CAPITOLO VI

IL CAPTATORE INFORMATICO NEL PROCEDIMENTO PENALE ALLA LUCE DELLE RECENTI MODIFICHE NORMATIVE ED EVOLUZIONI GIURISPRUDENZIALI

di *Marco Pittiruti*

Sommario: 1. Le potenzialità investigative dell'agente intrusore. — 2. Captatore informatico e intercettazioni di comunicazioni tra presenti. — 3. Gli impieghi *extra codicem* del captatore informatico tra atipicità probatoria e tutela dei diritti fondamentali.

1. Le potenzialità investigative dell'agente intrusore.

L'impiego da parte della pubblica accusa di strumenti fino ad ora appannaggio della criminalità informatica e riconducibili alla onnicomprensiva nozione di *malware* — termine che racchiude una vasta pletora di *software* dannosi per l'utente — rappresenta la più evidente manifestazione della ormai avvenuta compenetrazione tra ritrovati tecnologici ed accertamento processuale penale.

Nel novero degli strumenti utilizzati per apprendere elementi utili all'accertamento dei reati, il captatore informatico rappresenta un formidabile arnese investigativo dalle pressoché illimitate potenzialità applicative. Invero, il programma-spia, una volta inserito in un sistema informatico, può rivestire una duplice funzione. Da un lato, esso consente, se utilizzato per la *online surveillance*, di "captare il flusso informativo intercorrente tra le periferiche (quali video, tastiera, microfono, *webcam*) e il micro processore del dispositivo *target*, permettendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo (*screenshot*), digitato attraverso la tastiera (*keylogger*), detto attraverso il microfono, visto per mezzo della *webcam* del sistema bersaglio" (FELICIONI). Dall'altro lato, esso permette agli inquirenti una *online search* della strumentazione oggetto di attenzione investigativa, ossia, di prendere visione e di copiare qualsiasi dato contenuto nel sistema infetto. E si badi: non solo quelli registrati nel sistema ma altresì, in tempo reale, quelli in corso di formazione.

Naturalmente, alle elevate capacità intrusive del captatore è direttamente proporzionale il detrimento che l'attrezzo può arrecare ai diritti fondamentali del soggetto verso cui è orientata l'attività di ricerca. In primo luogo, viene in considerazione l'inviolabilità del domicilio di cui all'art. 14 Cost., nella duplice prospettiva dell'intuibile violazione del domicilio informatico e persino del domicilio *tout court*, qualora l'agente intrusore attivi la videocamera del *computer* o dello *smartphone* e carpisca quanto si svolge nell'ambiente in cui è collocato il dispositivo: se esso si trova nel domicilio, quindi, le immagini trasferite agli inquirenti saranno quelle protette dall'art. 14 Cost. Ulteriori implicazioni si registrano in ordine all'art. 15 Cost., giacché, perlomeno in astratto, il captatore consente di prendere cognizione di ogni attività comunicativa posta in essere dal soggetto monitorato mediante il collegamento ad *Internet*. E da ultimo, può paventarsi, sulla scia della giurisprudenza del *Bundesverfassungsgericht* tedesco, una lesione del neonato diritto all'uso riservato delle tecnologie informatiche, dotato di copertura costituzionale in quanto enucleabile dall'art. 2 Cost. che riconosce i diritti inviolabili della persona (Flor, Orlandi). Se poi dal piano nazionale si passa a quello sovranazionale, risulta compromesso il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza imposto dall'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Come noto, perché l'autorità pubblica possa inficiare i diritti sopra menzionati, è prevista una riserva di legge (artt. 14 Cost. e 8 CEDU) o una duplice riserva di legge e di giurisdizione (art. 15 Cost.). Per tale ragione, anteriormente alla riforma operata dal d.lgs. n. 216/2017, in assenza di una specifica normativa, l'attenzione della dottrina si concentrava precipuamente sulla collocazione sistematica del mezzo di ricerca della prova in questione e sulla sua compatibilità con i suesposti principi fondamentali.

