CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

L'ACQUISIZIONE DI DATI MEDIANTE SCREENSHOT TRA INTERCETTAZIONE TELEMATICA E PROVA ATIPICA

Con la pronuncia n. 3591/2022, il tema delle investigazioni a mezzo Trojan torna a far parlare di sé. Nel caso di specie, i giudici di legittimità configurano quale intercettazione telematica, ex art. 266 bis c.p.p., l'acquisizione di un "file" in corso di redazione su "personal computer" mediante "screenshot" eseguito da un captatore informatico, «trattandosi di mera constatazione del dato informatico in corso di realizzazione, oggetto di "comportamento comunicativo». Superando tale impostazione, l'Autore si sofferma sulle potenzialità del captatore informatico quale tecnica di sorveglianza speciale da remoto non sempre in grado di reggere alle censure di costituzionalità.

di **Wanda Nocerino**
IUS/16 - DIRITTO PROCESSUALE PENALE
Estratto dal n. 6/2022 - ISSN 2532-9871

Direttore responsabile
Alessio Giaquinto

Pubblicato, Giovedì 23 Giugno 2022

CamminoDiritto.it
ISSN 2532-9871

Abstract ENG

With the sentence n. 3591/2022 the issue of investigations by Trojan Horse makes people talk again. In the present case, the judges of legitimacy configure the acquisition of a "file" being drawn up on a "personal computer" by means of a "screenshot" performed by a computer detector as an electronic interception pursuant to art. 266 bis of the Criminal Code, "since it is a mere ascertainment of the computer data in progress, the object of" communicative behavior. "Overcoming this approach, the Author dwells on the potential of the computer detector as a special remote surveillance technique not always able to withstand the complaints of constitutionality.

Sommario: 1. Gli screenshot al vaglio della Suprema Corte; 2. Le potenzialità funzionali del captatore informatico; 2.1. Segue: le istantanee di schermo. Una modalità di indagine dai contorni sfumati; 3. Il (fallace) tentativo di sussumibilità delle investigazioni a mezzo Trojan nelle categorie probatorie; 4. L'incompleta manovra legislativa; 5. Tra tipicità e atipicità; 6. Le posizioni pregresse sulle funzioni atipiche; 7. Gli screenshot quale modalità tecnologicamente avanzata di videoripresa investigativa nel domicilio; 8. Conclusioni: tentativi di tipizzazione e nuove patologie.

1. Gli screenshot al vaglio della Suprema Corte

Ancora una volta i giudici di legittimità si sono dovuti confrontare sul tema "caldo" delle investigazioni tramite captatore informatico e sull'impiego processuale dei dati acquisiti mediante l'«onnivoro strumento».

In particolare, la Suprema Corte si è pronunciata sull'uso del virus Trojan per acquisire le istantanee dello schermo (c.d. screenshot) di un computer in uso all'indagato. A tal proposito, i giudici chiariscono che «[È] legittima l'acquisizione di un "file" in corso di redazione su "personal computer" mediante "screenshot" eseguito da un captatore informatico, trattandosi di mera constatazione del dato informatico in corso di realizzazione, oggetto di "comportamento comunicativo", suscettibile di intercettazione ed anche di videoregistrazione ai sensi dell'art. 266 bis c.p.p., e non di perquisizione informatica diretta alla ricerca ed estrapolazione di dati preesistenti».

Per comprendere appieno l'iter logico seguito dalla Corte, si ritiene opportuno ripercorrere brevemente la vicenda giudiziaria che ha dato origine alla quaestio de qua, che prende le mosse da un ricorso cautelare della difesa dell'indagato.

CamminoDiritto.it
ISSN 2532-9871

Il Tribunale del riesame di Reggio Calabria confermava l'ordinanza di custodia cautelare in carcere emessa nei confronti dell'indagato per il reato di associazione per delinquere volta alla frode nel pagamento di IVA e accise sui prodotti petroliferi e a riciclaggio dei relativi proventi. Elemento centrale per la sussistenza dei "gravi indizi di reità" era – secondo il Tribunale – il contenuto di alcune intercettazioni telematiche esperite con l'ausilio del virus Trojan relative ad operazioni economiche dalle quali si evinceva che c'erano stati numerosi pagamenti in contanti finalizzati a procurare all'indagato la provvista necessaria al perfezionamento del contratto.

Avverso tale ordinanza ricorreva per Cassazione la difesa dell'indagato, deducendo (tra l'altro) l'inosservanza di norma processuale stabilita a pena di inutilizzabilità, ex art. 606 c.p.p., lett. c) c.p.p., con riferimento all'estrazione di un file excel dal computer in uso all'indagato con l'ausilio del captatore informatico (già impiegato per l'esperimento di intercettazioni ambientali debitamente autorizzate).

A parere del ricorrente, tale attività investigativa – diversamente da come intesa dal Tribunale[1] – si sarebbe dovuta inquadrare nel genus delle perquisizioni informatiche, ex art. 247, comma 1 bis c.p.p., mentre la relativa acquisizione del documento informatico sarebbe qualificabile quale sequestro. Non essendo state adottate le garanzie tipiche poste a presidio dell'esperimento di tali atti investigativi (principalmente, le norme a tutela dell'intervento del difensore, ossia gli artt. 250, 365 e 369 c.p.p., e la disciplina introdotta dalla l. n. 48 del 2008 a presidio dell'acquisizione dei dati informatici), a parere della difesa l'atto sarebbe stato da qualificare quale perquisizione illegittima, escludendosi peraltro, di poter far rifluire tale "perquisizione da remoto" nella categoria della "prova atipica", in teoria ammissibile in presenza dei requisiti previsti dall'art. 189 c.p.p.

La Suprema Corte rigetta l'eccezione difensiva, avallando la soluzione offerta dal Tribunale del riesame.

Precisamente, secondo i giudici di legittimità, lo screenshot di un file excel 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. 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 c.d. comunicativo del quale è ammessa la captazione previo provvedimento autorizzativo dell'autorità giudiziaria.

2. Le potenzialità funzionali del captatore informatico

CamminoDiritto.it
ISSN 2532-9871

Ancor prima di entrare nel merito delle scelte dei giudici di legittimità, lo studioso è chiamato a confrontarsi con le caratteristiche ontologiche del captatore informatico quale prodromo essenziale per cogliere al meglio le riflessioni giuridiche che verranno svolte nel prosieguo della trattazione.

Il captatore informatico è un malware appartenente alla categoria dei sistemi informatici di controllo da remoto (Remote Control System), dal momento che consente di manovrare a distanza la macchina-bersaglio attraverso una connessione di Rete da un qualsiasi altro calcolatore, sfruttando un'architettura di tipo client/server. Attraverso quest'ultimo, abbattendo la protezione del dispositivo, il captatore penetra nell'apparato oggetto di indagine e, nel mentre, tramite il client, il monitorante ne acquisisce il pieno controllo.

La dottrina maggioritaria distingue le attività esperibili a mezzo Trojan in due macro-aree: le online search e le online surveillance[2].

I programmi spia appartenenti alla prima categoria consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico attenzionato.

