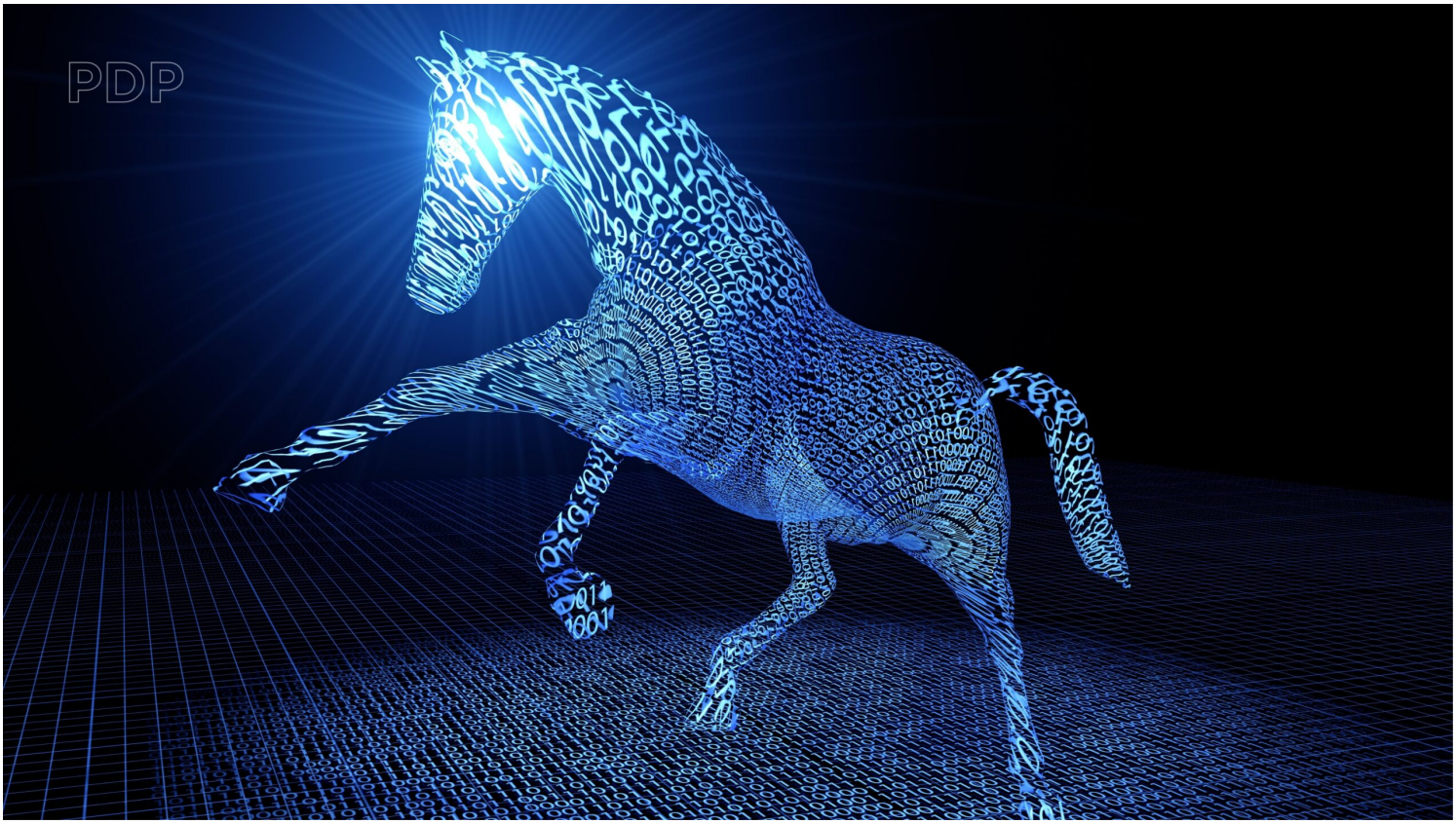
IL CAVALLO DI TROIA E L'ISPE-PERQUI-INTERCETTAZIONE

Leonardo Filippi



1. L'ordigno onnivoro

Eravamo stati facili profeti quando paventavamo l'avvento del *trojan*, ordigno onnivoro che tutto e chiunque, dovunque e comunque non solo intercetta, ma ispeziona, perquisisce e acquisisce (e può anche, insidiosamente, immettere dati nel dispositivo intercettato). Sono infatti impressionanti le funzioni che il "cavallo di Troia" può svolgere. Esso, infatti, può attivare il microfono (registrando i colloqui che si svolgono nello spazio che circonda il portatore del dispositivo); può captare il traffico dati in arrivo o in partenza dal dispositivo "infettato"; può mettere in funzione la *web-camera* (permettendo di registrare le immagini

circostanti); può perquisire l'*hard disk* dell'apparecchio "bersaglio", facendo copia di *files* che eventualmente possono essere trasmessi agli inquirenti; può decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*); può infine fotografare ciò che appare sullo schermo del dispositivo colpito (*screenshot*). Perciò, il "cavallo di Troia" non si limita a registrare le conversazioni "tra presenti", ma consente sia un'attività di *on line surveillance*, nella quale è ricompresa la captazione di flussi informativi riconducibile alla disciplina delle intercettazioni, sia un'attività di *on line search*, nella quale rientra la copia e la successiva trasmissione all'esterno di *files* contenuti nel dispositivo "target".

Si susseguono però le pronunce giurisprudenziali che legittimano tali invasive potenzialità intrusive, pur in assenza dei connotati caratteristici dell'intercettazione.

2. L'intercettazione

Com'è noto, l'art. 266 c.p.p. non offre una nozione di intercettazione, limitandosi ad elencare i casi ammessi di intercettazioni telefoniche, di altre forme di telecomunicazione e di comunicazioni tra presenti, anche con l'inserimento di un captatore informatico. Secondo la definizione offerta dalle Sezioni unite Torcasio del 2003, l'intercettazione consiste nella captazione, occulta e contestuale, di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo, attuata da un soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato[1]. Emergono con nitidezza in questa definizione i caratteri dell'intercettazione.

Oggetto dell'intercettazione deve quindi essere, anzitutto, una comunicazione o conversazione, cioè un messaggio scambiato tra due o più interlocutori, perché solo questa è coperta della riserva di legge *ex* art. 15 Cost. Sul punto la giurisprudenza ha però esteso oltremodo il concetto, ammettendo "comportamenti comunicativi"[2], laddove l'art. 267 c.p.p. autorizza, almeno per l'impiego del captatore, l'attivazione del microfono e quindi si riferisce soltanto alla conversazione verbale; altre volte la Corte di cassazione ricorre alla nozione di prova atipica[3] e addirittura è arrivata ad affermare che le riprese audio-video, disposte previa autorizzazione del giudice, delle effusioni e dei rapporti sessuali tra l'indagato e la minore vittima di violenza sessuale all'interno di un domicilio privato, sono utilizzabili in quanto configurano intercettazioni di comportamenti comunicativi, ancorchè di tipo non verbale, espressivi di interazione ed idonei a trasmettere contenuti del pensiero e stati d'animo[4]. Inoltre, la comunicazione deve essere oggettivamente segreta, nel senso che la sua segretezza deve emergere oggettivamente dalle caratteristiche della stessa, cioè dal suo

contenuto e dalle modalità con cui essa si svolge; pertanto, non è intercettazione ascoltare ciò che taluno comunica ad altri a voce alta o su onde radio[5].