2. Captatore informatico e intercettazione di comunicazioni tra presenti.

Per quanto il d.lgs. n. 216/2017 abbia evidentemente limato gli attriti registrati nella stagione precedente, si tratta di questioni ancora oggi aperte. Con la menzionata riforma, infatti, il legislatore ha inteso disciplinare soltanto uno dei possibili impieghi dell'agente intrusore, vale a dire, come espressamente stabilisce il novellato art. 266, comma 2, c.p.p., l'intercettazione di comunicazioni tra presenti mediante l'inserimento su un dispositivo elettronico portatile.

Anteriormente alla novella, tutte le acquisizioni di conversazioni, telefonate o flussi di dati, a seconda delle caratteristiche del *virus* utilizzato, erano ricondotte alle captazioni di cui agli artt. 266 e ss. c.p.p. Da questo angolo visuale, l'ingresso di una specifica disciplina in tema di agente intrusore nel codice di rito va salutato con favore, giacché la mera equiparazione del congegno in parola alle tradizionali microspie, con conseguente applicabilità delle regole dettate per le intercettazioni, non appariva del tutto soddisfacente. Il captatore informatico presenta, invero, un «*quid pluris*, rispetto alle ordinarie potenzialità dell'intercettazione, costituito [...] dalla possibilità di captare conversazioni tra presenti non solo in una pluralità di luoghi, a seconda degli spostamenti del soggetto, ma, ciò che costituisce il fulcro problematico della questione, senza limitazione di luogo» (Cass. pen., sez. VI, 26 maggio 2015, Musumeci, in *Guida dir.*, 2015, 83 ss.).

Dall'imperfetta sovrapponibilità tra le intercettazioni "tradizionali" e quelle poste in essere attraverso il captatore informatico la Corte di cassazione non aveva, però, desunto l'impossibilità di attivazione *tout court* del congegno in parola. Piuttosto, perché i risultati della captazione fossero utilizzabili, a causa dell'insidiosità dello strumento utilizzato, il decreto autorizzativo avrebbe dovuto, secondo un orientamento, indicare i luoghi ove la captazione dovesse svolgersi, come desumibile dall'art. 266, comma 2, c.p.p., il quale, nel contemplare l'intercettazione di comunicazioni tra presenti in luoghi di privata dimora, subordinandola al requisito che vi sia fondato motivo per ritenere che ivi si stia svolgendo l'attività criminosa, fa riferimento «alla captazione di conversazioni che avvengano in un determinato luogo e non ovunque» (Cass. pen., sez. VI, 26 maggio 2015, Musumeci, cit.).

La tesi appena esposta incontrava, tuttavia, una fondamentale obiezione attinente al dato dell'imprevedibilità, quanto al *locus* della captazione, della intercettazione di comunicazioni tra presenti per il tramite di cimice informatica (Filippi). Giacché il proprietario di uno *smartphone* o di un *tablet* porta la strumentazione con sé in tutti i luoghi frequentati, poteva per il giudice essere assai disagevole, se non addirittura impossibile, indicare in sede autorizzativa gli ambienti nei quali la captazione è ammessa.

L'obiezione in parola è stata, in effetti, autorevolmente recepita dalle Sezioni Unite (Cass. pen., sez. un., 28 aprile 2016, Scurato, in *Proc. pen. giust.*, 2016, 100), le quali, in un *dictum* incentrato precipuamente "sul problema degli spazi suscettibili dall'essere toccati dall'intercettazione" (Camon), hanno affermato la natura necessariamente itinerante dell'attività di captazione svolta mediante *malware*.

Secondo i giudici di legittimità, «il requisito autorizzativo delle intercettazioni tra presenti, incentrato sul fondato motivo di ritenere

che nei luoghi di privata dimora investiti dalle captazioni si stia svolgendo l'attività criminosa, si pone in tutta la sua pienezza, non consentendo eccezioni di alcun genere» (Cass. pen., sez. un., 28 aprile 2016, Scurato, cit.). Poiché, in caso di intercettazione mediante agente intrusore, il giudice «non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto», è impedito il doveroso «controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale» (Cass. pen., sez. un., 28 aprile 2016, Scurato, cit.). Di qui, la logica conclusione secondo cui l'utilizzo del *malware* è consentito unicamente allorché la legge espressamente preveda la possibilità di effettuare captazioni domiciliari pur in assenza della gravità indiziaria sull'attuale svolgimento dell'attività criminosa nei luoghi di cui all'art. 614 c.p.: vale a dire, nell'ambito dei procedimenti finalizzati all'accertamento dei reati di criminalità organizzata.