In particolare, tale tipologia di software è tecnicamente in grado di entrare in maniera occulta all'interno del dispositivo bersaglio al fine di estrapolare dati e informazioni che, una volta copiati, vengono trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione attraverso un indirizzo Internet, in modalità nascosta e protetta.

Attraverso i programmi spia che realizzano la c.d. online surveillance, invece, è possibile monitorare il flusso di dati che coinvolgono un determinato sistema informatico o telematico (ora e durata delle connessioni, invio e ricezione di e-mail, chat, siti Internet visitati, file scaricati, ecc.).

Tentando di "scomporre" le singole attività esperibili mediante il captatore informatico, può dirsi che il malware è in grado di acquisire flussi di comunicazioni tra sistemi informatici e telematici (posta elettronica, messaggistica come Whatsapp, conversazioni Voip come Skype), attivare microfono e/o telecamera e rilevatori GPS. Può, inoltre, eseguire attività di Trojan, vale a dire entrare nella memoria del dispositivo e acquisire tutte le informazioni ivi giacenti o transitanti. In questo caso, il virus è in grado di registrare tutto quanto digitato sulla tastiera (keylogging) e tutto quanto appare sullo schermo (screenshot).

Ogni singola attività può essere abilitata a distanza e, analogamente, disabilitata, ma solo

CamminoDiritto.it
ISSN 2532-9871

dal momento in cui il comando arriva al captatore; ciò vuol dire che può avvenire contestualmente all'invio del comando oppure in maniera ritardata. Inoltre, l'esportazione dei dati verso il server può non avvenire in tempo reale (magari per indisponibilità della Rete) e, in questo caso, le informazioni vengono custodite nell'apparato infettato in attesa della disponibilità d'invio[3].

2.1. Segue: le istantanee di schermo. Una modalità di indagine dai contorni sfumati

L'attività di online search compiuta sulla macchina bersaglio non esaurisce la sua portata nell'osservazione, ricerca e acquisizione dei dati ivi giacenti o transitanti. Il captatore informatico, infatti, può essere impiegato anche in veste di "fotocopiatore" del dispositivo infetto, essendo in grado di captare e registrare l'output video del dispositivo bersaglio, permettendo agli inquirenti di apprendere tutta l'attività visualizzata sullo schermo e di memorizzarla mediante fermo immagine (screenshot).

In tali ipotesi, il malware non funge soltanto da strumento di copia dal server (computer infettato) al client (computer in uso alla p.g.) ma funziona come se fosse un vero e proprio «specchio dello schermo»[4] del dispositivo infettato, idoneo a riflettere – in tempo pressoché reale – le attività che sono compiute all'interno del sistema, consentendo la graduale acquisizione di ciò che nel tempo si somma al dato già acquisito.

Precisamente, con l'uso del Trojan su questa modalità "screenshot" si acquisisce in chiaro (parte di) ciò che è cifrato e che appare sullo schermo dello smartphone o di un personal computer nel momento in cui l'utente utilizza lo strumento informatico[5].

Con delle vere e proprie fotografie dello schermo effettuate dal software posto all'interno dello smartphone/pc, il malware acquisisce – o può comunque acquisire – le informazioni più svariate sia dei contenuti comunicativi sia di quelli non comunicativi. Non si tratta di intercettazione ambientale con l'uso del microfono; non si tratta di captare da remoto tutti i file e contenuti del supporto; bensì soltanto di fare una "foto" di ciò che appare a video ovvero di ciò che l'utente del telefono sta facendo. Spesso quello che viene captato è ciò che si è tentato inutilmente di acquisire con le intercettazioni telematiche. A discrezione dell'operatore, ogni "tot" secondi/minuti/ore (è possibile quindi anche variare il tempo) si può impostare uno screenshot che riprende l'attività che appare sullo schermo. Si pensi alla rubrica, alla navigazione web, al contenuto di una email scritta o letta o ad un documento. Se la cadenza degli screen shot è frequente, potrebbe captare anche una conversazione via chat in tempo reale, ovvero in corso tra due soggetti che si stanno scrivendo mediante le App di messaggistica istantanea.

Si tratta, in questi casi, di una vera e propria forma di sorveglianza perpetua che permette

CamminoDiritto.it
ISSN 2532-9871

di constatare l'evolversi dell'attività criminosa in essere, ma che – allo stesso tempo – incidentalmente coinvolge ogni forma di estrinsecazione dell'attività umana mediante il mezzo informatico, sia essa riconducibile alla vita professionale o a quella privata.

3. Il (fallace) tentativo di sussumibilità delle investigazioni a mezzo Trojan nelle categorie probatorie

Proprio dalla sua intrinseca poliedricità derivano le maggiori perplessità dei giuristi: posto che la tecnologia consente di modulare l'impiego del Trojan a seconda delle esigenze investigative da soddisfare, sembra imprescindibile qualificare giuridicamente le singole attività riconducibili al sistema di controllo da remoto, in modo da individuare la disciplina cui le stesse devono soggiacere, verificando al contempo la tenuta costituzionale e codicistica degli atti di indagine così raccolti.

Invero, la possibilità di attrarre le plurime attività investigative condotte dal Trojan nel genus dei mezzi di ricerca della prova tipici e atipici sarà oggetto di trattazione autonoma nel prosieguo della trattazione[6], rappresentando il punctum dolens della disciplina vigente.

In prima approssimazione, potrebbe ritenersi che l'attivazione del microfono del dispositivo infettato consenta al malware di eseguire intercettazioni tra presenti (art. 266, comma 2 c.p.p.), figurando quale nuova tecnica investigativa da impiegare in luogo delle tradizionali microspie[7]. Inoltre, la captazione del flusso di comunicazioni tra sistemi informatici e telematici potrebbe configurarsi quale intercettazione telematica (art. 266 bis c.p.p.); mentre l'accesso al sistema per ricercare tracce e gli altri effetti materiali del reato che possono giacere nella macchina-bersaglio ed eventualmente acquisire i file di interesse investigativo, potrebbe essere sussunta nell'àmbito delle ispezioni, perquisizioni e sequestri informatici (artt. 244, comma 2, 247, comma 2 bis, 253 e 254 c.p.p.)[8].

Senza voler approfondire le ragioni che spingono l'interprete a discostarsi da una simile e improvvida parificazione, può anticiparsi che gli esiti investigativi ottenuti tramite captatore sembrano difficilmente riconducibili al catalogo degli atti noti, perché le caratteristiche che potrebbero assimilarli ad essi appaiono sempre cedevoli rispetto ai profili differenziali determinati dalle peculiarità dello strumento tecnico impiegato.

In altri termini, pur potendo prima facie avvicinare i risultati investigativi ottenuti mediante il captatore informatico a quelli ricavabili dall'esperimento delle intercettazioni, delle ispezioni, delle perquisizioni e dei sequestri informatici, le potenzialità intrinseche dello strumento portano all'esecuzione di atti di indagine completamente inediti che assommano le caratteristiche proprie dei mezzi di ricerca della prova tipici[9]. A ben

CamminoDiritto.it
ISSN 2532-9871

guardare, infatti, gli esiti fattuali del Trojan sono così ampi e complessi da delineare figure probatorie amorfe, mai normate dal legislatore, rappresentando (tutt'al più) strumenti di esecuzione di mezzi di ricerca della prova atipici[10].

