CAPITOLO I – Il captatore informatico (*rectius* RCS: *remote control system*)

SOMMARIO: 1. Le indagini informatiche. – 2. La definizione di captatore informatico. – 2.1. Le differenti tipologie e funzionalità del captatore informatico. – 2.2. *Online search* e *online surveillance*. – 2.3. Attività tipica e attività atipica (anticipazioni). – 3. La necessità di un nuovo strumento d'indagine. – 3.1. La crittografia *end-to-end* (*e2ee*). – 3.2. Il caso *Eyepyramid*. – 3.3. Il caso *Apple*. – 3.4. I rischi nell'utilizzo del captatore informatico. – 3.5. Considerazioni conclusive.

1. Le indagini informatiche.

Negli ultimi anni, lo sviluppo sempre più rapido della tecnologia e la semplicità dell'accesso a *Internet* hanno mutato radicalmente i connotati della società, nonché la natura e l'intensità delle comunicazioni nei rapporti interpersonali. È una realtà ormai quasi obsoleta quella di scrivere una lettera su carta, stante l'istantaneità della comunicazione offerta dai vari strumenti accessibili *online*[1].

Ma l'attività comunicativa non è sicuramente l'unica ad aver subito una facilitazione nel suo svolgimento con l'avvento della c.d. era digitale: la "digitalizzazione" ha altresì agevolato l'esecuzione di varie attività in ambito lavorativo (basti pensare alle varie iniziative volte alla promozione dello *smart working* – o lavoro agile –, recentemente preso in considerazione anche dal legislatore nazionale[2] e ampiamente valorizzato nell'anno in corso al fine di far fronte all'emergenza *COVID*-19), sociale e culturale.

[1] A titolo esemplificativo, basti pensare alle applicazioni di messaggistica istantanea (quali *Whatsapp, Telegram, Viber*, ecc.) utilizzate quotidianamente da miliardi di utenti, che consentono altresì (come avremo modo di analizzare in seguito) di effettuare telefonate *online*, prescindendo dunque dall'uso della tradizionale linea telefonica. Ancora, tra tali strumenti si possono annoverare anche i vari *Social Network* (*Facebook, Instagram, Twitter,* ecc.) che dispongono di un'apposita sezione dedicata allo scambio di messaggi privati tra utenti. Senza infine dimenticare le "tradizionali" *e-mail*.

[2] Ex art. 18, comma 1 della Legge n. 81/2017: «Le disposizioni del presente capo [...] promuovono il lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva».

Se da un lato questo avanzamento tecnologico comporta innegabili vantaggi e opportunità, dall'altro si presta facilmente a utilizzi illeciti, quale strumento utile non solo per la commissione di "nuovi" reati[3], ma anche di reati tradizionali con nuove modalità.
I dispositivi elettronici, in considerazione del costante utilizzo che ciascuno ne fa, risultano essere equiparabili a «una "scatola nera" della nostra più intima personalità»[4], contenente qualsiasi tipo di informazione, fotografia, documento, ecc.
La "digitalizzazione", quale fenomeno globale che ha trasformato la società, impatta notevolmente anche sul processo penale. Il *computer* (e qualsiasi altro *device*) non è più solamente elemento costitutivo della fattispecie (ossia l'oggetto su cui ricade la condotta criminosa) o mezzo per la perpetrazione di un reato, ma assume un'importanza essenziale come fonte di prova, a prescindere dalla fattispecie delittuosa in relazione alla quale si sta procedendo: se, come si è detto, i dispositivi elettronici consentono un accesso a tutto tondo alle informazioni riguardanti un individuo, allora diventa certamente interesse degli organi inquirenti quello di poter accedere a tale "patrimonio". Tuttavia, ciò comporta una serie di difficoltà relative agli strumenti d'investigazione utilizzabili e alla loro qualificazione giuridica.
Considerazione fondamentale dalla quale è opportuno muovere è che le indagini informatiche si distinguono considerevolmente da quelle tradizionali almeno per quattro differenti ragioni.
In primo luogo, occorre considerare la natura promiscua dei dati reperibili: i sistemi informatici sono equiparabili a dei contenitori senza fondo, all'interno dei quali sono custoditi informazioni e dati di ogni sorta, capaci di circolare a velocità incontrollabili mediante *Internet*. A fronte di tale considerazione, risulta evidente l'elevato rischio di imbattersi in informazioni altre rispetto a quelle pertinenti all'indagine per la quale si procede[5]; considerevole deve essere, pertanto, la preparazione a livello tecnico dei