Sia pure apprezzabile nella misura in cui conteneva i margini di applicabilità del congegno investigativo in analisi, anche questa soluzione non era immune da perplessità, in quanto ancorava al reato per cui si procede — e, dunque, ad una scelta del pubblico ministero sprovvista, almeno nella fase iniziale del procedimento, di controllo alcuno — la possibilità di attivare l'insidioso congegno investigativo. Per consentire l'utilizzo dello strumento captativo, in altre parole, bastava formulare l'imputazione in ordine a una fattispecie di criminalità organizzata. C'è da dire che la soluzione prospettata veniva presentata dalle stesse Sezioni Unite come provvisoria. E infatti, un dato emergeva chiaro dalla pronuncia in parola: ovverosia, la necessità di un intervento legislativo volto a disciplinare compiutamente la materia *de qua*.

A colmare l'evidente lacuna si è incaricato il d.lgs. n. 216/2017, che ha dato attuazione, sul punto, alle deleghe previste dalla l. n. 103/2017 (c.d. legge Orlando). La riforma ha avuto un *iter* assai accidentato, giacché l'entrata in vigore è stata prorogata in diverse occasioni, da ultimo con il d.l. n. 161/2019, convertito con modificazioni dalla l. n. 7/2020 (c.d. legge Bonafede), che ha disposto l'applicabilità delle nuove previsioni alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 30 aprile 2020. Alcuni tratti dell'impianto normativo disegnato dalla riforma Orlando, inoltre, sono stati ritoccati da successivi interventi legislativi, a conferma della difficoltà di raggiungere un soddisfacente bilanciamento tra esigenze investigative e tutela del segreto delle comunicazioni.

Le modifiche hanno recepito solo parzialmente le indicazioni provenienti dal consesso allargato. Appare, anzitutto, inedita la "speciale condizione (generale) di ammissibilità" (Bronzo) dell'agente intrusore coniata dalla riforma Orlando, secondo cui l'impiego del

peculiare strumento deve essere "necessario" per lo svolgimento delle indagini (art. 267, comma 1, c.p.p.). Ciò, in aggiunta ai tradizionali presupposti relativi alla sussistenza di gravi indizi di reato e all'assoluta indispensabilità dell'intercettazione per la prosecuzione dell'attività investigativa. Si onera, quindi, il giudice che autorizza la captazione di redigere una motivazione rafforzata che individui le "specifiche necessità operative che rendano appunto manifesta una più agevole riuscita dell'operazione" (PRETTI) mediante l'impiego del *malware*.

L'impianto normativo delineato dal d.lgs. n. 216/2017 si pone, invece, sostanzialmente in linea con l'arresto giurisprudenziale sopra menzionato laddove consente "sempre" (art. 266, comma 2-*bis*, c.p.p.) l'impiego di agenti intrusori nei procedimenti per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. al fine di intercettare comunicazioni tra presenti nei luoghi di privata dimora. Va segnalato che la l. n. 3/2019 e il d.l. n. 161/2019 hanno, poi, esteso l'applicazione di questa disciplina ai procedimenti finalizzati all'accertamento di delitti commessi da pubblici ufficiali e da incaricati di pubblico servizio contro la pubblica amministrazione punibili con la pena della reclusione non inferiore nel massimo a cinque anni. Tuttavia, mentre nei procedimenti per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater* c.p.p. non è richiesta l'indicazione, nel decreto autorizzativo, dei luoghi e dei tempi nei quali è consentita l'attivazione del captatore (art. 267, comma 1, c.p.p.), in quelli finalizzati all'accertamento di delitti commessi da pubblici ufficiali e da incaricati di pubblico servizio è necessaria l'elencazione delle ragioni che giustificano l'impiego del congegno anche nei luoghi di privata dimora (art. 266, comma 2-*bis*, c.p.p.).