Intanto, consentendo l'attivazione della videocamera eventualmente collocata sul dispositivo, il captatore è in grado di effettuare videoriprese investigative "perpetue" e "ubiquitarie", potendo monitorare costantemente i comportamenti, comunicativi e non, della persona sottoposta a indagine, in ogni momento e in qualsiasi luogo si trovi; l'attivazione del GPS satellitare dell'apparato mobile infetto realizza una forma di pedinamento tecnologico avanzato, "mappando" ogni spostamento del soggetto attenzionato. Infine, l'ipotesi che il Trojan venga abilitato ad un'apprensione generale di tutto ciò che viene digitato sulla tastiera dell'indagato e di tutto quanto compare sullo schermo del dispositivo – anche di testi di tipo comunicativo – sembra di difficile inquadramento se non sul piano dell'atipicità.

In particolare, l'accesso al sistema per la ricerca di tutti dati utili alle indagini, anche se non strettamente connessi alla repressione del reato, determina un'intrusione a fini esplorativi (c.d. perquisizioni online)[11] che, come evidenziato, «è [...] assai più invasiva di un'intercettazione, dato che mentre in quest'ultima ipotesi si capta il contenuto comunicativo che un soggetto ha comunque deciso di rivelare al suo interlocutore, nel caso della visualizzazione dei contenuti digitali si può invadere la sfera più riservata di una persona»[12], determinando finanche una lesione «all'inviolabilità della psiche»[13].

Va comunque anticipato che anche la prospettiva per cui il malware può essere identificato quale strumento di perquisizione online – e, dunque, allocabile nell'àmbito dei mezzi di ricerca della prova atipici – non può essere accolta senza riserve: per evitare censure di incostituzionalità, infatti, anche le categorie probatorie non tipizzate devono garantire la tutela dei diritti inviolabili della persona[14], quali l'art. 13 Cost., baluardo della libertà di ogni individuo, l'art. 14 Cost., posto a protezione del domicilio, l'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione.

Come evidenziato dalla giurisprudenza[15] e dalla dottrina[16], con il captatore informatico è possibile svolgere (anche contemporaneamente) un'eterogenea congerie di attività tipiche e atipiche di indagine pesantemente intrusive delle libertà del soggetto destinatario, eziologicamente volte, come una sorta di "panopticon" benthamiano[17], a sorvegliare ogni atto quotidiano della vita. Dunque, «la valenza intrusiva del captatore è elevatissima, potendo esso effettuare contemporaneamente un'intercettazione ambientale, telematica, effettuare riprese audio e video, una geolocalizzazione, un appostamento e un pedinamento informatico, rastrellando una grande quantità di dati e immagini tratti

CamminoDiritto.it
ISSN 2532-9871

dall'ambiente circostante»[18].

Ci si trova, dunque, difronte ad uno strumento «onnivoro»[19], atto a realizzare forme di controllo assai pervasive e, proprio per tale ragione, di «spiccata invadenza»[20], tali da rendere pienamente comprensibili gli interrogativi da parte di chi sottolinea il potenziale grave vulnus alle garanzie fondamentali dei singoli, con l'aggravante dell'assenza di una rigida forma di regolamentazione delle attività – diverse e altre rispetto all'intercettazione stricto sensu intesa – esperibili tramite il mezzo in esame[21].

4. L'incompleta manovra legislativa

La materia delle intercettazioni mediante captatore informatico rappresenta il frutto di una stratificazione giurisprudenziale[22] e legislativa senza precedenti. Nonostante gli sforzi profusi, le nuove disposizioni trovano compiuta realizzazione solo quattro anni dopo il primo intervento riformatore. Questa vicenda, si è detto, «presenta i tratti del grottesco»[23] .

Più nel dettaglio, la riforma operata dal d.lgs. 29 dicembre 2017, n. 216[24], in attuazione della delega contenuta nell'art. 1 della l. 23 giugno 2017, n. 103[25], sarebbe dovuta entrare in vigore il 26 luglio 2018 ma subisce nell'immediatezza tre rinvii con altrettanti provvedimenti normativi: la data del 31 marzo 2019 prevista dall'art. 2 del d.l. 25 luglio 2018, n. 91 viene prorogata al 31 luglio 2019[26] e successivamente rinviata al 31 dicembre 2019[27]. Poi, proprio nel giorno della sua entrata in vigore, il Consiglio dei Ministri approva la contro-riforma del sistema delle intercettazioni[28]. Il che, sebbene inaspettato perché improvviso, non ha sorpreso a causa del mutamento della compagine governativa con l'insediamento in Parlamento della nuova legislatura[29].

Secondo la novella del 2019, la normativa avrebbe dovuto trovare applicazione ai procedimenti penali iscritti dopo il 29 febbraio 2020. Naturalmente, si è trattato di un termine irrealistico, «tanto da far sorgere il dubbio che fosse stato inserito solo per asseverare l'urgenza dell'intervento e giustificare il ricorso alla decretazione d'urgenza» [30].

Puntualmente, in sede di conversione, il Parlamento prospetta tempi ragionevolmente più lunghi, facendo slittare l'entrata in vigore tra il 30 aprile e il 1 maggio[31]. Ma ulteriori rinvii non tardano ad arrivare. Subito dopo l'approvazione della legge 7/2020, il mondo intero si accinge a combattere la lotta pandemica contro il Covid-19. La nuova emergenza impedisce evidentemente di completare quelle «complesse misure organizzative in atto, anche relativamente alla predisposizione di apparati elettronici e digitali» e di effettuare «le attività di collaudo dei sistemi presso i singoli uffici giudiziari delle procure della

CamminoDiritto.it
ISSN 2532-9871

Repubblica» in modo da «giungere all'entrata in vigore della disciplina con le misure organizzative completamente dispiegate e funzionanti»[32]. Così il 30 aprile 2020, viene procrastinata nuovamente l'entrata in vigore della normativa, stabilendo che le nuove disposizione si applicano ai procedimenti penali iscritti dopo il 31 agosto 2020[33].

Benchè al nuovo legislatore sia stata concessa la chance di "correggere il tiro" rispetto agli errori fatti e rilevati dalla dottrina e dalla giurisprudenza durante quest'ultimo biennio, la riforma sembra acuire le preoccupazioni degli esperti del settore, nascondendo molte insidie per la tenuta del sistema e l'efficacia stessa dello strumento intercettivo.

Al fine di individuare gli elementi di novità apportati dal legislatore del 2020, occorre inevitabilmente richiamare l'impianto normativo su cui si sedimenta la novella.