La captazione deve essere occulta rispetto ad almeno uno dei comunicanti (a differenza del sequestro che è atto scoperto e garantito), per cui nel caso in cui uno dei partecipanti alle conversazioni sia a conoscenza dello svolgimento delle intercettazioni, regolarmente autorizzate dall'autorità giudiziaria ed eseguite nelle forme di legge, il loro risultato è utilizzabile[6]. Il consenso di uno degli interlocutori non è sufficiente a rendere legittima l'intercettazione non autorizzata di una conversazione da parte di un terzo, in quanto anche la segretezza delle comunicazioni dell'ignaro interlocutore deve essere garantita[7].

Caratteristica dell'intercettazione è la captazione contestuale rispetto alla comunicazione in atto, per cui l'intercettazione capta una comunicazione in corso (come le conversazioni, anche con messaggistica istantanea), a differenza del sequestro che è atto palese e differito rispetto alla comunicazione, oltre che garantito dal diritto di difesa.

Altra caratteristica dell'intercettazione è la terzietà del captante, cioè che colui che capta la comunicazione sia un terzo rispetto ai comunicanti; di conseguenza, la registrazione effettuata da uno dei partecipanti alla conversazione non rientra nel novero delle intercettazioni[8].

Infine, occorre l'impiego di strumenti tecnici di percezione e registrazione del suono idonei a documentare il contenuto della comunicazione, per cui l'origliamento a orecchio nudo o l'ascolto di conversazioni o comunicazioni attuate mediante onde radio con l'uso di emittenti a irradiazione circolare non sono intercettazioni.

L'art. 266-*bis* c.p.p. regolamenta invece l'intercettazione di comunicazioni informatiche o telematiche. Per intercettazione informatica si intende la registrazione segreta di flussi di informazioni scambiate da due o più elaboratori collegati via cavo o comunque mediante collegamenti fisici. Si parla invece di intercettazione telematica quando la captazione riguarda i sistemi telematici, costituiti da reti di elaboratori che, per scambiarsi dati utilizzano cavi telefonici, reti di *computer* o altre forme di collegamento tra sistemi telematici.

L'intercettazione informatica o telematica capta il flusso delle comunicazioni informatiche o telematiche in partenza o in arrivo su un certo *account* in tempo reale rispetto alla comunicazione, come nel caso di

intercettazione di messaggi di posta elettronica, i quali, se invece sono già consegnati al destinatario e memorizzati sugli impianti dell'*internet service provider*, possono essere oggetto di sequestro a norma dell'art. 254 c.p.p.

Relativamente all'acquisizione delle *e-mail*, in taluni casi sono sorti problemi sull'inquadramento come intercettazione telematica *ex* art. 266-*bis* c.p.p. oppure come sequestro. Si sono perciò proposti diversi criteri per distinguere l'intercettazione dal sequestro della posta elettronica. Il più corretto è quello incentrato sull'attualità della comunicazione rispetto all'acquisizione della *e-mail*, per cui si tratta di intercettazione quando la captazione dell'*e-mail* avviene in tempo reale, contestualmente alla sua trasmissione. La *e-mail* rileva come comunicazione istantanea, allo stesso modo di quella telefonica o tra presenti, e può essere intercettata finchè la comunicazione è in corso. Pertanto, le *e-mail* già pervenute al destinatario ed archiviate in apposite cartelle nella memoria del p.c. non possono essere oggetto di intercettazione, trattandosi di un flusso di dati "già avvenuto", rispetto al quale manca uno dei presupposti tipici dell'intercettazione, cioè l'apprensione della comunicazione in tempo reale. In caso di ritardo nella consegna del messaggio dal *server* del mittente a quello del destinatario, la comunicazione è ancora in corso e può essere oggetto di intercettazione, come pure nell' ipotesi dell'acquisizione delle *e-mail* in transito sul *server* del gestore, mentre diverso è il caso in cui la polizia procede al sequestro della posta già consegnata e archiviata sul *server* del gestore. Nell'ipotesi di acquisizione di *e-mail* scaricata sul p.c. del destinatario ma da lui non ancora letta si può ritenere esaurito il corso della trasmissione e quindi essa è oggetto di sequestro e la stessa conclusione si dovrebbe raggiungere quando la *e-mail* è letta ma non dal destinatario ma da altri.

Non sembra condivisibile la tesi che vorrebbe distinguere l'intercettazione telematica dal sequestro in base alle modalità di effettuazione dell'atto di acquisizione, perché, com'è noto, mentre l'intercettazione è un'attività svolta in maniera occulta, il sequestro è anch'esso un atto a sorpresa, ma scoperto e differito, oltre che garantito. Pertanto, quando la percezione della comunicazione informatica avviene attraverso la duplicazione della casella di posta elettronica da parte del gestore del relativo servizio, con il conseguente inoltro di tutte le *e-mail* direttamente sul *server* della Procura della Repubblica, si tratta di intercettazione di flussi informatici *ex* art. 266-*bis* c.p.p. Se invece gli organi inquirenti si rivolgono direttamente all'ente che gestisce la corrispondenza elettronica o accedono direttamente al p.c. dell'interessato, l'apprensione dei dati digitali, per il suo carattere palese, dà luogo ad un'attività di sequestro.

In altre parole, l'art. 266-*bis* c.p.p. trova applicazione laddove si intenda captare il flusso delle comunicazioni telematiche in partenza o in arrivo su un certo *account*, mentre deve provvedersi al sequestro solo in relazione alla corrispondenza telematica immessa nei sistemi di comunicazione e già pervenuta al

destinatario e quindi custodita presso il fornitore di servizi, definito *service provider*.

Di conseguenza, si è affermato che le *chat*, come le *mail* e i *social network*, danno luogo ad un flusso di comunicazioni relativo a sistemi telematici, per la cui intercettazione opera il disposto dell'art. 266-*bis* c.p.p., laddove, invece, il sequestro di cui all'art. 254-*bis* c.p.p. non riguarda un flusso di comunicazioni (quale è quello che si realizza con le *chat*, anche se non contestuali) bensì dati detenuti da fornitori di servizi telematici (ad esempio su un *hard disk* o altro supporto informatico)[9].

L'intercettazione di *e-mail* o altri messaggi similari (che di solito si attua attraverso la clonazione dell'*account* di posta elettronica dell'indagato e immediata trasmissione dei dati presso una postazione di decodifica), la quale si caratterizza per la contestualità tra la captazione dei messaggi e la loro trasmissione e, quindi, ha ad oggetto un flusso comunicativo in atto e in ragione di ciò l'art. 266-*bis* c.p.p. predispone, proprio perché trattasi di un'attività di intercettazione telematica, una tutela rafforzata e l'adozione delle garanzie relative ai presupposti di applicabilità e alla necessità dell'autorizzazione giurisdizionale[10].

