impostazione classica. I dispositivi digitali sono in grado di registrare continuamente le nostre vite, "traducendole" in dati digitali. In questo nuovo mondo, chiamato dal filosofo Luciano Floridi "infosfera"[2], si sono sviluppate nuove tipologie di crimini, i cosiddetti *computer crime* e *cyber crime*[3], commessi con l'utilizzo di dispositivi tecnologici e della rete *web*.

A livello internazionale, un punto di riferimento importantissimo è rappresentato dalla *Convenzione sul Cybercrime* del Consiglio d'Europa, stipulata a Budapest nel 2001. In tale documento si è cercato di trovare un bilanciamento tra le esigenze investigative e le garanzie a tutela dei diritti degli individui nel campo delle indagini informatiche. Il risultato principale della Convenzione è consistito in una serie di principi processuali minimi, ai quali le legislazioni nazionali avrebbero dovuto adeguarsi: riserva di legge,

---

[1] Definizione dell'espressione *Information and Communication Technologies* – ICT, da Treccani.it: "tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni".

[2] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, I° ed. 2017, p. 12 ss.

[3] Secondo O. CALAVITA, *L'odissea del trojan horse. Tra potenzialità tecniche e lacune normative*, in *Diritto penale contemporaneo*, 11/2018, p. 46 ss., https://archiviodpc.dirittopenaleuomo.org/d/6323-l-odissea-del-trojan-horse, "I *cybercrimes* sono una sola delle due ampie categorie che possono essere ricondotte alla settore della disciplina penalistica definita 'diritto penale dell'informatica': accanto ad essi, infatti, si affiancano i *computercrimes*. Questi ultimi si caratterizzano per lo strumento con il quale vengono commessi (i.e. l'informatica); mentre i primi si distinguono per un utilizzo del web a fini criminosi".

riserva di giurisdizione, tutela della dignità umana e principio di proporzionalità. Inoltre, accanto ai principi generali appena enunciati, la Convenzione ha dedicato anche alcune disposizioni alle modalità di ricerca e di acquisizione della prova.
Il legislatore italiano si è allineato con estremo ritardo ai dettami della Convenzione con la legge di ratifica n. 48/2008[4]. Tuttavia, l'intervento è da ritenersi incompleto ed eccessivamente timido, poiché si è limitato ad adattare la disciplina previgente, senza introdurre alcun nuovo mezzo di ricerca della prova[5].

Si rende, dunque, necessario disciplinare anche i nuovi strumenti tecnologicamente all'avanguardia a disposizione delle autorità per la lotta al crimine informatico e tradizionale. In alcuni casi, per il legislatore italiano è sufficiente integrare norme già presenti nel *Codice penale e di procedura penale*. Ad esempio, la cd. *Riforma Orlando* del 2017 ha previsto al co. 2 dell'art. 266 c.p.p. la possibilità di effettuare l'intercettazione di comunicazioni anche mediante il captatore informatico. Tuttavia, in futuro sarà necessario che il legislatore introduca nuove disposizioni per disciplinare *ex-novo* strumenti investigativi e tecniche informatiche compatibili con la nuova realtà digitale.

Le indagini penali per i reati informatici non possono più essere svolte con i tradizionali mezzi di ricerca della prova. Infatti, i dispositivi informatici "producono" una nuova tipologia di elemento di prova – i dati digitali (o informatici) – estrapolabili dagli investigatori con strumenti tecnologici, come, ad esempio, il captatore informatico.
Il dato informatico presenta caratteristiche profondamente diverse rispetto alla classica prova materiale: è rappresentato in forma binaria, cioè in termini di 0 e 1, può essere copiato facilmente e riprodotto, ma è estremamente instabile, in quanto può essere alterato o cancellato, anche involontariamente, nel corso di un'indagine, con la conseguenza di falsarne il valore probatorio e impedirne l'utilizzo in giudizio. Per questa ragione, è necessario preservarne l'autenticità e l'integrità nelle fasi di acquisizione, conservazione e in sede processuale.

[4] Legge n. 48/2008, in Gazzetta Ufficiale, https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario

[5] O. CALAVITA, *L'odissea del trojan horse. Tra potenzialità tecniche e lacune normative*, in *Diritto penale contemporaneo*, (11/2018), p. 45 ss., https://archiviodpc.dirittopenaleuomo.org/d/6323-l-odissea-del-trojan-horse

L'importanza crescente che ha assunto il dato digitale nel contesto delle indagini penali ha portato alla nascita di un nuovo specifico settore delle scienze forensi, chiamato *digital forensics*, e di una nuova figura professionale – il tecnico forense – il quale svolge un ruolo essenziale nel supportare le attività investigative poiché possiede la conoscenza e la competenza tecnica necessaria per poter individuare, recuperare e analizzare il materiale informatico contenuto nei dispositivi. Il suo obiettivo è di estrapolare i dati, garantendone l'autenticità e l'integrità, in modo tale che possano essere utilizzati come elementi di prova in giudizio.

Il legislatore italiano ha inserito nella legge di recepimento della *Convenzione di Budapest* (L. 48/2008) una serie di regole da rispettare nello svolgimento delle indagini penali informatiche per preservare l'integrità dei dati raccolti[6], richiamandosi implicitamente alle *best practices* elaborate a livello internazionale nell'ambito della *digital forensics*, senza tuttavia tipizzarle. Si fa riferimento alle linee guida ISO[7], strumenti non vincolanti ma che forniscono importanti procedure tecniche per garantire l'integrità e l'autenticità dei dati.
Si allude, ad esempio, alla *"chain of custody"* (catena di custodia) che rappresenta un istituto giuridico ampiamente utilizzato nel sistema processuale statunitense per garantire l'autenticità e l'integrità dei dati raccolti durante le indagini. Lo strumento si basa su un processo di documentazione completa che registra in modo accurato ogni fase (ricerca, raccolta, custodia e analisi) e tiene traccia di ogni operazione svolta, con le rispettive date

[6] L'art. 8 legge n. 48/2008 recita: "all'articolo 244, comma 2 c.p.p., le parole 'anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione', all'articolo 247 c.p.p. le parole '1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione', all'articolo 248, co. 2 c.p.p., le parole 'presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici'".

[7] Standard ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition, and preservation of digital evidence*: "This International Standard provides guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence. These processes are required in an investigation that is designed to maintain the integrity of the digital evidence – an acceptable methodology in obtaining digital evidence that will contribute to its admissibility in legal and disciplinary actions as well as other required instances".

e l'indicazione delle persone che hanno avuto un contatto con i dati[8]. Il legislatore italiano ha assimilato tale strumento in maniera strutturalmente diversa, frammentandolo in vari articoli del *Codice di procedura penale*: un primo gruppo di norme concerne le operazioni per identificare i dati informatici (artt. 244-247 c.p.p.); un secondo insieme riguarda la raccolta di essi[9]. Tuttavia, la legge non regola la conservazione dei dati una volta transitati nei server della procura, né prevede che si documentino le attività svolte[10].

2. Definizione di captatore informatico: caratteristiche e profili tecnici

Il captatore informatico, noto anche come *trojan horse*[11], è uno strumento tecnologicamente all'avanguardia, utilizzato sempre più di frequente dagli investigatori per contrastare la criminalità, in particolare le fattispecie più gravi, come il terrorismo e la mafia. Le sue straordinarie capacità di intrusione nei dispositivi di soggetti indagati lo rendono indispensabile per la raccolta di elementi di prova.

Il *trojan* è composto da due moduli: il *server*, cioè un programma di piccola dimensione che infetta il dispositivo, inoculando un virus; e il *client*, cioè l'applicativo che il virus utilizza per controllare il *device*[12]. Volendo impiegare un linguaggio tecnico, esso rappresenta un *malware*, appartenente alla categoria dei programmi *Remote Control*

---

[8] L. BARTOLI, C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 140 ss.

[9] Secondo L. BARTOLI, C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 142, "Una volta individuato, il materiale d'interesse andrà raccolto: l'atto con cui si procede è il sequestro; presso i fornitori di servizi informatici, telematici e di telecomunicazioni, il codice prevede la possibilità di procedervi clonando le informazioni (art. 254-bis c.p.p.). Le accortezze da adottare sono descritte nei dettagli: occorre un supporto adeguato, una procedura che assicuri la conformità del duplicato rispetto all'originale e la sua immodificabilità. Al fornitore del servizio è poi ordinato di proteggere gli originali che, nonostante il sequestro, non escono mai dal suo possesso".