[3] Si allude, qui, ai c.d. *Cybercrimes*, individuabili come quelle attività criminose connotate dall'abuso di componenti tecnologiche informatiche, volte a compiere attacchi informatici attraverso l'uso di internet (ad es. *spamming* – invio massiccio di messaggi di posta elettronica senza il consenso del destinatario –, *phishing* – ossia il furto dell'identità, o comunque la commissione di atti volti a carpire dati sensibili degli utenti –, attacchi *DDOS* – che rendono inaccessibile un determinato servizio – , ecc.).
[4] R. BARONE, *Le indagini informatiche nella lotta al crimine*, consultabile al seguente indirizzo: *www.opiniojuris.it*, pag. 1.
[5] Si pensi, a titolo esemplificativo, alla possibilità di imbattersi in qualsiasi informazione concernente l'indagato di carattere strettamente personale, quali convinzioni religiose o politiche, del tutto irrilevanti ai fini dell'indagine. Ma non solo, ancor più "grave", forse, è il rischio di accedere a informazioni relative a terzi, del tutto estranei al procedimento penale, il cui diritto alla riservatezza e segretezza potrebbe così risultare pregiudicato.

soggetti chiamati a gestire il patrimonio informativo. Inoltre, tenendo conto della delicatezza delle informazioni così reperibili, è fondamentale la previsione di sanzioni severe volte a punire eventuali divulgazioni del materiale così acquisito in violazione del segreto investigativo (art. 329 c.p.p.).

In secondo luogo, da quanto appena detto deriva, altresì, la difficoltà, per gli organi inquirenti, di individuare precisamente e preventivamente le informazioni e i dati per la ricerca dei quali vengono poste in essere le indagini informatiche. Inoltre, non va sottovalutato il rischio di «indagini c.d. pro-attive (indagini ad alto contenuto tecnologico che si pongono a metà strada tra la prevenzione e la repressione»[6]), le quali, più che conseguire all'iscrizione di una *notitia criminis* nell'apposito registro del pubblico ministero, potrebbero essere utilizzate proprio al fine di ricercare e individuare tali notizie.

Ulteriore divergenza tra le indagini tradizionali e quelle informatiche si sostanzia nella rapida obsolescenza tecnologica: è necessario che gli strumenti e le tecniche utilizzate dagli organi inquirenti rimangano costantemente "al passo con i tempi", onde evitare di rendere vano lo svolgimento di questa "nuova" tipologia di indagini.

Da ultimo, stante la natura "inconsistente"[7], in termini fisici, dei dati e delle informazioni così reperibili, occorre considerare che, molto spesso, tali dati digitali vengono salvati in *server* situati in Paesi diversi da quello nel quale le indagini si stanno svolgendo (spesso si ricorre al salvataggio c.d. in *cloud*[8]); ne consegue la ricorrente necessità, da parte degli organi inquirenti, di collaborare con le autorità competenti dei Paesi esteri di volta in volta considerati[9].

Focalizzando ora l'attenzione sulle indagini informatiche, queste possono essere distinte in due macro-categorie, in relazione alle quali il *discrimen* è ravvisabile nella conoscibilità, da parte del soggetto sottoposto alle indagini, dell'atto d'indagine stesso: indagini palesi e indagini occulte (o segrete).

---

[6] M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, Giuffrè Editore, 2017, p. 10.

[7] S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018, p. 122.

[8] Il *cloud* (rectius: *cloud computing*) è emblematicamente rappresentato da una "nuvola" all'interno della quale si collocano i vari *devices* associabili al medesimo utente; quest'ultimo, mediante l'utilizzo della medesima combinazione di indirizzo *e-mail* e *password* può accedere da tutti i suoi dispositivi al patrimonio di informazioni che decide di caricare nel *server cloud*, dove avviene il c.d. *storage* di tali informazioni.

[9] S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, op. cit., p. 161 e ss.

Alla prima categoria[10] sono ascrivibili i mezzi di ricerca della prova tipici, quali ispezioni, perquisizioni e sequestri; il carattere "palese" di tali atti d'indagine è evidente: in relazione a ciascuno di essi l'indagato è a conoscenza dello svolgimento dell'atto, benché, talvolta, questi possano essere caratterizzati dall'ulteriore elemento dell'effetto a sorpresa.