Come già anticipato, il d.lgs. 216/2017 ha introdotto un nuovo comma 2 bis all'art. 266 c.p.p., prevedendo che sono sempre consentite le intercettazioni tra presenti – anche nei luoghi di privata dimora (art. 614 c.p.), a prescindere dalla sussistenza del fondato motivo di ritenere che in quel luogo si stia svolgendo un'attività criminosa – mediante l'inserimento di captatore informatico solo nel caso in cui si proceda per i delitti di cui all'art. 51, commi 3 bis e 3 quater c.p.p.[34]; viceversa, per tutte le altre fattispecie delittuose, le captazioni mediante virus informatico in àmbito domiciliare possono essere autorizzate solo ove sussista il sopra indicato requisito, seguendo la regolare disciplina delle intercettazioni.

Su questo impianto è poi intervenuta la l. 3/2019 che, innestando nella disposizione di cui all'art. 266, comma 2 bis c.p.p. una nuova categoria criminosa intercettabile senza limiti con l'ausilio del virus informatico, equipara de facto i procedimenti per i delitti "gravi" dei pubblici ufficiali contro la pubblica amministrazione a quelli di cui all'art. 51, commi 3 bis e 3 quater c.p.p.[35].

Tali modifiche sono oggetto di ulteriore interpolazione ad opera del d.l. 161/2019 con la specificazione che i delitti contro la pubblica amministrazione per cui si applica la più blanda disciplina di cui all'art. 266, comma 2 bis c.p.p. sono quelli commessi, oltre che dai pubblici ufficiali, anche dagli incaricati di pubblico servizio[36].

Come precisato, questa interpolazione sembra rivolta ad affrontare uno dei dubbi interpretativi che gli art. 4 e 6 del d.lgs. 216 del 2017 poteva ingenerare[37].

Una interpretazione letterale di tali disposizioni poteva indurre a ritenere che gli standards richiesti per le indagini in tema di criminalità organizzata fossero stati estesi alle

CamminoDiritto.it
ISSN 2532-9871

investigazioni che, nell'àmbito dei delitti contro la pubblica amministrazione, riguardavano più precisamente quelli di cui al Capo I – intitolato proprio "Dei delitti dei pubblici ufficiali contro la pubblica amministrazione" – del Titolo II del Libro II c.p.[38].

La previsione in parola, ai fini del ricorso al captatore informatico nei reati contro la pubblica amministrazione, riconosce rilievo alla qualifica soggettiva riconosciuta all'indagato: come precisato, «[S]embra sostenibile, pertanto, che lo strumento tecnologico in esame possa essere impiegato per tutti i "delitti contro la pubblica amministrazione", compresi nel titolo II, del Libro II del codice penale, commessi tanto dai pubblici ufficiali, quanto dagli incaricati di pubblico servizio, ovviamente sempre che sussistano i presupposti di ammissibilità indicati dalla norma [...]»[39].

Allo stato dell'arte, dunque, vige una disciplina "tripartita" in materia di captazioni nei luoghi domiciliari mediante Trojan: da una parte, vi sono i reati di criminalità organizzata ed economica (richiamati dall'art. 266, comma 2 bis c.p.p.), per cui sono sempre consentite le intercettazioni ambientali domiciliari; dall'altra, i reati "comuni", per i quali, invece, l'impiego dello strumento soggiace ai limiti di cui al comma 2 del medesimo articolo; dall'altra ancora, esiste una normazione ibrida in relazione ai procedimenti facenti capo a un'associazione per delinquere seppur diversa dalle fattispecie contemplate dall'art. 51, commi 3 bis e 3 quater c.p.p.[40] – nonché quelli la cui disciplina risulta equiparata all'art. 13 del d.l. n. 152/91 – per i quali, invece, pur non essendo previsto un limite all'intrusione domiciliare in ragione del "doppio binario investigativo", non trova applicazione né la disciplina più estensiva del nuovo comma 2 bis dell'art. 266 c.p.p. né le altre disposizioni derogatorie di cui all'art. 267, comma 1 e 2 bis c.p.p.

In relazione al decreto autorizzativo "rafforzato", il comma 1 dell'art. 267 c.p.p. viene progressivamente arricchito: prima, dall'art. 4, comma 1, lett. b, punto 1 del d.lgs. 216/2017 che introduce la precisazione dei tempi e dei luoghi oggetto di captazione nel caso in cui si proceda per delitti diversi da quelli di cui all'art. 51, commi 3 bis e 3 quater c.p.p.; poi, dall'art. 1, comma 4, lett. b, l. 3/2019, che amplia la deroga anche ai delitti commessi dai pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni determinata ai sensi dell'art. 4 c.p.p. Da ultimo, l'art. 2, comma 1, lett. d, punto 1, d.l. 161/2019 prevede che la deroga valga anche nel caso degli stessi delitti commessi dagli incaricati di pubblico servizio[41].

Occorre solo un'ultima precisazione: come espressamente previsto in sede di conversione del d.l. n. 161/2019, nel caso in cui si proceda per delitti contro la pubblica amministrazione di cui all'art. 266, comma 2 bis, c.p.p., il decreto autorizzativo deve anche specificare le ragioni che giustificano l'impiego del captatore informatico e l'esercizio delle operazioni anche nei luoghi di cui all'art. 614 c.p.[42].

CamminoDiritto.it
ISSN 2532-9871

Tale contenuto non sembra coincidere con il fondato motivo per ritenere che in un ambiente, riconducibile alla previsione dell'art. 614 c.p., sia in corso l'attività criminosa; presupposto richiesto dall'art. 266, comma 2 c.p.p. per lo svolgimento di intercettazioni tra presenti per reati diversi da quelli contemplati dal comma 2 bis dello stesso articolo in simili luoghi. Come sostenuto, si tratta verosimilmente «di qualcosa di meno della dimostrazione che sia in atto l'attività criminosa, ma comunque di un dato che vale a giustificare l'intrusione nel domicilio»[43].

Così facendo, il legislatore intende diversificare ulteriormente la disciplina prevista per i reati economici rispetto a quella riservata ai reati di cui all'art. 51, commi 3 bis e 3 quater, c.p.p., aggravando gli oneri motivazionali del giudice.

In sostanza, il decreto autorizzativo, pur non dovendo indicare i luoghi e i tempi delle captazioni in ragione del disposto di cui all'art. 267, comma 1 c.p.p., deve, per converso, prevedere i motivi che giustificano il ricorso allo strumento per le captazioni domiciliari che, è bene ribadirlo, non soggiace ad alcuna limitazione, secondo il disposto di cui all'art. 266, comma 2 bis c.p.p.

Discutibile appare la scelta di aggravare l'onere motivazione da parte del giudicante allorquando autorizza il compimento delle operazioni di intercettazione mediante captatore informatico all'interno del domicilio qualora si proceda per reati contro la pubblica amministrazione.

Come osservato, l'"utilità" richiesta «appare difficilmente rinnegabile, posto che [...] è facilmente intuibile l'utilità di una intercettazione all'interno dell'abitazione, specialmente laddove si ipotizzino confidenze dell'indagato con i familiari conviventi. Se si considera poi che, non trattandosi di un presupposto di ammissibilità, l'eventuale omessa indicazione delle suddette ragioni non sconta certamente la sanzione di inutilizzabilità dei risultati, di cui al comma 1 dell'art. 271 c.p.p., in quanto non eseguita al di fuori dei casi consentiti dalla legge, la novità appare, francamente, di modesta portata innovativa»[44].