[10] D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *JusOnline - Rivisita di Scienze Giuridiche*, 2017, n. 3, p. 405 ss., https://jus.vitaepensiero.it/news-papers-il-captatore-informatico-nella-legislazione-italiana-4843.html#_ftn3

[11] Questa denominazione allude allo stratagemma del cavallo di Troia ideato da Ulisse, grazie al quale i Greci riuscirono a penetrare a Troia, fino ad allora inutilmente assediata, come raccontato nell'*Iliade*, poema epico attribuito ad Omero. Analoga è la funzione del captatore che si infiltra occultamente in un dispositivo appartenente all'indagato.

[12] D. SANTORO, *Le intercettazioni ambientali. Attivazione del trojan, esigenze investigative, tutela della riservatezza in attuazione agli art. 13,14 e 15 della Costituzione*, Youcanprint, 2020, p. 23.

System (RCS), che viene installato nei dispositivi di un soggetto *target*, a sua totale insaputa e con la sua inconsapevole collaborazione.

L'inserimento del captatore nel dispositivo viene chiamato *inoculamento* ed è la fase più delicata e complicata[13]. Prima di procedere, è necessario effettuare un'analisi di fattibilità, normalmente svolta dalla società di spionaggio a cui le autorità affidano la gestione delle attività di intercettazione[14], in modo da definire le modalità operative di inserimento del *trojan*, sulla base delle caratteristiche specifiche dei dispositivi da infettare. Ad esempio, gli *IPhone* utilizzano il sistema operativo proprietario *IOS* che rende il dispositivo intercettabile nel solo caso in cui il soggetto target abbia effettuato per ragioni personali la procedura di *jailbreaking* che permette di superare le restrizioni di sicurezza e di acquisire maggior padronanza del sistema operativo stesso[15].

L'inoculamento può avvenire con due modalità diverse: diretta oppure da remoto. Nel primo caso, un agente di polizia accede fisicamente al dispositivo *target* (pc*, smartphone*, *tablet*) e inocula a livello *hardware* il virus. Questa modalità è la più rischiosa, perché esiste la concreta possibilità che il soggetto da intercettare possa accorgersi dell'intrusione e compromettere l'intera indagine. L'installazione indiretta o da remoto che non richiede un accesso fisico al *device* è la modalità più utilizzata ed è resa possibile dalle tecniche di *Social Engineering*[16]: attraverso l'invio di mail, messaggi, richieste di aggiornamento di app e di *software*, vengono introdotti occultamente *link* nel dispositivo del soggetto *target* che, una volta aperti, scaricano automaticamente e installano il *malware*.

---

[13] M. C. FALCHI, *Captatore informatico: i rischi di una mancata puntuale regolamentazione*, in *Ius in itiner*e, 2021, https://www.iusinitinere.it/captatore-informatico-i-rischi-di-una-mancata-puntuale-regolamentazione-29697

[14] Art. 268 c. 3-bis c.p.p. "Quando si procede a intercettazione di comunicazioni informatiche o telematiche [266 bis], il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati. […] l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'articolo 348, comma 4" e art. 348 c. 4 c.p.p. "La polizia giudiziaria […] può avvalersi di persone idonee […]".

[15] P. IOVINO, *Il trojan horse nelle indagini penali tra limiti normativi ed operativi,* in *Diritto.it*, 2022*,* p. 5 ss., https://www.diritto.it/il-trojan-horse-nelle-indagini-penali-tra-limiti-normativi-ed-operativi/

[16] G. DRAGONI, *Cos'è il Social Engineering, come difendersi e come riconoscerlo*, in *Osservatorio.net*, 2023, https://blog.osservatori.net/it_it/social-engineering-come-difendersi: "Il Social Engineering (o Ingegneria Sociale) è una tecnica di attacco cyber, basata sullo studio della psicologia e sullo sfruttamento dell'ignoranza e dell'impreparazione informatica delle persone comuni, per ottenere dati confidenziali (password, informazioni su conti correnti, informazioni finanziarie), estorcere denaro o persino rubarne l'identità".

Ci sono, tuttavia, alcune controindicazioni riguardanti il funzionamento del *trojan*. Infatti, i captatori sono soggetti a rapida obsolescenza e quindi possono essere "individuati" dagli antivirus più aggiornati[17], compromettendo l'indagine informatica. Inoltre, esistono programmi *ad hoc* per l'individuazione di intrusioni. Ormai molto spesso gli individui radicati nella criminalità si fanno assistere da soggetti altamente qualificati in campo informatico che offrono la loro *expertise* per proteggerne i dispositivi da intromissioni indesiderate.
Un altro ordine di problemi deriva dalle conseguenze che il *trojan* provoca ai dispositivi infettati: una diminuzione molto rapida della batteria e un alto consumo di dati cellulare, dovuto al trasferimento dei dati dal dispositivo al server della Polizia. Questi segnali possono far insospettire il soggetto controllato. Affinché il captatore funzioni correttamente è quindi necessario che l'apparecchio all'interno del quale viene installato sia dotato di collegamento ad internet in modo tale che gli investigatori possano regolare le attività di intercettazione e successivamente ricevere i dati captati nei server della Procura.

Una volta installato, il *trojan* permette alle autorità di controllare da remoto tutte le operazioni svolte dal dispositivo infettato, violando eventuali difese e diventando l'amministratore del sistema. La sua intrusione all'interno del *devic*e permette di superare il limite della crittografia, una tecnica di protezione sempre più diffusa tra le principali app di messaggistica istantanea che codifica chiamate e messaggi, impedendo a soggetti esterni alle comunicazioni di leggerle/ascoltarle[18]. Acquisiti i poteri di amministrazione, può accedere ad un ventaglio praticamente illimitato di informazioni presenti e future contenute nel dispositivo, grazie alle molteplici funzionalità di cui è dotato, attivabili anche contemporaneamente. Queste ultime sono raggruppabili in due tipologie di attività investigativa: le attività di *Online Search* e quelle di *Online Surveillance*. Le prime permettono di ricercare in maniera occulta informazioni all'interno della memoria del dispositivo infettato, consentendo di copiarle e di trasmetterle successivamente ai server

[17] W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021, p. 8.

[18] R. DE VITA & A. LAUDISIA, *I captatori informatici tra pericoli per i diritti umani e riduzionismo giuridico,* in *Eurispes*, 2019, p. 3 ss., https://eurispes.eu/wp-content/uploads/2016/04/vita-digitale-a-rischio.pdf

delle autorità investigative. Le attività di *Online Surveillance* prevedono il monitoraggio del flusso di dati che transita nel dispositivo in tempo reale[19].

Le potenzialità applicative del captatore sono state oggetto di diverse recenti pronunce, tra le quali occorre ricordare la descrizione dettagliata resa dalle Sezioni Unite della Corte di Cassazione nella *Sentenza Scurato* del 28 aprile 2016[20]:

- captare tutto il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia web mail, che out look);
- attivare il microfono e, dunque, di apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi;
- mettere in funzione la web camera, permettendo di carpire le immagini;
- perquisire l'hard disk e di fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira;
- decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*);
- visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*);
- sfuggire agli antivirus in commercio.

L'evidente capacità di penetrazione nella sfera privata dell'individuo rende il captatore uno strumento probatorio eccezionale, sempre più indispensabile per la lotta alla criminalità, in particolare per i reati più gravi come la mafia e il terrorismo.

3. Uso tipico del captatore informatico

Con la L. 23 giugno 2017, n. 103, *Modifiche al Codice penale, al codice di procedura penale e all'ordinamento penitenziario*, la cd. "Riforma Orlando", il legislatore ha deciso di disciplinare solamente una tra le diverse attività che il captatore informatico è in grado di compiere: l'intercettazione di comunicazioni, anche detta "intercettazione ambientale". L'intervento normativo si è innestato nell'ambito della disciplina delle intercettazioni, modificando il co. 2 dell'articolo 266 c.p.p., il quale ora prevede che l'intercettazione di

[19] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista brasileira de direito processual penal*, *3*(2, 2017), p. 484 ss., https://doi.org/10.22197/rbdpp.v3i2.71

[20] Cass., Sez. Un., 01 luglio 2016, n. 26889, sentenza Scurato.

comunicazioni tra presenti possa essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile.
Negli anni successivi, il legislatore è nuovamente intervenuto, ampliando il raggio d'azione del captatore informatico. La L. 9 gennaio 2019 n. 3, legge c.d. "Spazza corrotti", ne ha infatti esteso l'utilizzo anche ai delitti dei pubblici ufficiali contro la Pubblica Amministrazione, se i reati commessi prevedono una reclusione non inferiore a 5 anni. La L. 8 febbraio 2020 n.7, ha inoltre aggiunto che il captatore può essere impiegato anche per i delitti commessi dagli incaricati di servizio pubblico.