Inoltre, nell'uno come nell'altro caso, si consente che, in presenza di ragioni d'urgenza, il pubblico ministero possa provvisoriamente disporre la captazione mediante l'inserimento del *malware* nel dispositivo elettronico, con decreto soggetto a convalida da parte del giudice entro quarantotto ore dal provvedimento (art. 267, comma 2-*bis*, c.p.p.).

Viceversa, se si procede per reati diversi da quelli indicati dal comma 2-*bis* dell'art. 266 c.p.p. (naturalmente, entro i limiti di ammissibilità di cui all'art. 266, comma 1, c.p.p.), perché possa disporsi l'intercettazione mediante captatore informatico il giudice deve indicare, nel decreto autorizzativo, "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono" (art. 267, comma 1, c.p.p.).

Solo qualora l'intercettazione riguardi comunicazioni tra presenti in luoghi di privata dimora, opera la regola generale secondo cui la captazione è consentita solo allorché vi sia fondato motivo di ritenere che all'interno di quei luoghi si stia svolgendo l'attività criminosa (art. 266, comma 2, c.p.p.).

Simile impostazione legislativa si scontra, però, quanto all'impiego del "*virus* di Stato" (Torre) per l'accertamento di reati diversi da quelli di cui all'art. 51, comma 3-*bis* e 3-*quater* c.p.p. e da quelli commessi dal pubblico ufficiale e dall'incaricato di pubblico servizio contro la pubblica amministrazione, con il già rilevato dato attinente alla natura "ubiquitaria" (Corasaniti) della captazione. Segnatamente, il giudice è impossibilitato ad effettuare il doveroso controllo preventivo sul rispetto della normativa dettata dagli artt. 266, comma 2, e 267, comma 1, c.p.p., in quanto, «anche se fosse teoricamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione nel caso di ingresso in un luogo di privata dimora, [...] l'autorizzazione [all'attività di captazione] verrebbe disposta al buio» (Cass. pen., sez. un., 28 aprile 2016, Scurato, cit.).

Con riferimento alla delimitazione temporale dell'ascolto, l'innovativa previsione di una specifica indicazione, nel decreto autorizzativo, dei "tempi" di attivazione del microfono disegna un regime frastagliato e di complessa gestione da parte degli operanti, nel quale "i tempi di ascolto saranno individuati in ragione di due differenti variabili, l'una relativa all'arco temporale delle operazioni e l'altra in ragione delle singole occasioni di vera e propria captazione" (Pretti).

Il divieto di utilizzazione (art. 271, comma 1-*bis*, c.p.p.) dei dati acquisiti attraverso l'agente intrusore al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo — con successiva distruzione, disposta dal giudice in ogni stato e grado, della documentazione indebitamente appresa (art. 271, comma 3, c.p.p.) — non appare rimedio significativo per le accennate asimmetrie (Marandola). Difatti, per un verso, è lecito prevedere che il materiale captato potrà comunque orientare in maniera decisiva l'attività d'indagine o persino esercitare una celata — ma indubbia — influenza sul convincimento (ad esempio, in sede cautelare) del giudice, il quale, per valutare la rispondenza dell'attività investigativa al perimetro normativo, dovrà giocoforza prendere contezza dei risultati della stessa. Per altro verso, l'espressa regola di esclusione dettata dall'art. 271, comma 1-*bis*, c.p.p. collide con la possibilità che i luoghi e i tempi della captazione siano determinati in sede di decreto autorizzativo solo indirettamente e, dunque, in modo generico, con conseguente eventuale uso *ad explorandum* dell'agente intrusore.