3. Il sequestro

Diversa dall'intercettazione è l'attività di acquisizione *ex post* del dato conservato in memoria che documenta flussi già avvenuti, i cui dati, pertanto, possono essere acquisiti attraverso lo strumento del sequestro[11].

La Corte e.d.u. ha ravvisato una violazione del diritto alla segretezza della corrispondenza, tutelato dall'art. 8 C.e.d.u., in un caso in cui al ricorrente era stato sequestrato un cellulare contenente una serie di messaggi con due suoi difensori in un diverso procedimento penale[12]. La giurisprudenza di Strasburgo considera inviolabile il rapporto tra difensore e assistito e con valutazione *ex ante* presume che la conversazione o comunicazione tra essi attenga all'esercizio del diritto di difesa, salvo prova contraria, mentre in Italia la Corte di cassazione consente l'intercettazione tra legale e suo assistito e valuta *ex post* il contenuto della comunicazione o conversazione. Ma in questo modo è evidente la lesione sistematica del rapporto fiduciario tra difensore ed assistito. In Italia, sebbene l'art. 15 Cost. imponga la riserva di legge (oltre quella di giurisdizione) e l'art. 103, comma 5, c.p.p. preveda un incondizionato divieto di intercettare le conversazioni o comunicazioni dei difensori, la giurisprudenza consente addirittura sempre l'intercettazione della comunicazione tra difensore e assistito per accertarne caso per caso e solo *a posteriori* il contenuto e, soltanto se ne riconosce la natura difensiva, la registrazione non è acquisibile. Perciò, la Corte di cassazione afferma costantemente la necessità di un controllo caso per caso e in concreto sul contenuto della

conversazione[13]. E' pacifico che tali divieti probatori e di utilizzazione sono posti a garanzia della necessaria riservatezza dell'attività difensiva e quindi le comunicazioni e conversazioni tra assistito e difensore, riconoscibili dal numero di utenza del legale o da altri elementi, devono presumersi di natura difensiva, salvo prova contraria *aliunde* emergente, e pertanto non sono ammesse e, se erroneamente iniziate, devono essere immediatamente interrotte. Si dovrebbe perciò riflettere sui limiti che all'attività di indagine devono essere non solo posti legislativamente, ma anche rispettati nella prassi, per tutelare davvero la funzione difensiva. Si afferma invece nella giurisprudenza che il divieto di utilizzazione stabilito dall'art. 271, comma 2, c.p.p. non sussiste quando le conversazioni o le comunicazioni intercettate non siano pertinenti all'attività professionale svolta dalle persone indicate nell'art. 200, comma 1, c.p.p. e non riguardino di conseguenza fatti conosciuti per ragione della professione dalle stesse esercitata, oppure quando lo stesso difensore è sottoposto alle indagini[14]. La giurisprudenza più garantista riconosce che l'inutilizzabilità dei risultati delle intercettazioni con il proprio difensore sussiste quand'anche l'indagato non abbia ancora comunicato all'autorità procedente la nomina del difensore ai sensi dell'art. 96 c.p.p., in quanto ciò che rileva ai fini della garanzia di cui all'art. 103 c.p.p. è la natura del colloquio e non la formalizzazione del ruolo del difensore[15]. Trattandosi di prova inammissibile, la notizia appresa mediante l'intercettazione vietata non può essere acquisita altrimenti: perciò, ad esempio, sarebbeinutilizzabile la testimonianza del terzo, il quale abbia assistito al dialogo tra imputato e difensore. Per i soggetti tutelati dal segreto professionale l'art. 271, comma 2, c.p.p. si limita ad imporre il divieto di utilizzazione dei risultati dell'intercettazione, ma non proibisce che la notizia segreta possa essere appresa, ad esempio, per mezzo della testimonianza del terzo, al quale l'autore della confidenza abbia raccontato gli stessi fatti riferiti al professionista tenuto al segreto.

Si verte, quindi, in materia di sequestro quando manca la contemporaneità tra comunicazione e captazione. Il sequestro della posta elettronica (cd. *e-mail*) presso il fornitore di servizi o dalla memoria del dispositivo avviene non in tempo reale rispetto all'invio e ricezione della comunicazione, ma successivamente ed è atto a sorpresa ma scoperto e garantito. Quando invece la captazione avviene contemporaneamente alla trasmissione del messaggio deve operare la disciplina delle intercettazioni. Pertanto, deve provvedersi al sequestro solo in relazione alla corrispondenza telematica che sia stata immessa nei sistemi di comunicazione e sia custodita presso il fornitore di servizi, definito *service provider*, mentre l'art. 266-*bis* c.p.p. trova applicazione laddove si capti il flusso delle comunicazioni telematiche in partenza o in arrivo su un certo *account*. Il sequestro, a differenza dell'intercettazione, è assistito dal diritto di difesa *ex* artt. 365 e 366 c.p.p. e quindi con diritto di assistere, senza preavviso, al compimento dell'atto e all'esame del relativo verbale.

Si è, pertanto, affermato che i messaggi di posta elettronica non inviati dall'utente, ma salvati nella cartella "bozze" del proprio *account* o in apposito spazio virtuale (come *Dropbox* o *Google Drive*), accessibili solo digitando nome utente e *password*, costituiscono dei documenti informatici, ai sensi dell'art. 234 c.p.p., che possono essere sequestrati nel luogo ove avviene l'accesso da parte dell'utente attraverso l'inserimento della *password*, indipendentemente dalla localizzazione all'estero del *provider*, dovendosi escludere che si tratti di corrispondenza, soggetta alla disciplina di cui all'art. 254 c.p.p., o di dati informatici detenuti dal *provider*, sequestrabili nell'ambito della procedura prevista dall'art. 254-bis c.p.p.[16]

In giurisprudenza si afferma che i dati informatici scambiati attraverso la comunicazione (quali *e-mail*, *sms* e messaggi *WhatsApp*), contenuti in uno strumento elettronico (*computer* o telefono cellulare) e archiviati su apposita memoria, hanno natura documentale ai sensi dell'art. 234, sicché la loro acquisizione non costituisce attività di intercettazione disciplinata dagli artt. 266 ss. c.p.p. e, in particolare, dall'art. 266-*bis* c.p.p., atteso che quest'ultimo esige la captazione di un flusso di comunicazioni in atto ed è, pertanto, attività diversa dall'acquisizione *ex post* del dato conservato in memoria che documenta flussi già avvenuti. Tali dati, pertanto possono essere acquisiti attraverso lo strumento del sequestro, senza peraltro dover adottare la disciplina stabilita per la "corrispondenza" (art. 254 c.p.p.) perché detti messaggi non rientrano nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito.