Nel mondo contemporaneo, in cui le persone ricorrono costantemente nell'arco della giornata ai dispositivi smart per funzioni individuali e relazioni sociali, l'utilizzo del captatore come "cimice informatica" comporta la crescente possibilità che l'intercettazione avvenga anche in luoghi privati come, ad esempio, il domicilio. Esso è tutelato da diversi articoli della Costituzione: l'art. 13 definisce la libertà personale come inviolabile senza una previsione di legge e un atto motivato dell'autorità giudiziaria e l'art. 14 sancisce l'inviolabilità del domicilio, tranne nei casi stabiliti dalla legge[21].
La legge prevede particolari cautele quando le comunicazioni avvengano nei luoghi stabiliti dall'art. 614 c.p., cioè nei luoghi domiciliari riferibili al soggetto sottoposto ad indagini. In particolare, 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* c.p.p.). È però prevista una deroga a tale previsione qualora si tratti di "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 ufficiali o 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" (art. 266 co. 2 bis c.p.p.)[22]. In queste ipotesi, è sempre consentito l'uso del captatore. Si è ritenuto che una simile scelta, pur implicando un'intrusione più significativa nella sfera privata del cittadino, risulti indispensabile per contrastare da un lato gli eventuali comportamenti illegali tenuti da parte di pubblici ufficiali nei confronti

[21] Artt. 13-14 Costituzione, https://www.senato.it/istituzione/la-costituzione

[22] F. PALMIOTTO, *Captatori informatici e diritto alla difesa, il caso Exodus*. In *La legislazione penale* (2020), p. 3 ss: https://www.lalegislazionepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf

della Pubblica Amministrazione (e quindi nei confronti dello Stato) e dall'altra le più gravi fattispecie criminali, come la criminalità organizzata e il terrorismo.

L'uso del captatore nelle indagini deve essere autorizzato dal giudice. In particolare, l'art. 267 co. 1 c.p.p. prevede che il giudice per le indagini preliminari rilasci, mediante un decreto motivato, l'autorizzazione per condurre le operazioni previste dall'articolo 266 quando esistono prove consistenti di un possibile reato e quando l'intercettazione è assolutamente necessaria per continuare le indagini. Il decreto deve specificare le ragioni per cui questa modalità è essenziale per il progresso delle indagini. Inoltre, se l'indagine riguarda reati diversi da quelli specificati nell'articolo 51, paragrafi 3-bis e 3-quater, o da reati commessi da pubblici ufficiali o incaricati di pubblico servizio contro la pubblica amministrazione, per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, (come stabilito dall'articolo 4), il decreto deve specificare i luoghi e il periodo di tempo, anche in modo indiretto, in cui è permesso attivare il microfono.

La disciplina di esecuzione delle operazioni di intercettazione è prevista all'art. 268 c.p.p. ss. Le comunicazioni intercettate sono oggetto di registrazione e documentazione attraverso la stesura di un verbale (art. 268 co. 1 c.p.p.), soggetto alla supervisione del Pubblico Ministero al fine di tutelare la privacy e la reputazione delle persone intercettate, in particolare se estranee all'indagine (art. 268 co. 2 c.p.p.).
Le intercettazioni devono essere effettuate di regola tramite strumenti installati dalla/presso la Procura. Tuttavia, viste le limitazioni tecniche delle Procure, è consentito utilizzare anche altri impianti di pubblico servizio o quelli a disposizione della Polizia Giudiziaria (art. 268, comma 3, c.p.p.). Infatti, l'art. art. 348, comma 4, c.p.p. prevede che la polizia giudiziaria, se priva delle competenze tecnico/informatiche necessarie, possa avvalersi di persone qualificate nella gestione e utilizzo del captatore.
Il coinvolgimento e, in alcuni casi, l'affidamento dell'attività di intercettazione a soggetti privati è un tema che ha fatto sorgere numerose perplessità nel dibattito giuridico, in particolare dopo le rivelazioni sconcertanti del caso Exodus[23]. Nel 2019 l'indagine della ONG *Security Without Borders* ha dimostrato che centinaia di dispositivi di utenti italiani

[23] C. ANESI, R. ANGIUS, P. PETRASSO, *Exodus e non solo: le ombre sul mercato dei trojan di stato*, in *Wired*, 2019), https://www.wired.it/attualita/tech/2019/11/19/exodus-trojan-stato/

(anche non indagati) sarebbero stati infettati da Exodus, un *malware* progettato da una società calabrese e utilizzato da molte Procure, che ha esposto una quantità imprecisata di cittadini ad intercettazioni illegali[24].

Il materiale raccolto dalle intercettazioni e le relative documentazioni vengono custodite in un archivio digitale (art. 269 c.p.p.), al quale il giudice per le indagini preliminari e i difensori hanno diritto di accedere.
Al termine delle indagini, il captatore deve essere disattivato e, secondo l'art. 267 c.p.p., il termine di conservazione dei dati raccolti corrisponde al passaggio in giudicato della sentenza[25].
Le intercettazioni non sono utilizzabili se ottenute al di fuori dei casi previsti dalla legge o se non sono state rispettate le disposizioni specifiche in materia (artt. 267-268 c.p.p.). Inoltre, anche l'acquisizione al di fuori dei limiti di tempo e luogo indicati nel decreto autorizzativo comporta l'inutilizzabilità in giudizio.

L'utilizzazione delle risultanze ottenute mediante intercettazione in altri procedimenti è un tema che ha acceso un vivace dibattito tra dottrina e giurisprudenza[26]. Il legislatore è intervenuto, modificando l'art. 270 c.p.p. e, in particolare, il co. 1[27] che ora prevede "i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'articolo 266, comma 1".

---

[24] M. C. FALCHI, *Captatore informatico: i rischi di una mancata puntuale regolamentazione,* in *Ius in itiner*e, 2021, https://www.iusinitinere.it/captatore-informatico-i-rischi-di-una-mancata-puntuale-regolamentazione-29697

[25] F. PALMIOTTO, *Captatori informatici e diritto alla difesa, il caso Exodus*, in *La legislazione penale*, 2020, p. 4 ss., https://www.lalegislazionepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf.

[26] W. NOCERINO, A. ZAMPINI, *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, v. 7, n. 2, p. 1434 ss., in https://core.ac.uk/download/478497026.pdf.

[27] Il comma modificato dall'art. 2 comma 1, lettera g) del D. L. 30 dicembre 2019, n. 161, convertito con modificazioni dalla L. 28 febbraio 2020, n. 7. Il D.L. 30 dicembre 2019, n. 161, convertito con modificazioni dalla L. 28 febbraio 2020, n. 7, ha disposto (con l'art. 2, comma 8) che "Le disposizioni del presente articolo si applicano ai procedimenti penali iscritti successivamente al 30 aprile 2020".

La norma rafforza le condizioni che autorizzano l'utilizzo delle risultanze in procedimenti diversi da quelli indicati nel decreto autorizzativo attraverso l'introduzione del requisito della "rilevanza", in aggiunta a quello dell' "indispensabilità investigativa".
Così facendo, il legislatore ha notevolmente ampliato l'ambito di operatività nell'utilizzare il materiale captato in procedimenti diversi, integrando anche nel caso specifico l'intercettazione mediante l'uso del captatore informatico[28]. Infatti, oltre all'art. 270 co. 1 c.p.p., l'intervento legislativo prevede alcune modifiche alla disciplina delle intercettazioni effettuate mediante il captatore. In particolare, si prevede che i risultati delle intercettazioni tra presenti, operate con captatore informatico su dispositivo elettronico portatile, possano essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, purché essi siano indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza [29].
In questo modo rischia di perpetrarsi una violazione della riserva di giurisdizione prevista dall'art. 15 della Costituzione. Infatti, la circolazione delle risultanze anche per procedimenti diversi comporta il concreto rischio che le informazioni acquisite dal trojan circolino praticamente liberamente, senza che un giudice abbia autorizzato l'intercettazione[30].

Per concludere l'illustrazione del quadro normativo relativo alle intercettazioni compiute mediante l'utilizzo del captatore informatico, occorre citare anche gli artt. 191 c.p.p. e 271 c.p.p., i quali prevedono l'inutilizzabilità delle prove acquisite qualora fossero stati violati i divieti stabiliti dalla legge o qualora fossero state ottenute al di fuori delle ipotesi consentite dalla legge. Le due norme regolano i casi in cui il materiale raccolto sia viziato da inutilizzabilità. Le ipotesi previste sottraggono inevitabilmente al giudice elementi

[28] Suscitando non poche critiche, vedi ad esempio: W. Nocerino, A. Zampini, *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, v. 7, n. 2, p. 1441, in https://core.ac.uk/download/478497026.pdf

[29] Legge n. 7 del 2020 che modifica l'art. 2, comma 1, lett. *g*, d.l. n. 161 del 2019.

[30] W. NOCERINO, A. ZAMPINI, *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, v. 7, n. 2, p. 1440 ss, in https://core.ac.uk/download/478497026.pdf

conoscitivi potenzialmente decisivi nella ricostruzione dei fatti, aprendo un potenziale dibattito valoriale[31].