Proprio la necessità di impedire l'impiego patologico di mezzi di ricerca della prova per reperire *notitiae criminis* — come purtroppo emerso nella prassi (Cass. pen., sez. IV, 17 aprile 2012, soc. Ryanair, in *Cass. pen.*, 2013, 1523) — aveva indotto il legislatore a prevedere una disciplina apposita per la circolazione dei risultati. Il novellato art. 270, comma 1-*bis*, c.p.p., nel testo interpolato dalla riforma Orlando, consentiva l'utilizzabilità dei risultati delle operazioni investigative me-

diante captatore informatico "anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione", se indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza. La dizione diversa rispetto alla tradizionale ipotesi di circolazione delle intercettazioni di cui all'art. 270, comma 1, c.p.p. (che permetteva l'impiego dei risultati probatori in *procedimenti* diversi nella sola ipotesi della loro indispensabilità per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza) era stata interpretata nel senso della "non estensibilità dei risultati probatori conseguiti ad ulteriori reati pur appartenenti al medesimo procedimento o allo stesso piano investigativo" (Pretti). Il panorama normativo è, però, nuovamente mutato con la l. n. 7/2020. Alla luce del nuovo testo dell'art. 270, comma 1-*bis*, c.p.p., i risultati delle operazioni mediante *malware* possono essere utilizzati in procedimenti diversi se indispensabili per l'accertamento dei delitti indicati dall'art. 266, comma 2-*bis*, c.p.p. (art. 270, comma 1-*bis*, c.p.p.). Inoltre, il nuovo *incipit* dell'art. 270, comma 1-*bis*, c.p.p. richiama il primo comma della medesima disposizione, anch'esso oggetto di modifica, secondo cui l'impiego *aliunde* dei risultati delle captazioni è possibile solo se gli esiti dell'attività siano "rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'art. 266, comma 1, c.p.p.".

In prospettiva più generale, la normativa ora descritta, come risultante dalle numerose modifiche sin qui succedutesi, appare criticabile laddove prende in considerazione un solo aspetto della sfaccettata attività del captatore informatico e, precisamente, l'intercettazione di comunicazioni tra presenti su dispositivo mobile mediante "l'attivazione del microfono" (art. 267, comma 1, c.p.p.). Interpretando rigorosamente le nuove disposizioni, dunque, l'attivazione da remoto della videocamera della strumentazione-obiettivo si colloca ancora al di fuori del perimetro codicistico.

Inoltre, come premesso, le potenzialità dei *malware* informatici in uso agli operanti vanno ben al di là della mera attivazione del microfono o della videocamera per captare colloqui tra presenti. L'impiego della microspia informatica potrebbe, ad esempio, riguardare flussi di dati in entrata e in uscita dalla strumentazione, oppure conversazioni a distanza intercorse tra l'utilizzatore dell'apparecchio e soggetti terzi.

Non solo. L'art. 266, comma 2, c.p.p. è esplicito nel limitare il proprio perimetro applicativo alle ipotesi di *malware* installato su dispositivi *portatili*. Eppure, il *virus* può ben essere inoculato anche su strumentazione fissa quali *personal computer* o altre apparecchiature connesse ad *Internet* e dotate di videocamera e microfono, quali telecamere o televisori.

In siffatte ipotesi, potrebbe soccorrere, in via interpretativa, l'applicabilità delle disposizione relative alle intercettazioni "tradizionali". L'agente intrusore rappresenterebbe, insomma, una mera modalità operativa (art. 268, comma 3, c.p.p.) delle normali captazioni, sulla scorta della considerazione secondo cui "qualora il luogo sia ben definito e circoscritto, se è possibile installare una cimice allora deve ritenersi praticabile, qualora vi sia un dispositivo fisso adatto, l'inoculazione di un *virus* informatico al solo fine intercettivo-ambientale non itinerante" (CALAVITA).

Quanto all'impiego del *malware* per effettuare videoriprese, si dovrebbero applicare i principi a suo tempo dettati dalle Sezioni Unite (Cass. pen., sez. un., 28 marzo 2006, Prisco, in *Cass. pen*., 2006, 3937): dunque, "per le videoriprese comunicative a mezzo di captatore informatico, la disciplina è interamente mutuata dalle intercettazioni; per le videoriprese non comunicative si distingue tra i luoghi (domiciliari, riservati o pubblici)" (CONTI).