Secondo l'orientamento dominante la Corte di cassazione riconosce, ai sensi dell'art. 234 c.p.p., natura documentale ai messaggi e alle *chat Whatsapp* prodotte nel contesto di un processo penale, anche attraverso semplice *screenshot*. E ciò in quanto la captazione di messaggi e *chat* rappresenta una forma di documentazione di una conversazione *ex post* e non in corso e quindi sfugge alla disciplina delle intercettazioni o delle semplici registrazioni e ha valore di prova documentale[17] .

In particolare, possono essere acquisite per mezzo di un sequestro di dati informatici le *e-mail* conservate dal mittente nella cartella "bozze" (e perciò non inviate al destinatario, il quale, però, avendo la *password* dell'*account* vi accedeva)[18].

Si precisa che il decreto di sequestro (così come il decreto di convalida di sequestro) probatorio, anche ove abbia ad oggetto cose costituenti corpo di reato, deve contenere una specifica motivazione sulla finalità perseguita per l'accertamento dei fatti[19].

Particolare è l'acquisizione dei dati informatici, per la quale l'art. 254-*bis* c.p.p. (introdotto nel codice di rito penale dall'art. 8 l. 18.3.2008, n. 48, Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica) disciplina il sequestro presso fornitori di servizi informatici, telematici e di telecomunicazioni, stabilendo che l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. Tale sequestro ha ad oggetto i dati detenuti da fornitori di servizi telematici e non riguarda un flusso di comunicazioni in atto (quale è quello che si realizza con le *chat*, anche se non contestuali, le *mail* e i *social network*), che invece danno luogo ad un flusso di comunicazioni relativo a sistemi telematici, per la cui intercettazione opera il disposto dell'art. 266-*bis* c.p.p. In giurisprudenza è pacifico che costituisce sequestro probatorio l'acquisizione, mediante estrazione di copia informatica o riproduzione su supporto cartaceo, dei dati contenuti in un archivio informatico visionato nel corso di una perquisizione legittimamente eseguita ai sensi dell'art. 247 c.p.p., quando il trattenimento della copia determina la sottrazione all'interessato della esclusiva disponibilità dell'informazione[20] .

I dati informatici acquisiti da un *server* aziendale hanno natura di documenti, la cui attività acquisitiva non soggiace alla disciplina delle intercettazioni telefoniche, essendo invece legittima l'acquisizione mediante provvedimento di sequestro probatorio, il quale interviene per acquisire *ex post* i dati risultanti da precedenti e già avvenute comunicazioni telefoniche, così come conservati nella memoria fisica del computer e come tali cristallizzati e documentati da quei flussi[21].

Tuttavia, nella giurisprudenza si registra talvolta qualche sbandamento. Infatti, talvolta la Corte di cassazione individua l'elemento caratterizzante il "flusso informatico" tipico dell'intercettazione (a differenza del sequestro) nell'avvenuto inoltro della *e-mail* da parte del mittente e ravvisa perciò un'intercettazione quando la *e-mail* è inviata o ricevuta. Pertanto, indipendentemente dal sistema di intrusione utilizzato (quello dell'accesso diretto al p.c. ovvero occulto attraverso un programma-spia) quando si acquisiscono *e-mail* ormai spedite o ricevute, si pone in essere un'attività intercettativa. Si è perciò affermato che l'acquisizione di messaggi di posta elettronica, già ricevuti o spediti dall'indagato e conservati nelle rispettive caselle di posta in entrata e in uscita, costituisce attività di intercettazione, sottoposta alla disciplina di cui agli artt. 266 e 266-*bis* c.p.p., indipendentemente dal sistema intrusivo adottato dagli inquirenti[22]. Ancora la giurisprudenza afferma, con specifico riferimento alle intercettazioni dei messaggi tra dispositivi *Blackberry*,

che è legittima l'acquisizione di contenuti degli stessi mediante intercettazione operata ai sensi dell'art. 266 ss. c.p.p. poiché le *chat*, anche se non contestuali, costituiscono un flusso di comunicazioni[23] .

4. La mancanza di una disciplina legislativa sull'inoculazione del *malware*

È noto che, a norma dell'art. 266, comma 2, c.p.p., il programma informatico noto come "*cavallo di Troia*", ma denominato eufemisticamente dal codice "captatore informatico", può essere installato su un dispositivo elettronico portatile (cd. "*target*", che può essere un computer, un *tablet* o uno *smartphone*, purchè mobili) con modalità non disciplinata dalla legge.

L'installazione del *malware* avviene perciò, secondo le diverse prassi seguite dalla polizia giudiziaria, di norma a distanza e in modo occulto, per mezzo dell'invio di un'*e-mail*, un *s.m.s.* o di un'applicazione di un finto aggiornamento di un programma già installato. Ma la lacuna legislativa sulle modalità di installazione del *virus* rende tale mezzo di ricerca della prova contrastante con la "riserva di legge" posta dall'art. 15 Cost.

5. La violazione della libertà di autodeterminazione del controllando

Ma la insidiosità del captatore informatico emerge prepotentemente su diversi fronti. Il *virus trojan* infatti non limita soltanto la segretezza, ma talvolta pure la libertà di autodeterminazione della persona da intercettare. Ormai di regola nella prassi si verifica che, quando il portatore del dispositivo elettronico portatile non dà l'*input* che consente l'accesso al *malware* (ad es. non accetta l'aggiornamento proposto come "cavallo di Troia), la polizia giudiziaria ricorre ad ulteriori e più insidiosi stratagemmi, non previsti dalla legge, quali, ad esempio, di bloccare le telefonate in uscita dal cellulare per costringere l'ignaro soggetto ad operazioni che comportano l'accesso del *virus trojan* nel dispositivo, come accaduto nel noto "caso Palamara". Si è perciò dubitato della legittimità dell'impiego del *trojan horse*, quale conseguenza della modalità "subdola" di acquisizione della prova attraverso l'induzione del soggetto intercettato alla "autoinstallazione" del *virus*, con costi a carico del destinatario e in violazione del principio di autodeterminazione di cui all'art. 188 c.p.p.[24]