Diversamente da queste ultime, le indagini informatiche occulte sono caratterizzate dalla mancanza di consapevolezza del loro svolgimento da parte del destinatario; ciò, chiaramente, le rende più efficaci ma, al contempo, aumenta il rischio di pregiudizi alla sfera privata dell'individuo.

Le indagini occulte possono ulteriormente essere distinte in attività di captazione passiva e attiva[11].

Nella prima rientrano le intercettazioni telematiche disciplinate dall'art. 266-*bis* c.p.p., in relazione alle quali non è ravvisabile una intrusione fisica da parte degli organi inquirenti nel dispositivo *target*[12]. Infatti, mediante l'intercettazione telematica, gli organi inquirenti acquisiscono conoscenza del «flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi».

Alla seconda sono invece ascrivibili, tra gli altri[13], tutti gli atti di indagine posti in essere ricorrendo all'ausilio dei c.d. captatori informatici, *malware* del tipo *trojan horse* che, una volta inoculati nel dispositivo *target*, consentono sostanzialmente di ottenere il totale controllo del *device*, come se questo fosse nelle mani del suo utilizzatore, permettendo così l'accesso a un'incredibile quantità di informazioni. Proprio di tali virus informatici ci occuperemo nel prosieguo di questa trattazione.

[10] Le indagini informatiche c.d. palesi sono state introdotte nel nostro ordinamento dalla Legge n. 48/2008, con la quale è stata ratificata la Convenzione *Cybercrime* del Consiglio d'Europa del 2001.

[11] F. PALMIOTTO, *Le indagini informatiche e la tutela della riservatezza informatica*, consultabile al seguente indirizzo: *www.lalegislazionepenale.eu*, pag. 3.

[12] Con il concetto di "dispositivo *target*" si suole individuare il *device* nel quale, come vedremo, il captatore informatico viene inoculato.

[13] Sono altresì riconducibili alle indagini informatiche occulte il c.d. pedinamento informatico, le indagini *undercover online*, il c.d. *data retention* (ossia la conservazione dei dati personali), il *cloud computing* e il monitoraggio dei siti *internet* visitati.

2. La definizione di captatore informatico.

Varie sono le denominazioni attribuite al captatore in dottrina e in giurisprudenza: taluni parlano di "agente intrusore"[14], altri di *trojan horse*, di perquisizioni *online*, di acquisizione occulta da remoto o, ancora, di *virus* di Stato[15]. Appare tuttavia più opportuno riferirsi a tale tipo di tecnologia utilizzando il nome di "sistema di controllo remoto" (RCS: *remote control system*)[16], nozione generica che meglio consente di racchiudere al suo interno le molteplici finalità di utilizzo del captatore informatico.

Dal punto di vista strettamente tecnico-informatico, un sistema di controllo remoto consiste in un *malware*[17], del tipo *trojan horse*[18], che viene installato occultamente nel dispositivo del destinatario mediante il "consenso" (seppur indiretto) del proprietario dello stesso che, eseguendo o installando il programma nel quale il *virus* è nascosto, consente allo stesso l'accesso al sistema.

Il *software* è composto da due programmi: un *server* e un *client*. Il primo consente di violare le difese del bersaglio, introducendosi all'interno dello stesso; il secondo, invece, viene utilizzato al fine di prendere il controllo del dispositivo infetto.

L'inoculazione del *server* può essere effettuata materialmente, avendo accesso materiale al sistema, o telematicamente, a distanza. Il primo metodo, certamente più rischioso per gli inquirenti, non si differenzia in alcun modo dall'installazione della microspia

---

[14] Cass., sez. VI, 26 maggio 2015, n. 27100, Musumeci, in C.E.D. Cass. 265654.

[15] A tal proposito, tuttavia, non manca chi obietta che è fuorviante parlare di *virus* di Stato, considerato che manca, nel nostro Paese, una tecnologia sviluppata e gestita direttamente dallo Stato, che fa invece ricorso a programmi e strumenti predisposti da privati.

[16] Utilizzano tale acronimo M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, op. cit.; O. CALAVITA, *L'odissea del trojan horse*, in *Diritto Penale Contemporaneo*, fasc. 11/2018, p. 48; ancora, Procura Generale presso la Corte di Cassazione, *Memoria per la Camera di Consiglio delle Sezioni Unite del 28 aprile 2016*, Num.Ric.Gen 6889/16, p. 4.