[31] W. NOCERINO, A. ZAMPINI, *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in *Rev. Bras. de Direito Processual Penal*, Porto Alegre, v. 7, n. 2, p. 1415 ss, in https://core.ac.uk/download/478497026.pdf

2. Uso atipico del captatore informatico

Il captatore informatico è "uno strumento probatorio dalle formidabili capacità di penetrazione nella sfera privata dell'individuo"[32], il cui utilizzo non può prescindere da un attento bilanciamento tra le esigenze investigative e il rispetto dei diritti individuali che rischiano di subire gravi lesioni.

Il legislatore ha tipizzato solamente una tra le diverse potenzialità dello strumento: l'intercettazione di comunicazioni. Rimangono senza una definizione legislativa tutti gli altri utilizzi possibili, la cui sorte è oggetto di vivaci dibatti e preoccupazioni tra gli operatori coinvolti, soprattutto per l'intrusione nella sfera privata dei soggetti (anche non indagati) che essi sono in grado di compiere. I quesiti principali che bisogna porsi sono i seguenti: gli investigatori possano utilizzare il captatore, sfruttando le funzioni non disciplinate dal Legislatore? E, se la risposta fosse affermativa, quali sarebbero le basi normative per permettere alle prove ricavate di entrare in giudizio?

Il problema è presente e reale. Infatti, varie sentenze[33] hanno evidenziato che nella prassi investigativa c'è la tendenza ad utilizzare il *trojan* al di fuori del suo perimetro tipico, per compiere attività riconducibili *all'online search* e *online surveillance*, operazioni atipiche che permettono di ottenere una quantità di informazioni potenzialmente illimitata[34].

La questione viene affrontata in dottrina e giurisprudenza, analizzando l'uso atipico da diversi punti di vista: c'è chi cerca di farlo rientrare nei mezzi di ricerca della prova già disciplinati dal Codice penale, chi utilizza l'art. 189 c.p.p. come "scudo protettivo" per renderne lecito l'uso atipico; ancora c'è chi cerca di utilizzare l'art. 266 c.p.p. per far rientrare nel concetto di intercettazione anche gli altri utilizzi del captatore.

---

[32] F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista brasileira de direito processual penal*, *3*(2) 2017, p. 483-510, https://doi.org/10.22197/rbdpp.v3i2.71

[33] Cass., 16 dicembre 2020, n. 36061, in Sist. pen., 11 gennaio 2021, in cui si fa un cenno alle "altre modalità tecniche meno invasive", con ciò presupponendo usi ulteriori del virus; Id., Sez. V, 18 marzo 2019, n. 15071, in C.E.D. Cass., n. 275104, in cui il captatore informatico viene equiparato ad uno "spy-software".

[34] Cass., sez. V, 20 ottobre 2017, n. 48370, cit., p. 2505, "captazione in tempo reale di un flusso di dati intercorso su un determinato schermo o all'interno di un supporto [...] nonché la documentazione relativa ad un flusso unidirezionale di dati confinati all'interno dei circuiti del computer".

1. Affinità e differenze con i mezzi tradizionali di ricerca della prova

Si è anzitutto tentato di trovare una collocazione normativa all'uso atipico del captatore, in particolare le attività di *online search*, facendolo rientrare nella disciplina dei tradizionali mezzi di ricerca della prova. In particolare, quelli che ne condividono alcune somiglianze sotto il profilo dei risultati investigativi: l'ispezione[35] (art. 244 ss. c.p.p.); la perquisizione[36] (art. 247 ss. c.p.p.); e il sequestro probatorio[37] (art. 253 ss. c.p.p.). Si tratta tre strumenti che con la legge 48/2008[38] sono stati adeguati all'evoluzione tecnologica e al ruolo sempre più importante del dato digitale. Un aspetto in comune tra il captatore e questi mezzi di ricerca della prova è sicuramente la finalità perseguita: cercare di acquisire documenti e dati necessari per accertare un determinato fatto.

Tuttavia, i primi problemi si verificano quando ci si imbatte nelle regole processuali che presidiano tali istituti, le quali rappresentano un limite difficilmente superabile per l'inclusione delle attività di intrusione, ricerca e acquisizione condotte mediante il captatore nel *genus* dei mezzi di ricerca della prova tipici[39].

Anzitutto, le ispezioni e le perquisizioni mirano "ad uno scopo ben preciso, circoscrivendo l'oggetto della 'ricerca' (tracce, effetti materiali del reato)"[40]. Al contrario, l'attività del captatore non mira ad acquisire elementi specifici, ma consiste in un'acquisizione indiscriminata dei dati all'interno del *device*.

Inoltre, tenendo conto del principio di proporzionalità nella limitazione delle libertà fondamentali, si evidenziano altre due evidenti differenze.

---

[35] Mezzo di ricerca della prova quando occorre accertare le tracce e gli altri effetti materiali del reato, ovvero descrivere lo stato dei luoghi.

[36] Mezzo di ricerca della prova utilizzato allo scopo di rinvenire sulla persona o in luogo cose pertinenti al reato, o il corpo del reato stesso.

[37] Mezzo di ricerca della prova il cui fine è di acquisire elementi necessari alla ricostruzione del fatto.

[38] Con riferimento alle ispezioni, è stato modificato il comma 2 dell'art. 244 c.p.p. che legittima l'autorità a compiere operazioni tecniche anche su sistemi e supporti informatici, adottando misure necessarie ad assicurare l'integrità e la conservazione. In materia di perquisizioni, l'art. 8 comma 2, l. 48/2008 ha introdotto il comma 1-bis all'art. 247 c.p.p., che recita: "Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". Infine, in tema di sequestro sono state aggiornate le norme (art. 254 c.p.p. ss.), adeguando la disciplina nei casi in cui l'attività di ricerca coinvolga dati informatici.

[39] W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021, pp. 168 ss.

[40] W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021, p. 169.

La prima riguarda le garanzie difensive che l'ordinamento riconosce alla difesa; infatti, è previsto che, qualora le indagini richiedano mezzi investigativi quali l'ispezione, la perquisizione e il sequestro, la difesa venga avvisata prima (art. 364 c.p.p.), durante o dopo (art. 250 c.p.p. e art. 253 c.p.p.) il compimento dell'atto. Ad esempio, l'art. 364 c.p.p. prevede che, nel caso di ispezioni, al difensore venga dato avviso almeno ventiquattro ore prima del compimento dell'atto.

Sono disposizioni che offrono garanzie difensive alla persona sottoposta alle indagini, in quanto operano un bilanciamento tra esigenze investigative ed il diritto alla difesa. Invece, già dalla denominazione di *trojan horse* si evince la natura occulta dello strumento adottato. D'altra parte, avvisare l'indagato della presenza dell'agente intrusore equivarrebbe a vanificarne l'efficacia investigativa.

La seconda differenza riguarda la temporaneità delle operazioni. Infatti l'ispezione, la perquisizione e il sequestro devono concludersi nel tempo indicato nel decreto autorizzativo, cioè il tempo necessario per il compimento dell'atto. Invece, il *trojan* si introduce in maniera permanente nel *device* acquisendo in maniera indiscriminata informazioni e dati[41].

È quindi evidente che, nonostante alcuni limitati aspetti in comune, il captatore non possa trova "asilo" all'interno dei mezzi di ricerca della prova tradizionali.

2. La prova atipica

Come si è detto, al di fuori dell'utilizzo disciplinato dall'art. 266 co. 2 c.p.p., tutte le altre funzioni del captatore sono prive di una specifica regolamentazione. Ciò potrebbero portare a ritenere che esse vadano etichettate come attività investigative insuscettibili di fornire materiali probatori utilizzabili in giudizio (art. 191 c.p.p.). Tuttavia, il processo penale italiano non prevede un principio di tassatività della prova e dunque non viene esclusa a priori l'utilizzabilità delle prove atipiche[42]. Infatti, il giudice "può assumere

[41] W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021, p. 171.

[42] Oltre all'articolo 189 c.p.p., ci sono altri articoli nell'ordinamento che autorizzano la Polizia giudiziaria e il Pubblico Ministero a compiere atti di indagine anche non espressamente disciplinati dalla legge. L'art. 55 c.p.p. stabilisce che "La polizia giudiziaria deve, anche di propria iniziativa, prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale", mentre l'articolo 348 c.p.p. prevede che il pubblico

anche prove[43] non disciplinate dalla legge" (art. 189 c.p.p.). Il giudice dovrà comunque effettuare un'attenta analisi allo scopo di valutare se la prova atipica rispetti le tre condizioni previste dall'art. 189 c.p.p. Egli "[..] può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova". Il legislatore richiede quindi il rispetto di tre requisiti: che le prove atipiche devono essere affidabili sul piano della genuinità dell'accertamento dei fatti; non devono ledere la libertà morale della persona; infine, trattandosi di una prova non disciplinata dal legislatore, il giudice dovrà rivolgersi alle parti e prescrivere le modalità di assunzione della prova. L'art. 189 c.p.p. è da considerarsi una norma necessaria per evitare esagerate restrizioni ai fini dell'accertamento della verità, in ragione del rapido e continuo sviluppo tecnologico che amplia notevolmente gli strumenti investigativi a disposizione.