In realtà, il captatore viene inconsapevolmente auto-installato dal soggetto controllato, che viene indotto a

farlo con artifici e raggiri: gli si fa credere che è un'operazione che serve a ripristinare o a migliorare la funzionalità del suo *device* quando, invece, si tratta di un modo subdolo per spingerlo a compiere un atto che altrimenti non avrebbe posto in essere e che, a sua insaputa, inocula il *virus trojan* nel suo dispositivo e quindi consente l'intercettazione. In questo caso, a nostro parere, il pubblico ministero viene meno al suo dovere di lealtà processuale e viola il principio di autodeterminazione garantito dall'art. 188 c.p.p. a chiunque, e *in primis* all'indagato. Come noto, tale disposizione vieta l'utilizzazione, neppure con il consenso della persona interessata, di "metodi o tecniche idonei ad influire sulla libertà di autodeterminazione", e il divieto non riguarda soltanto il contenuto della dichiarazione, ma anche qualsiasi costrizione, fisica o psichica, ad un *facere*. Ma non è ammissibile che lo Stato, al fine di reprimere le condotte illecite dei criminali, scenda al loro livello ingannando l'indagato per indurlo a consentire inconsapevolmente l'accesso al "cavallo di Troia". E siccome l'impiego di tali fraudolente manovre è diventato ormai la regola, il problema non può essere più ignorato. Ed in effetti, già la denominazione di "cavallo di Troia" dovrebbe far capire che si tratta di una manovra fraudolenta. Infatti, mentre per le tradizionali forme di intercettazione non è mai necessaria una collaborazione della persona da monitorare, per il *trojan*, salvo i rari casi in cui si riesca ad avere la disponibilità fisica dell'apparecchio per il tempo necessario all'installazione del *virus*, si deve sempre ricorrere ad una "trappola" per inoculare il *malware* sull'apparecchio portatile, senza alcun consenso da parte del titolare del dispositivo controllato ed anzi con la sua inconsapevole collaborazione fraudolentemente indotta. Di solito si invia al *device* da monitorare una *mail* o altro messaggio, apparentemente inoffensivo, aprendo il quale si scarica il *virus* senza averne alcuna consapevolezza. Inoltre, le modalità di questa "trappola" non sono indicate dalla legge, con conseguente limitazione talvolta anche della libertà domiciliare in plateale violazione della riserva di legge; di conseguenza, tali stratagemmi sfuggono alle prescrizioni ed al controllo sia del p.m. sia del g.i.p. e sono lasciate all'estemporanea e incontrollabile iniziativa della polizia giudiziaria. In fondo, "trappole" del genere sono sempre state praticate: si pensi all'espediente cui ricorre la polizia giudiziaria, per sistemare le microspie, di entrare a casa del sospettato, sotto le mentite spoglie di un operaio del gas o della società elettrica o di accedere all'abitacolo della vettura con i doppioni delle chiavi.

Il captatore informatico, dopo la sua inoculazione, per essere attivato, richiede un impulso da parte dell'ignaro soggetto controllando, che viene fraudolentemente indotto ad un comportamento attivo (ad es., aprire una *e-mail* o un'applicazione apparentemente utile oppure resettare il dispositivo) che non avrebbe certamente compiuto se avesse saputo che serviva a sottoporlo a controllo. Tale comportamento attivo fraudolentemente richiesto al soggetto passivo del controllo pone un primo problema sulla legittimità di una prova ottenuta in modo sleale dallo Stato, prospettandogli una situazione diversa da quella reale. In altre parole, lo Stato pone in essere "artifizi e raggiri" per indurre in errore il cittadino e costringerlo ad un atto che procura agli inquirenti l'"ingiusto profitto" di poterlo controllare, con suo evidente danno. Tale metodologia

investigativa, come detto non disciplinata dalla legge ma lasciata pericolosamente alla prassi poliziesca, pone fondati dubbi di conformità all'art. 188 c.p.p. che vieta l'utilizzazione, "neppure con il consenso della persona interessata", di "metodi o tecniche idonei a influire sulla libertà di autodeterminazione". Non può infatti revocarsi in dubbio che il comportamento collaborativo chiesto al controllando sia ottenuto rappresentandogli una realtà difforme da quella reale (ad es. gli si prospetta l'aggiornamento di un programma mentre in realtà egli inconsapevolmente consente l'inoculazione del *malware*) e quindi incide sulla libertà di autodeterminazione del soggetto. È lecito perciò dubitare della legittimità dell'impiego del *trojan horse*, quale conseguenza della modalità "subdola" di acquisizione della prova attraverso l'induzione del soggetto intercettato alla "autoinstallazione" del *virus*, con costi a carico del destinatario[25] e in violazione del principio di autodeterminazione di cui all'art. 188 c.p.p.

È facile la conclusione per cui dal contrasto con tale imperioso divieto probatorio, deriva, *ex* art. 191 c.p.p., l'inutilizzabilità del summenzionato "cavallo di Troia".

Ma la giurisprudenza nega che l'impiego del captatore possa ledere la libertà di autodeterminazione del soggetto[26].

6. I dubbi sul *server* utilizzato

Abbiamo già avuto occasione di osservare quali dubbi siano sorti anche sul funzionamento del *trojan*[27], nonostante sui "casi" e soprattutto sul "modo" in cui il "cavallo di Troia" intercetta le nostre comunicazioni esista nell'art. 15 Cost. una riserva assoluta di legge ma nessuna disposizione legislativa ne disciplina il funzionamento.

I dubbi sono tanto seri da provocare l'emissione di una circolare della Procura di Milano. La situazione attuale, infatti, mostra che sono poche le società proprietarie dei *trojan* noleggiati alle Procure del nostro Paese e la maggior parte di queste fornisce programmi che nemmeno conosce esattamente (con il rischio di inquinare la prova e di intercettare anche terzi estranei), dopo averli a propria volta noleggiati da altre società, spesso addirittura estere, che li hanno brevettati. E' emerso dalle cronache giudiziarie sul "caso Palamara", che le intercettazioni disposte dalla Procura di Perugia, prima di finire nel *server* della stessa Procura, rimbalzavano su un *server* di transito collocato dalla società privata che gestiva il *malware* presso la Procura di Napoli, all' insaputa di tutti e persino della stessa Procura. Ma tale sistema non si è verificato soltanto nel caso Palamara, ma è prassi da sempre ormai generalizzata da molti fornitori di *trojan* alle

Procure di tutta Italia.

Si tratta di un sistema, ancora sconosciuto persino alle Procure che se ne avvalgono, che lascia aperta una miriade di problemi che riguardano la segretezza delle nostre comunicazioni e la *privacy* di tutti. Pertanto, occorre conoscere come funzioni il meccanismo del "cavallo di Troia", visto che la maggior parte dei fornitori l'ha noleggiato a sua volta e non ne conosce nemmeno l'esatto funzionamento. Occorre sapere chi, come e dove mette mano ai dati acquisiti, visto che i *server* si trovano al di fuori della Procura che ha disposto le intercettazioni, talvolta addirittura all'estero, e quindi senza il necessario controllo del P.M. Infine è fondamentale accertare se in tutti questi anni possano essersi verificate manomissioni, anche involontarie, dei dati utilizzati come prova nei processi penali.