In relazione, invece, ai profili "tecnici", vanno segnalate, le modifiche apportate all'art. 89 disp. att. c.p.p. Si interviene sul comma 2, prevedendo che, ai fini dell'installazione e dell'intercettazione attraverso captatore informatico in dispositivi elettronici portatili devono – anziché possono – essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministero della giustizia. Si tratta di una modifica che, nel voler rafforzare il divieto d'uso di programmi non conformi, appare di scarso impatto rispetto a quanto già era previsto dal "decreto Bonafede".

CamminoDiritto.it
ISSN 2532-9871

Al comma 3 del medesimo articolo, viene introdotta una nuova procedura di trasferimento e custodia dei dati appresi, per cui gli stessi devono essere "conferiti" presso gli impianti della procura della Repubblica[45] e ivi trasmessi ricorrendo a procedure tecniche idonee a garantire l'integrale corrispondenza tra quanto registrato e trasmesso[46]. Se, tuttavia, appare impossibile procedere al contestuale trasferimento dei dati intercettati, il verbale deve anche indicare le ragioni tecniche impeditive e della successione cronologica degli accadimenti captati e delle conversazioni intercettate.

L'aspetto maggiormente rilevante della novella del 2020 inerisce alle riforme che intaccano la disciplina dei divieti di utilizzazione probatoria dei dati illegittimamente appresi (art. 270 c.p.p.)[47].

Più precisamente, il comma 1 dell'art. 270 c.p.p., rimasto immune ai ritocchi normativi pregressi, subisce una modifica in sede di conversione sotto un duplice profilo: da un lato, si rafforzano le condizioni che legittimano l'impiego dei risultati captativi in procedimenti diversi da quelli indicati nel decreto autorizzativo; dall'altro, viene introdotta un'ulteriore ipotesi derogatoria al regime di inutilizzabilità, prevedendo che la trasmigrazione del captato possa considerarsi legittima allorquando risulti «necessaria e indispensabile» non solo per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio, ma anche dei reati di cui all'art. 266, comma 1 c.p.p.[48].

L'inserimento, a distanza di meno di due mesi dalla pronuncia delle Sezioni Unite "Cavallo"[49], del riferimento all'art. 266 c.p.p. potrebbe indurre a ritenere, in sede di prima ma poco attenta esegesi della norma, che il legislatore abbia inteso positivizzare le condizioni indicate dalla Suprema Corte ai fini dell'impiego extraprocedimentale delle risultanze intercettive.

In questo senso, potrebbe propendersi per l'utilizzabilità delle captazioni in procedimenti diversi sempre che si tratti di fattispecie ricomprese nel catalogo declinato dal comma 1 dell'art. 266 c.p.p., ovverosia di reati per i quali sarebbero comunque state consentite ab origine le operazioni di intercettazione.

Come anche sostenuto dalla dottrina[50], una simile lettura non può essere avallata, in quanto il riferimento all'art. 266 c.p.p. nell'attuale formulazione dell'art. 270 c.p.p. è accostato non all'indicazione del divieto di utilizzazione in procedimenti diversi quanto piuttosto alle ipotesi dei reati per i quali sia previsto l'arresto obbligatorio in flagranza e per i quali l'utilizzabilità è invece ammessa senza limiti.

Di conseguenza, la nuova disciplina ammette l'impiego dei risultati delle intercettazioni in procedimenti diversi non soltanto qualora le captazioni risultino necessarie ed

CamminoDiritto.it
ISSN 2532-9871

indispensabili per l'accertamento dei delitti per i quali sia previsto l'arresto obbligatorio in flagranza ma anche, in alternativa, per i reati indicati nel corpo del comma 1 dell'art. 266 c.p.p. La bontà di tale soluzione interpretativa trova conferma, peraltro, proprio nei lavori parlamentari[51], laddove si indica che tale modifica estende l'utilizzabilità delle intercettazioni in procedimenti diversi anche nei casi indicati dall'art. 266 c.p.p. per i quali non sia previsto l'arresto obbligatorio in flagranza[52].

Per quanto concerne il comma 1 bis dell'art. 270 c.p.p., nella formulazione originaria del 2017, si era previsto che i risultati raccolti mediante captatore informatico non potessero essere utilizzati per la prova di delitti diversi da quelli autorizzati, «salvo che gli stessi siano necessari per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio».

Anche sul punto, il legislatore del 2020 interviene in maniera assai incisiva, ribaltando la struttura della disposizione che, da norma di divieto, si trasforma in una norma di autorizzazione, con l'unica condizione che i reati da provare rientrino nella categoria di quelli per i quali il ricorso al captatore è autorizzato dal relativo decreto.

Ai sensi della nuova normativa, fermo restando il divieto di impiego del prodotto delle captazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte[53], «[...] i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'articolo 266, comma 2 bis» c.p.p.[54], condizionando il loro impiego al canone della "indispensabilità"[55].

Allo stato, dunque, è possibile utilizzare le risultanze delle attività captative condotte mediante Trojan per la prova di reati diversi da quelli contemplati dal decreto autorizzativo, purché ricompresi tra i gravi crimini di cui all'art. 51, commi 3 bis e 3 quater c.p.p. e quelli commessi dai pubblici ufficiali o gli incaricati di pubblico servizio contro la pubblica amministrazione, nonché per la prova dei delitti per i quali è obbligatorio l'arresto in flagranza.

A ben guardare, la contro-riforma tende a sgretolare la regola dell'inutilizzabilità, estendendo il perimetro di operatività del regime derogatorio: nell'ottica di un coordinamento con l'interpretazione fornita dalla Suprema Corte al concetto di "diverso reato" e "diverso procedimento"[56], si deve ritenere che il divieto di circolazione delle informazioni apprese mediante captatore non opera (oltre che in relazione ai casi espressamente previsti dal dettato normativo di cui al comma 1 dell'art. 270 c.p.p., espressamente richiamato nell'incipit del comma 1 bis del medesimo articolo), con

CamminoDiritto.it
ISSN 2532-9871

riferimento ai reati diversi ma connessi ex art. 12 c.p.p.[57], nonché ai reati diversi non connessi che rientrano nei casi di cui all'art. 266, comma 2 bis c.p.p.

La novella apre, dunque, la strada "libera" circolazione probatoria delle risultanze della captazione digitale determinando una sostanziale violazione della garanzia della riserva di giurisdizione prevista dall'art. 15 Cost.[58], con riferimento all'intercettazione confluita nel "procedimento diverso", in assenza di qualsivoglia controllo da parte del giudice procedente.

In sostanza, il rischio è che una volta ottenuta l'autorizzazione all'impiego del virus informatico in riferimento ad un certo reato all'interno di un determinato procedimento – e quindi anche sulla base di motivi concernenti la posizione dell'indagato in quel procedimento per quella specifica fattispecie delittuosa – le informazioni ottenute possano essere utilizzate anche in indagini diverse per la prova di reati differenti, benché, in questi non sussistano o comunque non siano stati verificati i presupposti per l'emissione di un analogo provvedimento autorizzativo.