Il primo e il secondo requisito possono ritenersi soddisfatti, poiché è evidente che il *trojan* è in grado di accertare i fatti. Inoltre, una importante sentenza della Corte di Cassazione ha escluso che il captatore sia uno strumento in grado di pregiudicare la libertà morale delle persone coinvolte nell'indagine[44].

Secondo la dottrina, il requisito del contraddittorio tra le parti può essere soddisfatto a posteriori poiché un contraddittorio *ex ante* eliminerebbe praticamente *in toto* l'utilità dell'azione investigativa, in quanto il soggetto *target* verrebbe a conoscenza delle finalità degli investigatori.

Quindi, dopo un'analisi dell'art. 189 c.p.p., si potrebbe ritenere che in linea di principio l'utilizzo del captatore come mezzo di ricerca della prova atipico possa essere ammesso entro certi limiti. Tuttavia, tra gli esperti si registrano inevitabilmente diverse posizioni.

---

ministero possa compiere ogni attività necessaria, anche se atipica, per assumere le determinazioni inerenti all'esercizio dell'azione penale.

[43] Per la verità, tale norma si riferisce alle prove non disciplinate e non ai mezzi di ricerca della prova atipici; ma, secondo la dottrina più accreditata è possibile – con un'interpretazione elastica – far rientrare anche gli atti investigativi atipici nella norma.

[44] Secondo Cass. pen., Sez. V, 11 novembre 2020 (ud. 30 settembre 2020), n. 31604 "va escluso che il captatore informatico possa inquadrarsi tra i 'metodi o le tecniche' idonei ad influire sulla libertà di determinazione del soggetto, come tali vietati dall'art. 188 cod. proc. pen." dal momento che lo stesso "non esercita alcuna pressione sulla libertà fisica e morale della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità»".

Secondo l'indirizzo prevalente in dottrina (e nella giurisprudenza), la prova non regolata dalla legge che violi i diritti fondamentali va considerata inammissibile[45]; secondo l'altra, le prove atipiche andrebbero considerate ammissibili finché l'art. 189 c.p.p. non verrà dichiarato parzialmente illegittimo dalla Corte Costituzionale[46].

3. I diritti fondamentali costituzionalmente tutelati

Per poter ammettere l'utilizzo atipico del captatore informatico come mezzo di ricerca della prova non è sufficiente lo "scudo protettivo" dell'art. 189 c.p.p., ma è anche necessario verificare se lo strumento lede i diritti fondamentali.

Ci si riferisce, in particolare, al diritto alla libertà personale (art. 13, Costituzione[47]), al diritto all'intimità domiciliare (art. 14, Costituzione[48]) e al diritto alla libertà e alla segretezza delle comunicazioni (art. 15, Costituzione[49]). Le attività investigative che violano questi tre diritti fondamentali devono essere previste tassativamente dalla legge. Infatti, una loro limitazione è legittima solo se autorizzata con atto motivato dall'autorità giudiziaria (riserva di giurisdizione) e nei casi e modi previsti dalla legge (riserva di legge)[50].

Ne consegue che l'attività investigativa svolta mediante l'utilizzo atipico del captatore informatico, non essendo disciplinata dal Legislatore, debba ritenersi incostituzionale e pertanto non sfruttabile.

La Corte Costituzionale sembra aderire a questa impostazione, avendo dichiarato in più occasioni l'inutilizzabilità dei risultati probatori di un'attività di ricerca della prova

---

[45] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista brasileira de direito processual penal*, *3*(2) 2017, p. 488, https://doi.org/10.22197/rbdpp.v3i2.71

[46] F. CORDERO, *Procedura penale*, Milano, Giuffrè, 2003, p. 848.

[47] Articolo 13, Costituzione: "La libertà personale è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge […]".

[48] Articolo 14 , Costituzione: "Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale […]".

[49] Articolo 15, Costituzione: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

[50] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista brasileira de direito processual penal*, *3*(2) 2017, p. 486 ss, URL: https://doi.org/10.22197/rbdpp.v3i2.71

direttamente lesiva di un diritto costituzionalmente garantito[51]. Secondo la sentenza 34/1973[52] della Corte Costituzionale, "le attività compiute in dispregio dei diritti fondamentali del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito". In una successiva sentenza[53], la Corte Costituzionale ha poi confermato che "non possono validamente ammettersi in giudizio mezzi di prova che siano stati acquisiti attraverso attività compiute in violazione delle garanzie costituzionali poste a tutela dei fondamentali diritti dell'uomo e del cittadino".

4. I diritti fondamentali riconosciuti a livello europeo

A livello internazionale, anche l'art. 8 della *Convenzione europea dei diritti dell'uomo* (CEDU)[54] tutela l'individuo, prevedendo che eventuali limitazioni dei suoi diritti (vita privata, domicilio e corrispondenza) siano "previste dalla legge" e "necessarie in una società democratica". La concezione di "legge" a livello europeo è meno stringente rispetto alla definizione italiana, in quanto la Corte Europea dei Diritti dell'Uomo accoglie un concetto di legge più ampio, che ricomprende – oltre alla tradizionale legge ordinaria prodotta dai Parlamenti nazionali – le fonti di rango inferiore e il diritto giurisprudenziale. Le condizioni di legittimità dell'ingerenza pubblica sono disciplinate dal già citato articolo 8 CEDU e dagli articoli 7, 8 e 52 della *Carta dei diritti fondamentali dell'Unione europea*[55]. Affinché una norma possa fungere da base normativa per una limitazione dei diritti fondamentali dell'individuo deve essere: sufficientemente "chiara

[51] V. FRACASSO, *"Liberi tutti" nell'utilizzo del trojan di Stato?*, In *Giurisprudenza Penale Web*(10) 2022, pp. 17, https://www.giurisprudenzapenale.com/2022/10/03/liberi-tutti-nellutilizzo-del-trojan-di-stato/

[52] Sentenza n. 34/1973 Corte Costituzionale, in Consulta Online, https://giurcost.org/decisioni/1973/0034s-73.html

[53] Sentenza n. 81/1993 Corte Costituzionale, in Consulta Online, https://giurcost.org/decisioni/1993/0081s-93.html

[54] Articolo 8, *Diritto al rispetto della vita privata e familiare*: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria […]".

[55] Articolo 7, *Rispetto della vita privata e della vita familiare*: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni"; articolo 8, *Protezione dei dati di carattere personale*: "Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano […]"; articolo 52, *Portata dei diritti garantiti*: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà".

e precisa" per il destinatario; "accessibile" e "prevedibile"[56] in relazione ai suoi effetti. Inoltre, la Corte Europea ha stabilito le garanzie minime che le normative riguardanti l'utilizzo di strumenti di sorveglianza/intrusione devono rispettare in modo tale da evitare un'ingerenza eccessiva e ingiustificata da parte dello Stato. Sono necessarie dunque: l'indicazione dei presupposti fattuali della captazione e della natura dei reati che autorizzano la misura; la definizione delle categorie di persone in rapporto alle quali la captazione può essere svolta; i limiti di durata delle intercettazioni; la procedura da seguire per l'esame, l'archiviazione e la cancellazione dei dati ottenuti; le precauzioni da prendere al momento di comunicare i dati a soggetti terzi[57].

Infine, per poter essere legittimo l'intervento dello Stato, il test di "necessità e proporzionalità" deve dare esito positivo. Esso permette infatti di bilanciare l'interesse pubblico nella prevenzione e repressione dei reati – che giustifica l'uso di misure di sorveglianza occulta – con le libertà e i diritti fondamentali degli individui. Il test richiede di valutare preliminarmente la pertinenza e l'idoneità della misura adottata dallo Stato in relazione all'obiettivo legittimo perseguito. Inoltre, bisogna verificare se l'interesse pubblico non possa essere raggiunto con misure meno invasive e che le deroghe o le restrizioni ai diritti fondamentali dei singoli siano limitate al minimo necessario. È fondamentale, nello scrutinio di proporzionalità, la presenza di adeguate ed efficaci garanzie per evitare abusi e ingerenze eccessive.