[17] Si definisce *malware* ogni programma informatico usato per disturbare le operazioni svolte da un utente di un computer; vari sono i possibili utilizzi di tale programma, ma quello che qui interessa concerne la possibilità di acquisire il sostanziale controllo del dispositivo *target*, potendo monitorare in tempo reale l'attività mediante lo stesso svolta.

[18] Il *trojan horse* è un tipo di *malware* in grado di occultare la propria presenza all'interno di un altro programma apparentemente utile e innocuo che, in ragione di ciò, viene volontariamente eseguito o installato dal proprietario del *device* "attaccato", consentendo l'accesso al *virus*. In dottrina si è evidenziato, metaforicamente, che «il virus *trojan* prende il suo nome [...] dal leggendario cavallo di Troia che, per mezzo di Odisseo, [...] riuscì a entrare dentro le mura di Troia, con inganno, ed espugnarla. Così come il cavallo [...] sconfisse i troiani entrando all'interno della loro cittadella [...], così anche il predetto virus riesce ad entrare, con inganno, nell'apparecchio [...] che si vuole intercettare, non per distruggerlo né tantomeno per danneggiarlo, ma per carpire qualsiasi dato che ivi possa trovarvi» (M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* in *Diritto penale contemporaneo*, fasc. 2/2018, pag. 23).

tradizionale, da tempo utilizzata nell'ambito delle intercettazioni c.d. "ambientali". Di maggior interesse appare qui, anche in ragione delle problematiche giuridiche che comporta, l'installazione telematica: il programma viene inavvertitamente installato (da qui il nome "cavallo di Troia") nel *device* da parte del destinatario dello stesso, mediante un'azione apparentemente innocua. Varie sono le modalità di inoculazione del captatore: mediante l'invio di un'*e-mail*, nella quale il *malware* appare come innocuo allegato della stessa; mediante un sito *web*, in questo caso il *virus* viene trasmesso occultandolo all'interno del *download* di un file; ancora, attraverso falsi *update*[19] scaricati volontariamente dall'utente.

Una volta installato, il captatore informatico consente al suo "*dominus"* di ottenere il controllo completo del dispositivo *target*, potendo visualizzare (o ascoltare) in tempo reale qualsiasi attività compiuta dal proprietario e attivare le periferiche del *device* (ossia il microfono e la fotocamera), trasformandolo in una "cimice mobile" che può permettere costantemente di carpire immagini e suoni che circondano il dispositivo in questione.

Tale controllo è possibile mediante la creazione di una c.d. *backdoor*[20]*,* che crea un contatto tra il centro di ascolto remoto del "pirata" e il *device* nel quale il *virus* viene inoculato.

In relazione a quanto appena detto si può arguire che, al fine di permettere la riuscita di tali operazioni, è indispensabile il contributo del proprietario del dispositivo da infettare, senza il quale l'intera operazione potrebbe essere vanificata.

Proprio in questa necessaria collaborazione, seppur inconscia, del destinatario si cela uno dei principali limiti di tale mezzo di ricerca della prova: se è vero che il *quivis de populo* mai potrebbe accorgersi di tale macchinazione, in particolari contesti criminali questo meccanismo potrebbe trovare un insuperabile ostacolo nella diffidenza dei possibili destinatari nei confronti di *input* provenienti dall'esterno, soprattutto se da fonti ignote.

Un'ulteriore problematica relativa a tale tipo di tecnologia è individuabile nella sua rapida obsolescenza: considerata la celerità dello sviluppo tecnologico, è molto elevato il rischio di utilizzare un metodo d'intrusione che nell'ambito criminale bersaglio sia già stato

[19] Per *update* si intendono gli aggiornamenti rilasciati dagli sviluppatori delle varie applicazioni dei dispositivi elettronici, che permettono di migliorare il funzionamento delle stesse mediante la correzione dei c.d. *bug* (errori dell'applicazione) e l'introduzione di nuove funzionalità.

[20] Una *backdoor*, letteralmente "porta sul retro", è un metodo, spesso occulto, che consente di aggirare i normali meccanismi di autenticazione di un sistema informatico, eludendone, in sostanza, i presidi di sicurezza.

superato, permettendo ai potenziali destinatari dei controlli, mediante l'utilizzo di avanzati *software antivirus*[21], di ravvisare la presenza del programma infettante ancora prima di poter iniziare qualsiasi tipo di attività, precludendo così l'installazione del *malware*.