5. Tra tipicità e atipicità

Lo si è anticipato sin dalle prime battute del lavoro[59]; il più complesso problema da risolvere è la tassonomia probatoria in cui ascrivere il captatore informatico. Date le sue potenzialità tecnologiche dirompenti è suscettibile di molteplici inquadramenti, ben potendo appartenere a ciascuna categoria dei mezzi di ricerca della prova a disposizione del codice di procedura penale italiano.

Si sa che il legislatore – tra le diverse alternative prospettabili – ha scelto di limitare le funzionalità del virus, di modo che, attraverso l'attivazione del microfono del dispositivo "infetto", si potesse procedere alla sola captazione delle registrazioni audio. L'obiettivo è quello di attribuire al captatore elettronico un preciso volto, quello di una «cimice informatica»[60], ossia di uno strumento inedito per dare esecuzione ad un mezzo tradizionale di ricerca della prova, rappresentato dall'intercettazione di conversazioni e comunicazioni tra presenti (art. 266, comma 2 c.p.p.)[61].

Probabilmente (ma più che una supposizione è una certezza) il legislatore ha cercato la soluzione più agevole, quella che comporta meno sacrificio in termini di utilità investigativa, senza rinunciare – almeno formalmente – alla tutela dei diritti inviolabili.

Se l'impiego del Trojan Horse fosse davvero limitato a quanto or ora descritto non ci sarebbero problemi né questioni di cui parlare. Tuttavia, così non è.

CamminoDiritto.it
ISSN 2532-9871

L'introduzione di una legge ad hoc volta a disciplinare l'impiego del captatore informatico nel processo penale quale strumento tecnico di intercettazione ambientale non esaurisce né l'impiego che se ne fa quotidianamente né la querelle processuale. Il Trojan continua a suscitare forte disagio tra gli studiosi e gli operatori, spiegabile con la congenita illimitatezza delle sue funzioni, da un lato, e l'inquietante silenzio legislativo, dall'altro.

Sul punto, si registrano due orientamenti dottrinali antitetici: c'è chi[62] propende per l'illiceità della "altre" attività che il virus – almeno in potenza – è in grado di dispiegare e chi[63], al contrario, ne ammette una qualche forma di utilizzo in ragione della "tipicità" dei risultati probatori ottenuti.

Più in particolare, stante l'incidenza sul piano dei diritti fondamentali di una simile tecnica investigativa, secondo alcuni parrebbe necessario limitarne il più possibile la sfera operativa, restringendo il campo di azione alle sole intercettazioni di comunicazioni tra presenti, come previsto nella novella del 2017: la mancanza di una previsione legislativa espressa delle funzioni diverse dalla captazione di conversazioni e comunicazioni ex art. 266, comma 2 c.p.p., «potrebbe suonare come un'esclusione»[64].

Contrariamente, si sostiene che la lacuna legislativa non permette di ritenere che le attività investigative di cui si discute debbano ritenersi vietate e, come tali, insuscettibili di fornire materiali probatori utilizzabili in giudizio. Ciò «perché alcune di tali attività [...] sono riconducibili a strumenti di ricerca della prova già disciplinati dalla legge (segnatamente, l'intercettazione di comunicazioni) e comunque, perché nel sistema processuale penale italiano non esiste un principio di tassatività della prova, essendo il giudice espressamente autorizzato ad assumere anche "prove non disciplinate dalla legge" (art. 189 c.p.p.)»[65].

A ben riflettere, dalle impostazioni dottrinali richiamate emerge che la legittimità degli atti di indagine provenienti dagli usi ultronei del Trojan è strettamente interconnessa alla qualifica giuridica ad essi riconosciuta: qualora tali atti dovessero rientrare nell'àmbito delle categorie probatorie più o meno note al sistema processuale, non sarebbe preclusa la possibilità di utilizzare le altre funzioni del captatore informatico che esulano dall'attivazione del microfono del dispositivo; se, invece, il polimorfismo del virus desse luogo ad atti di indagine non sussumibili in nessun mezzo di ricerca della prova (tipico o atipico), allora si dovrebbe ritenere che il software possa assumere solamente la fisionomia di una cimice informatica.

6. Le posizioni pregresse sulle funzioni atipiche

CamminoDiritto.it
ISSN 2532-9871

Delineato lo stato dell'arte, sembra doveroso comprendere le posizioni della giurisprudenza che – nei suoi illustri e isolati precedenti – tende ad assimilare due funzionalità del Trojan in modalità di online search, ossia il keylogging e gli screenshot.

In particolare, la Corte ne consacra la legittimità ritenendo che tali attività rappresentino solo una modalità nuova, stravagante e diversa di istituti giuridici tradizionali[66].

In relazione al keylogging, una recente pronuncia della Suprema Corte chiarisce che «l'uso del Trojan [...] è [volto] all'acquisizione delle password di accesso agli account di posta elettronica. Ottenute queste password, gli inquirenti [...] prendono visione dei messaggi che vengono via via inviati o ricevuti e dei messaggi che vengono salvati nella cartella "bozze"». Di conseguenza, «si è usato il programma informatico [...] così come si è da sempre usata la microspia per le intercettazioni»[67].

In sostanza, a parere della Suprema Corte, la funzione di keylogging rappresenta solo una modalità alternativa alle tradizionali microspie, idonea a compiere intercettazioni telematiche (art. 266 bis c.p.p.) o ambientali (art. 266, comma 2 c.p.p.).

Sul punto, tuttavia, si avanzano delle riserve. Non sembra, invero, che il software sia adoperato per cogliere comunicazioni, quanto piuttosto per individuare ciò che viene digitato sul computer; in questo modo vengono acquisite le password che consentono l'accesso agli account di posta elettronica ed alle mail contenute.

In questi casi, «[A]ppare arduo ricomprendere la digitazione sulla tastiera di un computer necessaria per accedere ad una casella di posta elettronica nel concetto di comunicazione» [68], rappresentando un flusso unidirezionale di dati.

D'altra parte, l'attività acquisitiva delle credenziali di accesso alla casella di posta elettronica, prodromica all'attività intercettiva stricto sensu intesa, non così agevolmente può essere sussunta nell'àmbito di un'ispezione o una perquisizione di tipo elettronico che ha condotto al sequestro della password[69]. Come già più volte chiarito, a fronte di un'incompatibilità intrinseca tra il captatore informatico – che determina un monitoraggio occulto e totalizzante del soggetto attenzionato – e i mezzi di ricerca della prova tipici – che si traducono in atti investigativi palesi –, sembra che l'attività de qua rappresenti un'indagine "scomposta" nella quale i risultati investigativi tipici sono il frutto di atti di indagine atipici.

Il ragionamento or ora condotto può essere in parte esteso anche all'impiego degli screenshot nel procedimento penale.

CamminoDiritto.it
ISSN 2532-9871

Di recente, la Corte di Cassazione ha previsto che l'acquisizione degli screenshot o dei singoli file può essere assimilata «alla captazione in tempo reale di flussi informatici transitati sul computer dell'indagato, ovvero di flussi informatici transitati sui dispositivi, rientrante, quest'ultima, nel concetto di intercettazione»[70].