Tale soluzione, tuttavia, non appare pienamente soddisfacente sotto il profilo delle garanzie, in ragione delle già richiamate asimmetrie tra intercettazioni "tradizionali" e *malware* impiegato a fini investigativi e, nello specifico, la maggiore afflittività di quest'ultimo su diritti costituzionalmente tutelati. Il che fa propendere per l'impossibilità di captazioni mediante agente intrusore al di là delle ristrette ipotesi previste dal codice di rito.

Si è ben consapevoli che la tesi volta a sostenere l'illegittimità di simili attività investigative ha un notevole costo in termini di efficacia delle attività di accertamento dei reati. Ciò conforta nel sostenere che — in ossequio all'assunto per cui "*new facts will demand new law*" (KERR) — sarebbe stato quanto mai opportuno un intervento riformatore organico, tale da disciplinare, in apposita sezione del capo IV, tutti gli impieghi investigativi del captatore informatico, con scelte legislative in grado di trovare un efficace bilanciamento tra i due poli della efficienza investigativa e della tutela della segretezza delle comunicazioni e della riservatezza dell'indagato. Allo stato attuale, però, deve ritenersi che la sicura incidenza del *virus* di Stato su diritti fondamentali tutelati da espressa riserva di legge non consenta interpretazioni analogiche estensive della nuova disciplina.

3. Gli impieghi *extra codicem* del captatore informatico tra atipicità probatoria e tutela dei diritti fondamentali.

L'acquisizione di documenti già formati e in corso di formazione all'interno del dispositivo *target* dell'attività investigativa — altra funzione "tradizionale" del *malware* — giace senza dubbio al di fuori

del terreno di elezione degli artt. 266 e 266-*bis* c.p.p., poiché i dati captati non attengono a comunicazioni né ad un flusso di dati intercorrente tra sistemi informatici o telematici.

Si tratta, allora, di appurare se le suddette attività di ricerca della prova, estranee all'alveo delle intercettazioni, possano ritenersi disciplinate da altro istituto codicistico oppure se, per ricavarne la relativa disciplina, debba farsi necessariamente leva sull'ampio contenitore di cui all'art. 189 c.p.p. e, precipuamente, sull'atipicità dell'attività investigativa.

A tale proposito, viene subito in considerazione l'art. 247 c.p.p. In effetti, l'utilizzo di un captatore informatico a fini investigativi, nella sua declinazione di *online search*, è stato agli albori definito da attenti commentatori quale perquisizione *online* oppure elettronica (Marcolini). Ad accomunare i due strumenti è, invero, la natura di atto a sorpresa avente quale fine la ricerca di una *res* in possesso dell'indagato.

I due congegni non sono, però, pienamente sovrapponibili. L'impiego del captatore informatico oblitera il requisito, specificamente previsto dall'art. 247, comma 1-*bis*, c.p.p. con riguardo alle perquisizioni informatiche, secondo cui i dati digitali da apprendere devono essere pertinenti al reato. Difatti, il *malware* consente l'acquisizione di ogni dato contenuto all'interno della strumentazione, a prescindere dal rapporto che lega quanto acquisito con il reato oggetto dell'accertamento, con il conseguente rischio di impiego a fini esplorativi del *virus*.

Inoltre, a marcare ulteriormente il confine tra la perquisizione informatica e quella *online*, sta il dato che per la riuscita della seconda è indispensabile che l'utilizzatore del sistema-obiettivo ignori di essere sottoposto al monitoraggio. Diversamente, nella prima il soggetto perquisito avverte di essere soggetto ad un atto autoritativo, cui si accompagnano le garanzie di cui agli artt. 250 e 365 c.p.p. (Palmieri).

Ne consegue, quale corollario, la fisiologica protrazione nel tempo — contrastante con la tradizionale natura di atto unico e temporalmente limitato delle perquisizioni informatiche — delle operazioni mediante *malware*. Il che impedisce l'azionabilità dello strumento di controllo di cui all'art. 324 c.p.p. per verificare la legittimità dell'eventuale apprensione delle informazioni rilevanti per l'indagine.