2.1. Le differenti tipologie e funzionalità del captatore informatico.

Parlando di captatore informatico è doveroso sottolineare come con tale termine non ci si possa riferire a un unico programma: infatti, all'interno dell'alveo dei *remote control systems* (*RCS*) sono individuabili molteplici *software* capaci di sorvegliare il dispositivo bersaglio; il captatore, quindi, è qualificabile come un *genus*, entro il quale sono individuabili una molteplicità di *species*.

A livello tecnico, le attività che questi *malware* possono svolgere sono potenzialmente illimitate, ma ciò che qui interessa sono i loro possibili utilizzi in ambito processuale. Sovviene, in tal senso, la classificazione delle varie funzioni che il *trojan* può espletare effettuata dalla Corte di Cassazione a Sezioni Unite nella celebre sentenza Scurato[22], "*leading case*" in materia: «uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente:

- di captare tutto il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia *web mail*, che *out look*);
- di 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;
- di mettere in funzione la *web camera*, permettendo di carpire le immagini;
- di perquisire lo *hard disk* e di fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira;
- di decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*);

[21] Il *software antivirus* è una tecnologia difensiva finalizzata, come suggerisce il nome stesso, a individuare la presenza di eventuali *virus* (tra i quali rientrano i *malware*) all'interno di un dispositivo e, ancor prima della loro installazione, di prevenire la stessa mediante apposito avviso all'utente.
[22] Cass. pen. sez. un., 28 aprile 2016, n. 26889, Scurato, in C.E.D. Cass. 266905-266906.

- di sfuggire agli antivirus in commercio»[23].

In termini pratici, dunque, l'utilizzo di tale «"bulimico" congegno»[24] consente agli inquirenti di registrare le telefonate effettuate anche mediante applicazioni che ricorrono all'utilizzo della crittografia, utilizzare il dispositivo per intercettazioni "ambientali", sfruttare i sistemi GPS per geolocalizzare gli individui sorvegliati, conoscere il contenuto di *e-mail*, SMS, visualizzare la cronologia delle ricerche *web*, ecc.

2.2. Online search e online surveillance.

In materia di captatori informatici in ambito investigativo, da un punto di vista tecnico, la dottrina suole distinguere due differenti modalità operative: *online search* e *online surveillance*[25].

La prima consente la perquisizione da remoto dell'*hard-disk*[26] e di effettuarne una copia totale o parziale; permette dunque la perquisizione (ricerca) e il sequestro (copia) di dati c.d. statici, in quanto già memorizzati nel *device* (si parla, a tal proposito, di "copiatore informatico"[27]). Concentrando l'attenzione sugli istituti processuali appena individuati, occorre notare che il codice di rito disciplina il sequestro del corpo del reato e delle cose pertinenti al reato necessarie al fine dell'accertamento dei fatti (art. 253 c.p.p.): nel caso in cui il corpo del reato o le cose pertinenti al reato sono dei dispositivi informatici (es. *smartphone, tablet*, computer e in genere ogni altro dispositivo c.d. *smart*) è allora possibile ottenere una copia del loro contenuto, conformemente all'art. 258 c.p.p. («Copie dei documenti sequestrati»), ma solo dopo il materiale sequestro del *device*; ne consegue che l'operazione non avviene a distanza.

---

[23] Classificazione effettuata da Cass., sez. un., 28 aprile 2016, n. 26889, Scurato, cit., al punto 1 della motivazione

[24] L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, consultabile al seguente indirizzo: *www.ilpenalista.it*

[25] In dottrina, ricorre a questa distinzione M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, op. cit.; M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* in *Diritto penale contemporaneo*, fasc. 2/2018; O. CALAVITA, *L'odissea del trojan horse*, in *Diritto Penale Contemporaneo*, fasc. 11/2018; R. DE VITA e A. LAUDISA, *Vita digitale a rischio: I captatori informatici tra pericoli per i diritti umani e riduzionismo giuridico,* consultabile al seguente indirizzo: *www.devita.law*

[26] L'*hard-disk*, in italiano disco rigido, è un dispositivo di memoria di massa, di tipo magnetico, che utilizza uno o più dischi per l'archiviazione di dati e applicazioni (sistemi operativi, programmi, file, ecc.); "volgarmente", dunque, contiene l'intera memoria di un dispositivo.

[27] M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, op. cit., p. 19.