Anche in questo caso, l'assimilazione di questa peculiare tecnica investigativa alle intercettazioni telematiche appare eccessivamente semplicistica[71]. Pur potendo captare anche un flusso comunicativo, «[N]on si tratta di intercettazioni ambientali con l'uso del microfono; non si tratta di captare da remoto tutti i file e contenuti del supporto, bensì [...] di fare una "foto" di ciò che appare a video ovvero di ciò che l'utente del telefono sta facendo»[72].

Pur sussistendo un decreto con cui si autorizza l'intercettazione telematica, avvalendosi del Trojan in modalità screenshot si acquisisce in chiaro (parte di) ciò che è cifrato e che appare sullo schermo dello smartphone o di un computer nel momento in cui l'utente utilizza lo strumento informatico: con delle vere e proprie fotografie dello schermo effettuate dal software posto all'interno del dispositivo elettronico il malware acquisisce – o può comunque acquisire – le informazioni più svariate sia dei contenuti comunicativi sia di quelli non comunicativi, nonché quelle che esulano dall'interesse investigativo concretamente perseguito dagli inquirenti[73].

Dunque, seppur il trend seguito dalla giurisprudenza sia volto a legittimare l'impiego del captatore a prescindere dalla funzione utilizzata, l'attività svolta con il captatore informatico realizza qualcosa di «trasversale»[74] rispetto al panorama giuridico esistente; attività che solo in parte, con interpretazioni estensive ai limiti della forzatura, è possibile far rientrare nel concetto di prova tipica.

In questi casi, si ritiene preferibile l'impostazione per cui l'attività de qua sia assimilabile alle perquisizioni online, avendo ad oggetto il monitoraggio occulto dei "movimenti" in rete atto all'acquisizione di informazioni – anche e molto spesso – non comunicative.

Non si può tuttavia negare che l'acquisizione di dati informatici condotta mediante l'impiego del malware rappresenti qualcosa di più e di diverso rispetto un'investigazione atipica "tradizionale": controllare in modo occulto e continuativo ciò che una persona digita sulla tastiera e ciò che visualizza sullo schermo del proprio device, non solo mette a repentaglio la riservatezza genericamente intesa del soggetto monitorato ma qualcosa di molto più profondo e intimo. Il dispositivo elettronico, soprattutto se mobile, rappresenta «un'appendice della persona, in grado di rivelarne i segreti più nascosti ed inconfessabili» [75]. Di qui, può sostenersi che la videoregistrazione della successione della schermata di

CamminoDiritto.it
ISSN 2532-9871

un computer e lo spionaggio della digitazione della tastiera rappresentano attività che giungono ad un livello di invasività tale da «aggredire il foro interno di una persona»[76], riferibile a quel complesso di diritti espressamente tutelato dagli artt. 14 e 15 Cost., anche con precipuo riferimento alla protezione della proiezione dell'individuo nell'etere digitale, presidiando la sua soggettività in rapporto a qualunque dato o attività svolta nell'àmbito di un sistema informatico e della Rete.

7. Gli screenshot quale modalità tecnologicamente avanzata di videoripresa investigativa nel domicilio

Dalla ricostruzione or ora effettuata, emerge che gli screenshot assumano sembianze diverse a seconda dell'oggetto captato e, dunque, i risultati investigativi appresi seguono discipline diversificate con altrettanti regimi di utilizzabilità a seconda della qualifica assunta.

In particolare, nel caso in cui l'oggetto della videoripresa sia rappresentato da sole immagini (ovvero da comportamenti non comunicativi, quali, ad esempio, i movimenti dei soggetti in un ambiente), il dato probatorio acquisito soggiace alla disciplina di cui all'art. 189 c.p.p.; viceversa, allorquando vengano appresi anche contenuti comunicativi (ad esempio, due persona che dialogano tra loro a gesti), tale attività è inquadrabile nel genus delle intercettazioni ambientali, ex art. 266, comma 2 c.p.p. [77].

In questa prospettiva, le videoriprese effettuate in un luogo pubblico[78], sono legittime e pienamente utilizzabili anche in assenza di un decreto autorizzativo, purché le modalità di assunzione previste dall'art. 189 c.p.p. siano state oggetto di contraddittorio, sia pure posticipato.

Nei luoghi "riservati"[79], soggetti alla tutela della privacy ma non a quella offerta al domicilio, la videoripresa deve essere autorizzata con apposito decreto, desumendo tale necessità dall'art. 2 Cost.

Infine, nei luoghi domiciliari[80] gli elementi di prova acquisiti ex art. 189 c.p.p., sono inutilizzabili, in quanto basati su un'attività che la legge vieta.

La fragilità di una disciplina così congegnata – non fondata su basi normative stabili ma su interpretazioni giurisprudenziali e dottrinali peraltro ondivaghe – determina effetti perniciosi sui limiti stessi del divieto introdotto, finendo per legittimare tutte quelle attività investigative dai contorni più sfumati, al limite tra acquisizione di immagini aventi ad oggetto comportamenti comunicativi e non[81], anche in luoghi non perfettamente

CamminoDiritto.it
ISSN 2532-9871

inquadrabili nelle categorie sopra indicate. In questo senso, è stato osservato come «residuano "zone grigie", dove la prassi è incline ad aperture in chiave autoritaristica»[82]. Non solo. L'erosione dei confini del divieto, combinato all'itineranza ontologica del virus informatico, potrebbe determinare l'apprensione di una mole di dati che non sempre sono esclusi dagli esiti procedimentali. A ben guardare, infatti, non sono mancate decisioni della giurisprudenza di legittimità in cui si è affermata la piena utilizzabilità delle videoriprese di comportamenti materiali realizzate in àmbito domiciliare, allorquando tale captazione fosse avvenuta "incidentalmente", nel corso di un'attività di un'indagine volta, in base ad una valutazione ex ante, alla registrazione di comportamenti comunicativi e, dunque, autorizzata ai sensi dell'art. 266, comma 2 c.p.p. Nel caso di specie, il fermo immagine non capta un "flusso di comunicazioni" in transito. Esso acquisisce un "flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer, ossia una relazione operativa tra microprocessore e video del sistema elettronico. In altri termini, non sembra che il software sia adoperato per cogliere comunicazioni, quanto piuttosto per individuare ciò che viene digitato sul computer.

Non dissimilmente da una ripresa fotografica, lo screenshot acquisice dati che – in questo caso – non hanno carattere comunicativo, all'interno del domicilio informatico quale può essere comunemente definito il dispositivo elettronico infetto. Da ciò, seguendo l'insegnamento delle Sezioni unite "Prisco" del 2006, si ricava un sillogismo perfetto: se lo screenshot è una videoripresa investigativa e posto che esso non acquisisce comportamenti non comunicativo nel domicilio, il dato acquisito deve ritenersi inutilizzabile[83]. Ma, si sa, l'inutilizzabilità costituisce una risposta inadeguata alla violazione dei diritti fondamentali, i cui esiti non verrebbero così scongiurati.