Sotto diverso angolo visuale, è la stessa mancanza di un rapporto diretto tra organi inquirenti e strumentazione da sottoporre all'attività investigativa a rappresentare il discrimine tra l'istituto in analisi e quello dell'ispezione informatica.

Agli albori dell'utilizzo del captatore informatico, lo strumento processuale adoperato dalla pubblica accusa per apprendere all'insaputa dell'utilizzatore i dati memorizzati all'interno di un sistema

informatico, nonché quelli ancora da formare, è stato un decreto di acquisizione di documentazione ai sensi dell'art. 234 c.p.p.

Si tratta, con ogni evidenza, di una forzatura interpretativa per due diverse ragioni. Anzitutto, l'istituto della prova documentale mal si adatta alla *digital evidence* in ragione dell'omesso riferimento, nella relativa disciplina, alla doverosa cautela circa la genuinità e corretta conservazione dei dati appresi (Del Coco). E ciò appare inaccettabile, a fronte della intrinseca fragilità e volatilità dei dati informatici (Marafioti). Proprio per questa ragione, del resto, il legislatore, con riferimento alle ipotesi di agente intrusore impiegato quale microspia informatica, ha imposto l'utilizzo di programmi conformi a requisiti tecnici stabiliti dal Ministro della Giustizia, nonché la realizzazione di controlli costanti di integrità a tutela dell'integrale corrispondenza tra dati captati e dati trasmessi agli impianti della procura della Repubblica successivamente al compimento delle operazioni investigative (art. 89, commi 2 e 3, disp. att. c.p.p.). Previsioni, queste, assai opportune, anche alla luce della possibilità che vengano a contatto con i dati soggetti esterni alla pubblica accusa: difatti, per le operazioni di avvio e cessazione delle registrazioni con agente intrusore, la polizia giudiziaria può avvalersi di persone idonee con specifiche competenze tecniche, le quali non possono rifiutare la propria opera (art. 268, comma 3-*bis*, c.p.p.).

Mentre, in più ampia prospettiva, le nuove disposizioni a tutela dell'integrità dei dati del captatore informatico confortano nel ritenere ormai codificato, nel nostro sistema, un vero e proprio statuto della prova digitale improntato ai principi di genuinità e non alterazione, che ha trovato la sua prima e più evidente manifestazione nelle interpolazioni operate dalla l. n. 48/2008 (artt. 244, comma 2, 247, comma 1-*bis*, 254-*bis*, 260, comma 2, nonché artt. 352, comma 1-*bis*, 354, comma 2, c.p.p.). L'articolato sistema che ne risulta precisa i criteri fondanti l'attività di ricerca della *digital evidence* ai quali l'attività degli operanti deve improntarsi, vale a dire la necessaria adozione di tecniche dirette ad assicurare la conformità dei dati acquisiti a quelli originali e a garantire la loro immodificabilità e corretta conservazione in vista della successiva presentazione in sede giudiziale.

In secondo luogo, è chiara l'anomalia conseguente all'applicazione dell'art. 234 c.p.p. per una acquisizione endoprocedimentale di "documenti" informatici che potrebbero persino ancora non esistere, giacché il congegno tecnico utilizzato consente la trasmissione periodica di tutti i dati contenuti nella memoria della strumentazione-bersaglio, quelli già presenti al momento di emanazione del decreto da parte del pubblico ministero così come quelli che successivamente potrebbero essere formati.

Ecco perché l'unico istituto cui ricondurre l'attività appena descritta parrebbe quello dei mezzi di ricerca atipici della prova: e proprio questa è stata la soluzione prescelta dalla Corte di Cassazione (Cass. pen., sez. V, 14 ottobre 2009, Virruso, in *CED Cassazione.*, rv. 246954, nonché, più di recente, Cass. pen., sez. V, 30 maggio 2017, n. 48370, in *Dir. pen. proc.*, 2018, 1063). Si tratta, però, di opzione ermeneutica da sottoporre ad attento scrutinio, stante la delicatezza dei valori in gioco.