Di volta in volta il giudice è chiamato a valutare, attraverso il test, se l'utilizzo del *trojan* possa rispettare concretamente tutti questi dettami e, di conseguenza, ritenersi legittimo. Sicuramente, nessun'altro strumento investigativo attualmente in possesso delle autorità investigative permette di ottenere le informazioni che il captatore è in grado di acquisire dal dispositivo infettato; tuttavia, come detto in precedenza, la maggior parte delle capacità dello strumento sono completamente prive di una definizione legislativa che le autorizzi e ne disciplini le modalità di utilizzo. Inoltre, allo stato attuale mancano le

---

[56] F. GRAZIANI, *La ricerca della prova digitale mediante captatore informatico nella prassi degli Stati e nell'ordinamento italiano: il difficile equilibrio tra prevenzione dei reati e tutela della riservatezza informatica*, in *La comunità internazionale,* 2019, Vol. LXXIV, pp. 400 ss., https://www.comunitainternazionale.it/uploads/model_4/.files/13_item_2.pdf?v=1588581399

[57] Corte europea dei diritti umani, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Roman Zakharov c. Russia*, par. 231.

garanzie necessarie per evitare il verificarsi di abusi o intercettazioni ben oltre il consentito.

5. Gli aspetti critici in relazione all'ordinamento italiano

Un ulteriore ostacolo insormontabile per l'uso atipico del captatore è dato dall'art. 615 *ter* c.p., il quale prevede che un'intrusione abusiva in un sistema informatico o telematico costituisca un reato punibile con la reclusione. Il domicilio informatico, inteso quindi come un'estensione del domicilio classico tutelato dall'ordinamento, diventa cioè uno spazio autonomo e separato dall'esterno, anche grazie a misure di sicurezza come, ad esempio, la password[58]. Per la Cassazione[59] il sistema informatico "costituisce uno dei luoghi di espressione della personalità dell'individuo, all'interno del quale l'interessato conserva i dati personali la cui diffusione ed utilizzo possono essere solo da lui decisi". Il "domicilio informatico" mantiene la stessa protezione riconosciuta al "domicilio" dall'articolo 14 Cost.

La sentenza n. 3067/1999[60] della Corte di Cassazione Penale ha accolto la nozione di domicilio informatico come "spazio ideale (ma anche fisico in cui sono contenuti i dati informatici), di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art. 14 Cost.)". L'attività di *online search* del *trojan* rientra perfettamente nella fattispecie criminosa prevista dall'articolo 615 *ter* del Codice Penale e, di conseguenza, è un'attività vietata dall'ordinamento e sanzionata penalmente.

6. Ipotesi di inserimento nella disciplina delle "intercettazioni"

Si è poi tentato di far rientrare le attività atipiche del captatore – in particolare le funzioni di *online search* (come, ad esempio, lo *screenshot*) – nell'alveo delle intercettazioni[61], attribuendo agli elementi raccolti il valore di "flusso di comunicazione". Ciò significa ritenere che, ad esempio, un *file* di testo *word* contenuto nel computer di un indagato abbia

[58] V. FRACASSO, *"Liberi tutti" nell'utilizzo del trojan di Stato?*, in *Giurisprudenza Penale Web*(10) 2022, pp. 15 ss, https://www.giurisprudenzapenale.com/2022/10/03/liberi-tutti-nellutilizzo-del-trojan-di-stato/

[59] Cass. Sez. V, 18 dicembre 2012, Valenza.

[60] Sentenza n. 3067/1999, https://www.penale.it/giuris/cass_012.htm

[61] V. FRACASSO, "Liberi tutti" nell'utilizzo del trojan di Stato?, in Giurisprudenza Penale Web (10) 2022, pp. 7 ss, https://www.giurisprudenzapenale.com/2022/10/03/liberi-tutti-nellutilizzo-del-trojan-di-stato/

un "comportamento comunicativo" e di conseguenza diventi intercettabile. Ma la soluzione appare molto forzata, poiché sembra cozzare con la natura e i presupposti delle intercettazioni nel nostro ordinamento, le quali possono essere autorizzate solo quando debba essere effettuata una captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti[62]. Analogamente l'art. 266 *bis* c.p.p. consente esclusivamente "l'intercettazione del flusso di comunicazioni[63] relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi".

La Corte di Cassazione[64] definisce "comportamenti comunicativi" "gli atti finalizzati a trasmettere il contenuto di un pensiero con la parola, i gesti, le espressioni fisiognomiche o altri atteggiamenti idonei a manifestarlo, mentre sono comportamenti 'non comunicativi' [...] tutti quelli, diversi dai primi, che rappresentano la mera presenza di cose o persone ed i loro movimenti, senza alcun nesso funzionale con l'attività di scambio o trasmissione di messaggi tra più soggetti"[65]. Appare quindi evidente la forzatura nel ritenere intercettabili dati informatici che non sono oggetto di una comunicazione.

7. Un'incerta collocazione sistematica

In conclusione, l'uso atipico del captatore nell'attuale quadro normativo sembra non poter trovare una sua collocazione. Non può rientrare nell'alveo dei tradizionali mezzi di ricerca della prova, nonostante esso presenti alcune somiglianze con questi ultimi. Sotto un diverso profilo, lo "scudo protettivo" del 189 c.p.p. non sembra sufficiente, poiché le attività atipiche (come l'*online search*) violano direttamente l'art. 14 della Costituzione

[62] (Cass. Sez. Un., 25.5.2003, n. 36747, *Torcasio*).

[63] Secondo la sentenza Viruso (Cass. Sez. 5, 14.10.2009 n. 16556) "per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro [...] non potendo ritenersi sufficiente l'elaborazione del pensiero e l'esternazione, anziché mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato", trovandosi altrimenti al cospetto "non [di] un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma [...] [di] "un flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer".

[64] Cass. Sez. III, 21 .11.2019 n. 15206.

[65] G. FROVA, *La Cassazione sulla riconducibilità all'art. 266 c.p.p. degli screenshot tramite captatore informatico*, in *Sistemapenale.it*, 2022, https://www.sistemapenale.it/it/scheda/cassazione-2022-3591-screenshot-captatore-informatico-online-surveillance

e, inoltre, integrano il reato previsto dall'art. 615 *ter* c.p.. Dal canto loro, la Corte Costituzionale e la Convenzione Europea dei Diritti dell'Uomo considerano illegittimi gli strumenti investigativi che ledono i diritti fondamentali e che non siano previsti dalla legge.

Tuttavia, è necessario anche ricordare che il *trojan*, sfruttando le sue funzionalità atipiche, permette di ottenere una quantità di informazioni fondamentali anche e soprattutto nelle indagini che hanno ad oggetto reati particolarmente gravi e pericolosi per la collettività.

È sicuramente necessaria un'analisi attenta degli interessi in gioco per cercare di arrivare ad una soluzione che possa garantire un giusto bilanciamento tra tutela degli individui ed esigenze investigative.

Un auspicabile futuro intervento del legislatore dovrà tenere presenti non solo le questioni prettamente giuridiche, ma anche gli aspetti tecnici e informatici dello strumento. Sarebbe opportuno affidare ad esperti qualificati nel campo della *digital forensics* il compito di "mappare" tutte le possibili attività che può compiere il *trojan horse* e definire in maniera chiare le varie fasi di "vita" del *malware* e, in particolare, la fase di disattivazione.

8. Il noto caso *Exodus* tra protezione della *privacy* ed esigenze investigative

Il tema dell'uso atipico del captatore informatico coinvolge, come si è rilevato, interessi di primaria importanza ma che entrano in conflitto tra loro: da un lato, l'esigenza investigativa di acquisire prove digitali da utilizzare nei procedimenti penali (in particolare per i reati di criminalità organizzata e terrorismo); dall'altro, la tutela dei diritti fondamentali dei soggetti coinvolti, protetti a livello costituzionale e sovranazionale.

Un esempio paradigmatico di tale conflitto è rappresentato dal noto caso *Exodus*, dove emergono le criticità che derivano dagli usi atipici non autorizzati del captatore e le gravi lacune della disciplina normativa in materia.

Exodus era un *malware* che è stato sviluppato dall'azienda calabrese E-surv per acquisire informazioni dai dispositivi sui quali veniva installato e che è stato utilizzato come *trojan* nell'ambito di indagini penali da circa il 80-90% delle Procure italiane[66].

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

Nel marzo del 2019, grazie al lavoro dei giornalisti di *Motherboar* e ai ricercatori di *Security Without Borders*, si è scoperto che il *malware* era "nascosto" in alcune app, all'apparenza innocue, presenti sul *Google Play Store*. Le app promettevano servizi di ottimizzazione delle prestazioni del dispositivo e promozioni, attirando l'attenzione di soggetti interessati a tali servizi. Chiunque le scaricasse veniva esposto ad una intercettazione illegale da parte di una società privata, senza essere indagato e senza un'autorizzazione di un giudice. Le risultanze acquisite dal *malware* venivano raggruppate in due cartelle in base al tipo: i *demo*, cioè gli indagati dalle Procure italiane; e *volontari*, cioè i soggetti che avevano installato l'app convinti che offrisse le prestazioni dichiarate. A quanto emerge dalle indagini, almeno 400 telefoni sono stati infettati e intercettati senza autorizzazione.