Di fronte a tante incognite, emerge una plateale violazione di legge, perché, com'è noto, l'art. 268, comma 3, c.p.p. impone che la registrazione avvenga mediante gli impianti installati presso la Procura della Repubblica, e quindi sotto il controllo del P.M. E tale violazione di legge comporta l'inutilizzabilità dei risultati dell'intercettazione, ex art. 271, comma 1, c.p.p. Ora la circolare della Procura di Milano per prima, ma non è difficile prevedere che sarà seguita da tutti gli uffici giudiziari, spinta dalla "necessità ed urgenza di ridefinire il tracciamento di accessi e interventi" sui *server* delle società private che forniscono alle Procure i *software* delle intercettazioni con captatore informatico, prescrive anzitutto alle società fornitrici che i "*server* di transito" (che sono necessari per non far capire al "bersaglio" che lo si sta intercettando) debbono stare in Italia, dal momento che talvolta sono situati all'estero. Si prescrive altresì che le finte "*App*" per indurre inconsapevolmente il "bersaglio" al sollecitato comportamento che installa il *virus* sul suo cellulare, debbano essere visibili, sui negozi virtuali di applicazioni, solo al "bersaglio" e non anche a ignari utenti che altrimenti potrebbero restare vittime di quella App. Infine, di fronte alla prassi generalizzata del noleggio, la circolare avvisa che d'ora in poi la Procura di Milano accetterà "esclusivamente captatori di proprietà dei fornitori, non noleggiati da società terze" e di cui i fornitori "conoscano nel dettaglio il funzionamento".

Apprezzabile, certamente, anche se tardiva, l'iniziativa della Procura di Milano. Anche se resta l'amarezza per il fatto che, in tutti questi anni, i G.I.P., che dovrebbero essere i garanti della legittimità delle intercettazioni e tutti i giudici d'Italia, che in questi anni le hanno utilizzate, spesso come unica prova, non si sono mai nemmeno posto il problema.

7. L'inutilizzabilità del *trojan* per intercettare le comunicazioni telefoniche o telematiche, né a fini di ispezione, perquisizione e sequestro

Ma non tutte le funzioni che il *malware* sarebbe in grado di svolgere sono ammesse dalla legge, perché l'art. 266, comma 2, c.p.p. limita l'impiego del captatore informatico all'intercettazione delle «comunicazioni tra presenti», che possono essere eseguite «anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile». L'invasività del *trojan*, installato sul dispositivo portatile, è infatti oltremodo potenziata, perché la sua capacità di captazione si spinge fino a seguire l'inconsapevole portatore del dispositivo portatile in ogni luogo in cui egli si rechi, coinvolgendo così qualunque altra persona, anche estranea alle indagini, ma che, per qualsiasi ragione, possa incontrare. Perciò l'art. 267, comma 1, c.p.p. disciplina specificamente i luoghi e il tempo in relazione ai quali «è consentita l'attivazione del microfono», confermando che l'unica attività consentita al *malware* è la registrazione sonora della comunicazione o conversazione tra presenti[28]. Lo stesso art. 266, comma 2, c.p.p. non ammette, invece, l'attività di *on line surveillance*, perché, come già ricordato, consente eccezionalmente l'utilizzo del captatore per intercettare le «comunicazioni tra presenti» e non le telecomunicazioni e quindi non è impiegabile per le comunicazioni telefoniche o telematiche (non a caso l'art. 266-*bis* c.p.p. non menziona il *trojan*).Tanto meno l'art. 266, comma 2, c.p.p. consente l'impiego del captatore per attività di *on line search*, che mirano ad ottenere documenti o dati già individuati, e che danno luogo alle perquisizioni informatiche o telematiche di cui all'art. 247, comma 1-bis, c.p.p.

8. Conclusioni

A nostro parere, occorre tornare ai principi fondamentali in tema di inviolabilità della corrispondenza e delle comunicazioni, ricordandosi che questa costituisce la regola, mentre la limitazione di tale diritto rappresenta l'eccezione. Solo in questo modo si può interpretare correttamente la disciplina del "cavallo di Troia", limitandolo ai casi eccezionali e non facendone un ordinario strumento di indagine.

---

[1] Sez. un., 28.5.2003, Torcasio ed altro, in *Cass. pen.,* 2004, 2094.

[2] Sez. I, n. 3591/2022 del 7.10.2021, afferma che lo *screenshot* di un file *Excel*, contenente un prospetto contabile, eseguito per mezzo di un captatore informatico, non darebbe luogo al sequestro di un documento informatico preesistente all'attività investigativa, ma costituirebbe intercettazione mediante captazione di un flusso di dati *in fieri*, e non sarebbe pertanto riconducibile ad una perquisizione. Il *file* era stato "fotografato" sul *personal computer* in uso ad un indagato dal *malware* ivi inoculato. Secondo la Corte, tale attività investigativa «non ha riguardato l'estrapolazione dal supporto digitale di documenti informatici preesistenti all'attività intercettiva, bensì esclusivamente la captazione di flussi di dati *in fieri*, cristallizzati nel momento stesso della loro formazione». Si sarebbe trattato, perciò, di «una attività di mera "constatazione" dei dati informatici in corso di realizzazione» che, pur non rappresentando una "comunicazione" in senso stretto, costituirebbe, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione - previo provvedimento autorizzativo dell'Autorità giudiziaria - nonché la videoregistrazione, dunque anche la fotografia, avvenuta nel caso di specie mediante *screen shot* della schermata. Secondo la sentenza, nel caso di specie, la "fotografia" sarebbe stata realizzata dalla polizia giudiziaria mentre il documento veniva visualizzato sullo schermo (dunque quando era in atto un flusso di dati) – per cui l'esecuzione dello *screenshot* non consisterebbe nell'estrazione dal *computer* di un documento informatico preesistente, ma si risolverebbe nella captazione di un flusso di dati in corso, cristallizzati nel momento stesso della loro formazione. Pur se tale fotografia non è riconducibile ad una "comunicazione" in senso stretto, secondo la Corte, essa rappresenterebbe un comportamento cd. comunicativo del quale è ammessa la captazione - ovviamente previo provvedimento autorizzativo del giudice - nonché la video-registrazione o, appunto, la fotografia.La Suprema Corte, pertanto, esclude che sia stata realizzata una perquisizione, essendo mancata qualsiasi ricerca e successiva estrapolazione di materiale preesistente dal supporto informatico. A tal proposito, non rileverebbe che nel documento acquisito figurino dati preesistenti alla sua formazione, perché si tratterebbe di una conseguenza della natura del medesimo, che nel caso in esame riporta poste di contabilità, riepilogative di operazioni economiche già effettuate ovvero in corso di realizzazione, delle quali era stata aggiornata l'annotazione e la memoria. In realtà, l'attività investigativa - eseguita da remoto con l'ausilio di un *malware* - dà luogo ad ispezione e perquisizione, regolati dagli artt. 244 e 247, comma 1-*bis*, c.p.p. e la successiva acquisizione del *file* informatico è ovviamente un sequestro. Ma tale attività di ispezione, perquisizione informatica o telematica e sequestro non è ammissibile mediante l'impiego del captatore informatico, giacchè l'art. 266, comma 2, c.p.p. limita l'impiego del captatore informatico all'intercettazione delle «comunicazioni tra presenti» e quindi non consente l'impiego del captatore per attività di *on line search*, che mirano a ispezionare, ricercare ed acquisire documenti o dati. Neppure tale attività di ricerca e acquisizione può essere contrabbandata come prova atipica[2] perché il codice di rito penale disciplina specificamente tali atti di indagine come ispezione, perquisizione e sequestro. Ma l'inquadramento come intercettazione informatica o telematica a mezzo del "cavallo di Troia", anziché come