Con riguardo ai requisiti imposti dall'art. 189 c.p.p., se non vi è dubbio circa l'idoneità rappresentativa del materiale captato in ordine all'accertamento dei fatti, qualche perplessità sorge circa la compatibilità del congegno con la doverosa tutela diritti fondamentali del soggetto attinto dall'attività investigativa (Caprioli). Quest'ultima, tuttavia, secondo la ricostruzione propugnata nelle pronunce in tema dai giudici di legittimità, non lederebbe alcun bene di rilievo costituzionale. In effetti, come accennato, è ben possibile, dal punto di vista tecnico, che il captatore si limiti all'acquisizione di documenti non destinati alla trasmissione e, dunque, operi al di là del perimetro applicativo dell'art. 15 Cost. Quanto al possibile contrasto con l'art. 14 Cost., la questione in ordine alla compatibilità con la tutela costituzionale del domicilio potrebbe ritenersi addirittura superata, una volta per tutte, dai progressi compiuti nella progettazione dei *malware* utilizzati quali "programmi-spia": al giorno d'oggi, i *trojan* possono essere inseriti nel sistema da remoto, senza alcuna intrusione "fisica" nel luogo ove il *computer* è localizzato.

Eppure, pare indubbio che la tutela del domicilio debba ritenersi, ormai, estesa anche al domicilio informatico, quale "luogo virtuale" in cui si esplica la libertà del cittadino, in ragione del diritto alla riservatezza di cui all'art. 8 CEDU. Assunto, questo, confortato da un innegabile dato: la condotta degli operanti che installano da remoto un *malware* su una strumentazione informatica integra l'elemento oggettivo del reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. Non sono, inoltre, mancate letture volte ad assegnare al domicilio informatico tutela a sé, quale *species* del *genus* diritto alla riservatezza, riconducibile all'art. 2 Cost. (Iovene).

Si fa presto a scorgere, allora, dietro al tema in parola, l'annoso quesito circa l'impiego processuale dei risultati di un mezzo di ricerca della prova atipico lesivo di principi costituzionali. Torna, insomma, a riproporsi, sul terreno del *virus* di Stato, la questione se, in tema di procedimento probatorio, valga il principio per cui ogni prova non vietata dal codice di rito sia ammissibile; oppure se, in ottica diametralmente opposta, in presenza di lesioni a diritti fondamentali, l'attività di ricerca sia consentita solo in presenza di una norma che la preveda espressamente.

Va detto che la soluzione preferibile appare quella di ritenere inutilizzabile il materiale raccolto al di fuori dei casi e modi previsti dalla legge, laddove la Costituzione sancisca una riserva di legge in materia. A fondamento della conclusione appena esposta sono enucleabili diversi argomenti. In primo luogo, essa ha l'indiscutibile pregio di evitare antinomie all'interno del sistema, tenendo a mente il rapporto gerarchico intercorrente tra Costituzione e codice di rito; in secondo luogo, l'applicabilità dell'art. 191 c.p.p. rappresenta un fronte di tutela avanzato in presenza di attività investigative di notevole invasività. E infine, si tenga in conto che l'impostazione promossa appare l'unica aderente al principio di legalità, il quale deve informare l'intero processo, come da costante insegnamento giurisprudenziale. In proposito, basti richiamare l'approdo delle Sezioni Unite (Cass. pen., sez. un., 28 marzo 2006, Prisco, cit.), secondo cui le prove atipiche lesive di diritti costituzionalmente tutelati non possono essere ammesse, in quanto prove illecite.

Se così è, proprio gli artt. 2, 14, 15 Cost. e art. 8 CEDU rappresentano un invalicabile argine all'impiego di captatori informatici in fase investigativa attraverso il *passe-partout* dell'art. 189 c.p.p., tanto da far ritenere che, qualora disposti, essi rientrerebbero nella categoria degli atti "giuridicamente inesistenti" (Daniele). Di qui, la doverosa applicazione dell'art. 191 c.p.p. quale antidoto contro pratiche investigative irrispettose di diritti costituzionalmente sanciti (Lupària). Questa appare l'unica soluzione attenta ai diritti fondamentali in assenza di una disciplina che detti regole specifiche per la *online search*.