Ma la questione ancora più sconcertante è stata scoperta dalla Procura di Benevento nel 2018, mentre la polizia stava svolgendo un'indagine mediante l'uso del captatore (autorizzato dal giudice) sul telefono dell'indagato. La procedura di accesso ai computer per visionare le risultanze ottenute era molto semplice: inserire l'indirizzo IP fornito da E-Surv e digitare la password e lo username (senza ulteriori sistemi di sicurezza). Uno degli ufficiali di polizia giudiziaria, a causa dei continui malfunzionamenti del computer in questione, decise di riavviarlo. Per curiosità provò allo stesso tempo ad accedere al sito dal suo telefono personale, scoprendo che non solo era possibile accedere da qualsiasi dispositivo (in linea di principio solo i computer della Procura avrebbero potuto connettersi), ma anche che, una volta digitati lo *username* e la *password*, era possibile visionare tutte le altre intercettazioni effettuate dalla Procura di Benevento e da tutte le altre Procure italiane mediante il malware Exodus.

Diventava così possibile per chiunque avesse le credenziali accedere a *screenshot*, registri delle chiamate, rubriche telefoniche, dati di calendario e soprattutto anche ai nominativi di alcuni agenti di Polizia Giudiziaria, le cui identità venivano esposte.

Inoltre, secondo le notizie giornalistiche, il server della Procura di Benevento che avrebbe dovuto contenere i risultati delle intercettazioni dell'indagine penale in svolgimento (circa 4 terabyte di dimensione) era completamente vuoto, mentre tutti i dati ottenuti mediante *Exodus* si trovavano all'interno di un server *off-shore* situato negli Stati Uniti.

Il *malware* presentava evidenti criticità[67]:

- i criteri di sicurezza per accedere ai dati dell'indagine erano completamente insufficienti, poiché i server delle Procure erano accessibili da qualsiasi dispositivo, semplicemente con il nome utente e la password;
- la mancanza di una "*target valide procedure*", cioè della procedura per verificare se il dispositivo potesse essere legittimamente infettato o meno, con la conseguenza che chiunque scaricasse una delle app fittizie era esposto ad intercettazione illegale;
- la possibilità di visionare tutti materiali raccolti delle altre Procure che utilizzavano Exodus;
- la mancanza di un sistema di disinstallazione del *software* (infatti per *Security Without Borders* i dispositivi non sono mai stati "disinfettati");
- l'accessibilità a funzioni non tipizzate del captatore, come "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";
- il trasferimento dei dati in un server *off-shore* negli Stati Uniti d'America, azione che, secondo l'ex amministratore delegato dell'azienda, serviva per garantire una catena di anonimizzazione, impedendo ad eventuali *hacker* di risalire all'indirizzo IP della Procura. Tuttavia, il trasferimento in server diversi da quelli della Procura si pone in netto contrasto con l'art. 89 co. 3 disp. att. cpp, il quale prevede che le comunicazioni intercettate mediante captatore informatico siano conferite esclusivamente negli impianti della Procura della Repubblica.

Il caso ha ovviamente suscitato la reazione di diverse Procure italiane, le quali hanno iniziato ad indagare ufficialmente. Secondo la Procura di Napoli, il server di *Exodus* sarebbe stato usato per attività di dossieraggio e ricatto. Inoltre, diversi *gigabyte* di dati relativi a importanti procedimenti (anche relativi ad indagini sulla Ndrangheta) sarebbero spariti. Da questi fatti deriva l'ipotesi che il vero guadagno dell'azienda E-surv fosse la vendita di informazioni segrete e non il servizio di intercettazione in sé. Anche la Procura di Roma ha competenza in materia, dato che Exodus fu utilizzato anche dai servizi segreti

[67] F. PALMIOTTO, *Captatori informatici e diritto alla difesa, il caso Exodus.* In *La legislazione penale (2020)*, pp. 8 ss.,https://www.lalegislazionepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf

italiani (Aise e Aisi)[68]. Il Procuratore aggiunto del Tribunale di Roma decise di sentire il numero uno dell'Aise per avere delle spiegazioni in merito. L'ipotesi formulata dalla Procura fu che qualcuno all'interno dei servizi segreti possa aver effettuato intercettazioni abusive e non autorizzate, evento che, se confermato, risulterebbe ovviamente molto grave.

La questione ha interessato il Garante per la Protezione dei Dati Personali che ha ritenuto l'accaduto "un fatto gravissimo", aggiungendo, inoltre, questa valutazione: "emerge con evidenza inequivocabile la notevole pericolosità di strumenti, quali i captatori informatici, che per quanto utili a fini investigativi rischiano, se utilizzati in assenza delle necessarie garanzie anche soltanto sul piano tecnico, di determinare inaccettabili violazioni della libertà dei cittadini"[69].
Il Garante ha anche presentato nel luglio del 2019 una "segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico"[70], dalla quale emergono varie perplessità riguardo agli interventi del legislatore in materia e allo strumento in sé. Il documento sottolinea le caratteristiche dei *malware*, evidenziandone da un lato l'oggettiva utilità investigativa e, dall'altro, il pericolo che possano trasformarsi in "pericolosi strumenti di sorveglianza massiva". Il captatore informatico è definito uno strumento in grado di "concentrare in un unico atto una pluralità di strumenti investigativi (perquisizioni del contenuto del pc, pedinamenti con il sistema satellitare, intercettazioni di ogni tipo, acquisizioni di tabulati) ma anche, in talune ipotesi, di eliminare le tracce delle operazioni effettuate, a volta anche alterando i dati acquisiti". Il Garante critica gli interventi del Legislatore in materia – in particolare la "riforma Orlando" – ritenendo che la disciplina non contenga "garanzie adeguate per impedire che, in ragione delle loro

[68] C. ANESI, R. ANGIUS e P. PETRASSO, *Exodus, gli affari dietro il malware di stato che spiava gli italiani* e *Exodus e non solo: le ombre sul mercato dei trojan di stato*, in *Wired.it*, 2019, https://www.wired.it/attualita/tech/2019/11/18/exodus-malware-affari-italia/ e https://www.wired.it/attualita/tech/2019/11/19/exodus-trojan-stato/

[69] Garante per la protezione dei dati personali. (2019, marzo 30). "Caso Exodus" - Software spia: Soro, fatto gravissimo, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9100800

[70] Garante per la protezione dei dati personali. (2019, Aprile 30). Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9107773

straordinarie potenzialità intrusive, questi strumenti investigativi, da preziosi ausiliari degli organi inquirenti, degenerino invece in mezzi di sorveglianza massiva o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, rendendolo estremamente permeabile se allocato in server non sicuri o, peggio, delocalizzati anche al di fuori dei confini nazionali".

3. Conclusioni

Al termine della mia ricerca, vorrei condividere alcune considerazioni personali riguardo ad una auspicabile revisione della disciplina sull'uso del captatore informatico che dovrebbe essere sfruttato anche in tutte le sue funzionalità atipiche e non più solamente nelle intercettazioni.

Continuare ad impiegare il trojan senza sfruttarne appieno le potenzialità rischia di complicare notevolmente gli sforzi delle autorità nel contrastare il crimine e addirittura di favorire la criminalità stessa, in particolare quella organizzata e il terrorismo.

È fondamentale che il mondo politico si impegni in una profonda riflessione con l'obiettivo di apportare aggiornamenti significativi alla disciplina vigente. Gli esperti di *digital forensics* potrebbero fornire un contributo cruciale, dando al legislatore l'indispensabile supporto tecnico al fine di elaborare una nuova disciplina che trovi un punto di equilibrio soddisfacente tra le esigenze investigative e la tutela dei diritti individuali.

Inoltre, la nuova disciplina dovrebbe prevedere il miglioramento della *chain of custody* per garantire la completa tracciabilità del percorso di acquisizione, uso e conservazione delle prove digitali da parte delle autorità investigative.

Come si è evidenziato, spesso si è fatto affidamento su aziende private, poiché le procure e le autorità investigative non dispongono delle competenze informatiche e forensi necessarie per utilizzare e gestire direttamente il captatore. Tuttavia, vicende come quelle relative al caso Exodus hanno messo in luce i rischi del ricorso a soggetti esterni: dal pericolo di compromissione involontaria dei dati raccolti alla possibilità di sottrazioni volontarie di dati d'indagine per effettuare ricatti e dossieraggio.