perquisizione e sequestro, come correttamente si sarebbe dovuto fare, ha permesso di eludere le garanzie difensive prescritte per l'ispezione, la perquisizione e il sequestro, consentendo di acquisire da remoto il *file* contenente il prospetto contabile senza rispettare le norme poste a tutela dell'intervento di una persona di fiducia (art. 250 c.p.p.), del diritto di assistenza del difensore (art. 365 c.p.p.), dell'invio dell'informazione di garanzia (art. 369 c.p.p.) e del diritto di riesame del decreto di sequestro (art. 257 c.p.p.). Ma, più in generale, l'improprio utilizzo del captatore in funzione di ispezione, perquisizione e sequestro ha impedito di adottare le «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione», come prescrivono gli artt. 244, comma 2, e 247, comma 1-*bis* c.p.p.; esso ha anche impedito la realizzazione di una copia dei dati originali, «su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità, potendo anche prescrivere la custodia degli originali anche in luoghi diversi dalla cancelleria o dalla segreteria» (art. 260, comma 2, c.p.p.).

[3] LeSezioni unite hanno affermato che le videoregistrazioni eseguite dalla polizia giudiziaria, anche d'iniziativa, vanno incluse nella categoria delle prove atipiche, soggette alla disciplina dettata dall'art. 189 c.p.p. e, trattandosi della documentazione di attività investigativa non ripetibile, possono essere allegate al relativo verbale e inserite nel fascicolo per il dibattimento.Le stesse Sezioni unite hanno infine affermato il principio che le videoregistrazioni in ambienti in cui è garantita l'intimità e la riservatezza, non riconducibili alla nozione di "domicilio", sono prove atipiche, soggette ad autorizzazione motivata dell'autorità giudiziaria e alla disciplina dettata dall'art. 189c.p.p. (Sez. un., 28.3.2006, Prisco, in *Dir. pen. e proc.*, 2006, 1347).

[4] Sez. III, n. 31515 del 22.7.2020 (dep. 11.11.2020), in *Cass. pen.*, 2021, p. 1348.

[5] È pacifico che esulano dall'ambito di applicabilità dell'art. 266 c.p.p. le conversazioni o comunicazioni attuate con l'uso di emittenti a irradiazione circolare, dal momento che queste, per la loro stessa natura, sono percepibili da chiunque disponga, nel raggio di irradiazione, di un apparecchio ricevente sintonizzato sulla stessa lunghezza d'onda e sono pertanto da considerare prive di ogni carattere di riservatezza : Sez. I, 20.5.1997, Bottaro ed altri, *CED* 207931; Sez. VI, 20.1.1995, Ventura e altro, *Guida dir.*, 1995, 21, 68; Sez. II, 12.11.1994, Seminara, in *Cass.pen.*, 1996, 861; Sez. I, 2.4.1991, Puzzo, *Arch. nuova proc. pen.*, 1991, 467.

[6] Sez. I, 7.11.2007, Ditto, in *Giur. it.*, 2009, 195.

[7] Sez. VI, n. 39771 del 25.9.2014, in *Cass. pen.*, 2014, 1166, secondo cui, nell'ipotesi in cui si proceda ad intercettazione di conversazioni tra presenti ad opera della polizia giudiziaria è sempre necessaria

l'autorizzazione del giudice anche se uno degli interlocutori ne è consapevole, in quanto la sua rinuncia alla riservatezza non rende lecita l'intercettazione ad opera di un terzo che è rimasto estraneo al colloquio. In senso contrario, Sez. IV, del 19.6.2001, La Pietra, in *Guida dir.*, 2001, 41, 95, secondo cui il consenso da parte del legittimo destinatario di una comunicazione telefonica a che un terzo (nella specie, un appartenente alla p.g.] possa ascoltare liberamente il contenuto della comunicazione medesima colloca il fatto stesso al di fuori della disciplina delle intercettazioni telefoniche, dovendosi tale situazione equiparare alla "rivelazione" di una conversazione a opera di chi vi abbia preso parte, al di fuori, perciò, di quel controllo delle conversazioni e delle comunicazioni effettuato "a sorpresa", che caratterizza l'intercettazione vera e propria. Si è anche affermato che l'utilizzabilità delle intercettazioni regolarmente autorizzate dall'autorità giudiziaria ed eseguite nelle forme di legge non viene meno per la circostanza che uno dei partecipanti alle conversazioni sia a conoscenza dello svolgimento delle intercettazioni. In questo caso non opera, infatti, la sanzione di inutilizzabilità applicabile nella diversa fattispecie in cui la polizia guidi la registrazione del contenuto di colloqui privati da parte di uno degli interlocutori, con propri apparecchi che possano captarne il contenuto durante il loro svolgimento e consentirne l'ascolto diretto, così realizzando indirettamente una intercettazione di conversazioni senza la previa autorizzazione dell'autorità giudiziaria (Sez. I, 12.12.2007, D.G., *CED* 238488).

[8] Le Sezioni Unite Torcasio del 2003 affermarono che la registrazione fonografica di conversazioni o comunicazioni realizzata, anche clandestinamente, da soggetto partecipe di dette comunicazioni, o comunque autorizzato ad assistervi, costituisce - sempre che non si tratti della riproduzione di atti processuali - prova documentale secondo la disciplina dell'art. 234 c.p.p. (Sez. Un., 28.5.2003, Torcasio, in *Cass. pen.*,2004, 2094).

[9] Trib. Roma (sez. riesame) 10.8.2015, Guarnera e altri.

[10] Sez. III, n. 29426 del 16.4.2019 (dep. 5.7.2019), in *Guida dir.*, 2019, n. 38, p. 102.

[11] È stato ritenuto legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel *personal computer* in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del *personal computer* o che in futuro sarebbero stati memorizzati (nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull' *hard disk* del computer

in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. c.p.p.) (Sez. V, n. 16556 del 14.10.2009 (dep.29.4.2010), Virruso e altri, Rv. 246954 – 01). Si afferma che i dati contenuti nella memoria di un telefono cellulare o di un *computer* sequestrati (s.m.s., messaggi *WhatsApp*, *e-mail*) possono essere acquisiti come documenti ai sensi dell'art. 234 c.p.p., non essendo necessario ricorrere alle regole stabilite per la corrispondenza, né a quelle relative alle intercettazioni telefoniche (Sez. VI, n. 28269 del 28.5.2019 (dep. 27.6.2019), P.M. in proc. P., in *Guida dir.,* 2019, n. 34, p. 72; Sez. V, n. 1822 del 21.11.2017 (dep.16.1.2018), in *Guida dir.*, 2018, n. 15, p. 96). In particolare, si afferma la legittimità del provvedimento con cui il giudice di merito rigetta l'istanza di acquisizione della trascrizione di conversazioni, effettuate via *WhatsApp* e registrate da uno degli interlocutori, in quanto, pur concretandosi essa nella memorizzazione di un fatto storico, costituente prova documentale, *ex* art. 234 c.p.p., la sua utilizzabilità è, tuttavia, condizionata all'acquisizione del supporto telematico o figurativo contenente la relativa registrazione, al fine di verificare l'affidabilità, la provenienza e l'attendibilità del contenuto di dette conversazioni (Sez. V, n. 49016 del 19.6.2017 (dep. 25.10.2017), in *Cass. pen.*, 2018, p. 2084).