Ne consegue che una nuova disciplina dovrebbe anche prevedere un rigoroso controllo sulle attività svolte dal personale e dagli amministratori delle società private che supportano le autorità e sugli strumenti utilizzati.

Infine, in una prospettiva ancora più ambiziosa, lo Stato potrebbe considerare l'ipotesi di sviluppare *software* propri e formare personale altamente specializzato, riducendo così la dipendenza da aziende private, che potrebbero privilegiare il profitto a discapito della sicurezza e della giustizia.

BIBLIOGRAFIA

A. ZAMPINI & W. NOCERINO, *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in *Revista Brasileira De Direito Processual Penal*, *7*(2) 2021, pp. 1411-1452
https://doi.org/10.22197/rbdpp.v7i2.504

C. ANESI , R. ANGIUS , P. PETRASSO, *Exodus e non solo: le ombre sul mercato dei trojan di stato*, in *Wired*, 2019
https://www.wired.it/attualita/tech/2019/11/19/exodus-trojan-stato/

C. MORELLI, *Le novità della legge di conversione sul DL intercettazioni*, in *Altalex,* 2020
https://www.altalex.com/documents/news/2020/02/28/trojan-di-stato-novita-intercettazioni

D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *JusOnline - Rivisita di Scienze Giuridiche, 2017* (n. 3), pp. 382-411
https://jus.vitaepensiero.it/news-papers-il-captatore-informatico-nella-legislazione-italiana-4843.html#_ftn3

E. LESTINI, *Captatore informatico: tra "tortura digitale" ed esigenze investigative*, in *Ius in Itinere, 2021*
https://www.iusinitinere.it/captatore-informatico-tra-tortura-digitale-ed-esigenze-investigative-35477

F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista brasileira de direito processual penal*, *3*(2) 2017, pp. 483-510, https://doi.org/10.22197/rbdpp.v3i2.71

F. GRAZIANI, *La ricerca della prova digitale mediante captatore informatico nella prassi degli Stati e nell'ordinamento italiano: il difficile equilibrio tra prevenzione dei*

reati e tutela della riservatezza informatica, in *La comunità internazionale*, Vol. LXXIV 2019, pp. 389-419
https://www.comunitainternazionale.it/uploads/model_4/.files/13_item_2.pdf?v=1588581399

F. PALMIOTTO, *Captatori informatici e diritto alla difesa*, il caso Exodus, in *La legislazione penale*, *2020*
https://www.lalegislazionepenale.eu/wp-content/uploads/2020/10/Palmiotto-Revisione-Finale.pdf

F. PALMIOTTO, *Le indagini informatiche e la tutela della riservatezza informatica*, in *La legislazione penale*, 2019
https://www.lalegislazionepenale.eu/wp-content/uploads/2019/06/Palmiotto-rubrica-speciale-Finale.pdf

G. FROVA*, La Cassazione sulla riconducibilità all'art. 266 c.p.p. degli screenshot tramite captatore informatico*, in *Sistemapenale*.it, 2022
https://www.sistemapenale.it/it/scheda/cassazione-2022-3591-screenshot-captatore-informatico-online-surveillance#:~:text=135)%2C%20nella%20giurisprudenza%20di%20legittimità,manifestarlo%2C%20mentre%20sono%20comportamenti%20“non

G. S. BASSI, *Il captatore informatico (cd. trojan horse) non rientra tra i metodi o le tecniche idonei ad influire sulla libertà di autodeterminazione del soggetto*, in *Giurisprudenza penale*, *2020*
https://www.giurisprudenzapenale.com/2020/11/15/il-captatore-informatico-cd-trojan-

G. DRAGONI, *Cos'è il Social Engineering, come difendersi e come riconoscerlo*, in *Osservatori.net*, 2023
https://blog.osservatori.net/it_it/social-engineering-come-difendersi

Garante per la protezione dei dati personali, *Parere sullo schema di decreto del Ministro della giustizia recante disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'articolo 7, commi 1 e 3, del decreto*, in *Garante privacy*, 2018
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8987309

Garante per la protezione dei dati personali, *Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*, in *Garante privacy*, 2019
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9107773

Garante per la protezione dei dati personali, "*Caso Exodus" - Software spia: Soro, fatto gravissimo*, in *Garante privacy*, 2019
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9100800

L. BARTOLI, C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, pp. 139-151
http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/IeD_2015_1-2_BartoliMaioli.pdf

M. A. SENOR, *Come funzionano i trojan di Stato?*, in *Altalex*, 2018
https://www.altalex.com/documents/news/2018/01/22/come-funzionano-i-trojan-di-stato

M. C. FALCHI, *Captatore informatico: i rischi di una mancata puntuale* regolamentazione, in *Ius in itiner*e, 2021
https://www.iusinitinere.it/captatore-informatico-i-rischi-di-una-mancata-puntuale-regolamentazione-29697

M. G. PUTATURO DONATI, *Il diritto al rispetto della «vita privata e familiare» di cui all'art. 8 della CEDU, nell'interpretazione della Corte Edu: il rilievo del detto principio sul piano del diritto internazionale e su quello del diritto interno,* in *Europeanrights.ue*, 2015, pp. 1 ss.,
http://www.europeanrights.eu/index.php?funzione=S&op=5&id=1059

M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, in *Diritto penale contemporaneo*, Fascicolo 2/2018, pp. 23-45
https://archiviodpc.dirittopenaleuomo.org/upload/1699-griffo218.pdf

M. TORRE, *Il captatore informatico nella legge delega 23 giugno 2017, n. 103*, in *JusOnline– Rivista di Scienze Giuridiche* (n.3/2017), pp. 435-444,
https://jus.vitaepensiero.it/news-papers-il-captatore-informatico-nella-legge-delega-23-giugno-2017-n-103-4837.html

O. CALAVITA, *L'odissea del trojan horse. Tra potenzialità tecniche e lacune normative*, in *Diritto penale contemporaneo*, (11/2018), pp. 45-76
https://archiviodpc.dirittopenaleuomo.org/d/6323-l-odissea-del-trojan-horse

P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma,* in *Processo Penale e Giustizia, 5/2016*
https://images.processopenaleegiustizia.it/f/fascicoli/Fascicolo5_2016_dDcMg_ppg.pdf

P. IOVINO, *Il trojan horse nelle indagini penali tra limiti normativi ed operativi*, in *Diritto.it*, 2022
https://www.diritto.it/il-trojan-horse-nelle-indagini-penali-tra-limiti-normativi-ed-operativi/

Procura della Repubblica presso la Corte di Cassazione, *Memoria per la camera di consiglio delle Sezioni Unite del 28 aprile 2016*
www.questionqegiustizia.it.

R. BUONANNO, *Il captatore informatico*, in *Office Advice*, *2021*
https://officeadvice.it/novita-giuridiche/il-captatore-informatico/

R. DE VITA & A. LAUDISIA, *I captatori informatici tra pericoli per i diritti umani e riduzionismo giuridico*, in *Eurispes,* 2019
https://eurispes.eu/wp-content/uploads/2016/04/vita-digitale-a-rischio.pdf

R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Rivista italiana di diritto e procedura penale*, *61*(2) 2018, pp. 538-556
https://hdl.handle.net/11585/643538

Redazione, *Trojan e Spyware: ecco come funzionano e quali sono i rischi,* in *Leurispes*, 2019
https://www.leurispes.it/trojan-e-spyware-ecco-come-funzionano-e-quali-sono-i-rischi/

Redazione, *Melillo sposa il trojan: "Stretta intercettazioni mina indagini e lotta alla mafia", ma la legge dice altro…."*, in *IlRiformista*, 2023
https://www.ilriformista.it/trojanmelillo-sposa-il-trojan-stretta-intercettazioni-mina-indagini-e-lotta-alla-mafia-ma-la-legge-dice-altro-341480/

T. DI GIULIO, *L'utilizzo del captatore informatico: il "trojan di Stato"*, in *Diritto consenso*, 2021
https://www.dirittoconsenso.it/2021/11/11/captatore-informatico-trojan-di-stato/

V. FRACASSO, *"Liberi tutti" nell'utilizzo del trojan di Stato?"*, in *Giurisprudenza Penale Web*(10) 2022
www.giurisprudenzapenale.com/2022/10/03/liberi-tutti-nellutilizzo-del-trojan-di-stato/

W. NOCERINO, A. ZAMPINI, *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in Rev. Bras. de Direito Processual Penal, Porto Alegre, v. 7, n. 2, p. 1411-1452
https://core.ac.uk/download/478497026.pdf

W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Cedam, 2021

W. NOCERINO, *L'acquisizione di dati mediante screenshot tra intercettazione telematica e prova atipica*, in *Rivisto Cammino Diritto*, Fasc. 06/2022
https://rivista.cammin3odiritto.it/articolo.asp?id=8457