[12] Corte e.d.u, Sez. V, 17.12.2020, Saber *v*. Norvegia.

[13] Sez. VI, 10.10.2005, Assinnata, in *Cass. pen.*, 2006, 3280.

[14] Sez. V, n. 35269 del 21.8.2013, D.B.; Sez. VI, n. 18638 del 17.3.2015, in *Cass. pen.*, 2015, 4169; Sez. II, n. 26323 del 29.5.2014, P.M. in proc. C.L., *CED* 259585; Sez. VI, 18.1.2008, P.F., *CED* 238441; Sez. III, 25.10.2017 (dep. 26.3.2018), Gallotti, n. 14007, in *Guida dir.*, 2018, n. 22, p. 74; Sez. III, n. 33049 del 17.5.2016, B., in *Guida dir.*,2016, n. 41, 76; Sez. VI, 16.10.2018, Cacciola e altri, in *Guida dir.*, 2019, n. 18, p. 74; Sez. V, 5.3.2013, P.M. in proc.Iamonte, in *Giust. pen.*,2013, III, 623; Sez. V, n. 42854 del 25.9.2014, *CED* 261081; Sez. IV, 22.9.2010, Alija e altri, in *Guida dir.*, 2011, n. 21, 58; Sez. II, n. 43410 del 6.10.2015, in *Cass. pen.*,2016, 2155.

[15] Sez. V, 18.2.2003, Ricciotti, in *Giust. pen.*, 2004, III, 43.

[16] Sez. IV, n. 40903/2016 del 28/6/2016, Grassi e altri, che precisa che la detenzione dei *files* all'interno di un singolo *account* protetto da *password* - come all'interno del proprio spazio *Cloud* - è dell'utente che dispone di

quella *password*, come la vettura è nella detenzione di chi ne ha la chiave, non del proprietario del parcheggio che gli ha concesso l'area).

[17] Sez. V,10.3.2021 (dep. 6.5.2021), n. 17552).

[18] Sez. IV, n. 40903 del 28.6.2016 (dep. 30.9.2016), Grassi e altri.

[19] Sez. Un., 19.4.2018 (dep. 27.7.2018), P.M. in proc. Bicchiri e altri, n. 36072, Rv. 273548). Si afferma che l'estrazione di copia integrale dei dati, contenuti in dispositivi informatici o telematici sottoposti a sequestro probatorio, realizza solo una copia-mezzo, che consente la restituzione del dispositivo, ma non legittima il trattenimento della totalità delle informazioni apprese oltre il tempo necessario a selezionare quelle pertinenti al reato per cui si procede (in motivazione la Corte ha precisato che il p.m. è tenuto a predisporre un'adeguata organizzazione per compiere tale selezione nel tempo più breve possibile, soprattutto nel caso in cui i dati siano sequestrati a persone estranee al reato, e provvedere all'esito, alla restituzione della copia-integrale agli aventi diritto) (Sez. VI, n. 34265 del 22. 9. 2020 (dep. 2.12.2020), A. e altri, in *Cass. pen.*, 2021, p. 1001). Nello stesso senso, sez. VI, n. 33045 del 25.1.2018, Mazza; Sez. VI, n. 56733 del 12.9.2018, Macis, Rv. 274781; Sez. VI, n. 13156 del 4.3. 2020, Scagliarini).

[20] Sez. VI, n. 24617 del 10.6.2015, R., *CED* 264093 (in motivazione, la Corte ha osservato che le disposizioni introdotte dalla l. n. 48/2008 riconoscono al "dato informatico", in quanto tale, la caratteristica di oggetto del sequestro, di modo che la restituzione, previo trattenimento di copia, del supporto fisico di memorizzazione, non comporta il venir meno del sequestro quando permane, sul piano del diritto sostanziale, una perdita autonomamente valutabile per il titolare del dato); Sez. V, 23.5.2017, S., n. 25527, *CED* 269811; Sez. III, 21.9.2015, C., n. 38148, *CED* 265181. Va peraltro ricordato che le SU hanno affermato l'ammissibilità del ricorso per cassazione avverso l'ordinanza del tribunale del riesame di conferma del sequestro probatorio di un *computer* o di un supporto informatico, nel caso in cui ne risulti la restituzione previa estrazione di copia dei dati ivi contenuti, sempre che sia dedotto l'interesse, concreto e attuale, alla esclusiva disponibilità dei dati (Sez.un. 7.9.2017, Andreucci, n. 40963, *CED* 270497). Peraltro, secondo la giurisprudenza, l'estrazione dei dati archiviati in un *computer* non dà luogo ad accertamento tecnico irripetibile, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte, come si desume, del resto, dalla disciplina introdotta dalla l. 18.3.2008, n. 48 (Sez. II, n. 29061 del 1.7.2015, n. 29061, p.c. in proc. Artergiani e altro, in *Guida dir.*, 2015, n. 32, p. 91).

[21] Sez. VI, n. 28269 del 28.5.2019 (dep. 27.6.2019), P.M. in proc. P.

[22] Sez. IV, n. 46968 del 5.4. 2017 (dep.12.10.2017), Monteleone.

[23] Sez. III, n. 50452 del 10/11/2015, Guarnera e altri, Rv. 265615.

[24] Sez V, n. 31604 del 30.9.2020 (dep. 11.11.2020),Palazzo, in *Cass. pen.*, 2021, p. 2133, ha 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 c.p.p. Si afferma, infatti, che il *trojan horse* 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.

[25] Si è ritenuta legittima l'intercettazione a mezzo *trojan* anche se utilizza la batteria di proprietà privata dell'intercettato, effettuando un bilanciamento tra l'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio di obbligatorietà dell'azione penale, e il principio di inviolabilità delle comunicazioni (Sez. V, n. 10981 del 30.9.2020 (dep. 22.3.2021), Penza).

[26] Sez. V, n. 31604 del 30.9.2020 (dep. 11.11.2020),Palazzo, in *Cass. pen.*, 2021, p. 2133, ha 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 c.p.p., osservando che il *trojan horse* 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.

[27] FILIPPI, *Quel malaffare del trojan*, in *Penale, diritto e procedura*, 7.6.2021.

[28] Altro problema è quello dei luoghi e dei tempi di accensione e spegnimento del microfono poiché il decreto autorizzativo li indica "anche indirettamente", per cui l'attivazione del microfono è di fatto lasciata all'insindacabile opinione della polizia giudiziaria, la quale quindi è libera di scegliere le conversazioni ed i soggetti da intercettare oppure da tenere fuori delle indagini, come è emerso, clamorosamente, nel "caso Palamara".