8. Conclusioni: tentativi di tipizzazione e nuove patologie

Dopo aver ripercorso le tappe salienti della tormentata e convulsa legislazione in materia di intercettazioni tramite captatore informatico ed evidenziate le falle esistenti in rapporto alle funzioni atipiche esperibili mediante ricorso alle tecniche di remote forensics, possono trarsi alcune considerazioni che provano a spingersi fino ad avanzare possibili soluzioni giuridiche.

Allo stato dell'arte, il nobile tentativo di legalizzare l'ingresso del captatore informatico nelle indagini penali si scontra con l'irresolutezza del prodotto legislativo che non spicca per completezza e coerenza normativa. Sono tante le lacune e altrettanti i difetti metodologici; molteplici sono, poi, le incongruenze nella trasposizione, sul piano normativo, dei principi messi in luci dal delegante già nel 2017.

Nel complesso può dirsi che si tratta di una riforma che, tradendo gli originari intenti,

CamminoDiritto.it
ISSN 2532-9871

finisce per scontentare tutti gli interpreti del diritto, non essendo riuscita a coniugare le esigenze di sicurezza sociale con le istanze difensive.

Diverse ragioni fanno propendere l'interprete per una simile conclusione, compendiate in un'espressione che, forse, più di tutte può dettare la misura dell'insoddisfazione: la normativa così congegnata rappresenta uno dei più grandi ossimori ordinamentali offerti nell'ultimo tempo, dal momento che al caos generato degli spasmodici interventi riformatori non corrisponde la completezza della disciplina offerta. Nel marasma che di recente ha colpito la disciplina delle intercettazioni, infatti, si avverte come persa l'occasione per una ridefinizione costituzionalmente orientata delle altre attività (diverse dall'intercettazione di conversazioni e comunicazioni tra presenti) che il malware, almeno in potenza, è in grado di svolgere. E, come acutamente osservato, «[S]orge [...] il dubbio che l'indeterminatezza del presupposto sia tale da alimentare pratiche investigative idonee a scalfire anche il nucleo più intimo e inviolabile del diritto alla riservatezza»[84].

Probabilmente il legislatore nazionale preferisce tacere più che normare, lasciare agli interpreti del diritto l'arduo compito di definire i limiti e la portata dell'istituto piuttosto che fornire criteri e parametri di legalità per indirizzare le scelte dei pratici, consapevole che le ingerenze ai diritti fondamentali non hanno alcuna ripercussione in sede procedimentale in ragione dell'inutilizzabilità dei dati raccolti ultra vis, disattendendo, così, i dettami della giurisprudenza europea la quale, per contro, ritiene che «[O]gni intromissione riveste di per sé la caratteristica di ingerenza della pubblica autorità nella sfera privata e ciò anche quando di essa non si sia fatto un uso processualmente rilevante» [85].

In un contesto come questo, ricorrere alla pars construens, senza rimanere soffocati dalla pars destruens, non è cosa agevole; così come non è cosa agevole avanzare proposte de jure condendo e intravedere soluzioni adeguate a contemperare le esigenze di sicurezza, tutela delle prerogative individuali e rispetto delle regole su cui si fonda il processo penale, perché si rischia di scivolare in una realtà astratta e poco concreta.

Ma il giurista non può rimanere inerte, dovendo «scendere nell'arena»[86] dove il diritto processuale penale deve fare i conti con le resistenze culturali di un sistema che ricerca soluzioni più nette, polarizzatesi intorno a due estremi: negare completamente cittadinanza, nel circuito investigativo, al captatore informatico e, più in generale, ai nuovi ritrovati della tecnologia in nome della tutela delle garanzie inviolabili inevitabilmente compresse dall'uso di strumenti così tanto incidenti per le prerogative individuali; ovvero accogliere, senza riserve, l'impiego del virus quale strumento di esecuzione delle categorie probatorie tradizionali, intravedendo nella sicurezza collettiva l'unico valore per cui vale la pena comprimere i diritti e i valori costituzionalmente protetti.

CamminoDiritto.it
ISSN 2532-9871

A questo punto, ci si chiede se il sistema costituito possa offrire spazi per una diversa ricostruzione della disciplina, capace di tutelare, ad un tempo, i principi del giusto processo e le esigenze di sicurezza individuale e collettiva.

Probabilmente, come spesso accade, la strada maestra potrebbe essere quella intermedia, di equilibrio tra le due soluzioni antitetiche.

In questo senso, la dichiarazione di illegittimità per incostituzionalità delle attività di online surveillance condotte dal captatore informatico – con conseguente inutilizzabilità dei risultati acquisiti – non può (e non deve) rappresentare una conclusione ma un punto di partenza. L'obiettivo non è negare cittadinanza a tale strumento ma stabilire a quali condizioni possa considerarsi legittimo, tenuto conto dell'importanza che lo stesso va acquisendo ai fini delle indagini e della crescente attenzione che a livello europeo e internazionale viene dedicata al tema.

In altre parole, non potendo a priori considerarsi incostituzionale ogni strumento tecnico attraverso cui realizzare le indagini moderne, occorre che questo sistema venga minuziosamente regolamentato, tenendo conto del bilanciamento tra i vari interessi che possono venire in contrasto.

Inevitabile appare l'intervento normativo del legislatore, chiamato a tipizzare il complesso di attività esperibili attraverso l'impiego di strumenti di investigazione digitale ad alto contenuto tecnologico in forma chiara e compiuta, di modo tale da rendere le limitazioni alle prerogative individuali "tollerabili" secondo i parametri propri di una società democratica.

Sono sempre attuali le considerazioni del teorizzatore del positivismo giuridico, per cui « [Q]uanto maggiore sarà il numero di quelli che intenderanno e avranno fra le mani il sacro codice delle leggi, tanto men frequenti saranno i delitti, perché non v'ha dubbio che l'ignoranza e l'incertezza delle pene aiutino l'eloquenza delle passioni»[87].

Nonostante la normativizzazione delle tecniche di investigazioni digitale rappresenti un baluardo ineludibile contro gli arbìtri del giudicante, anche le modalità di intervento legislativo non risultano di immediata soluzione.

Prima facie, si potrebbe prospettare una soluzione "radicale", un intervento riformatore che consenta di innovare completamente la disciplina de qua attraverso la normazione di tutte le singole attività esperibili dall'agente intrusore. Così, da un lato, in ragione della legittimazione giurisprudenziale all'esecuzione di intercettazioni telematiche mediante

CamminoDiritto.it
ISSN 2532-9871

virus informatico[88], si potrebbe prospettare un "correttivo" al dettato di cui all'art. 266 bis c.p.p., rimasto immune alla smania riformatrice dell'ultimo tempo, in modo da tipizzare l'uso del Trojan quale nuova tecnica di esecuzione delle captazioni di flussi di comunicazioni relativi a sistemi informatici o telematici.

Per altro verso, a fronte delle molteplici funzionalità del captatore informatico, si potrebbe prevedere un intervento legislativo additivo delle norme disciplinanti i singoli mezzi di ricerca della prova, atto a tipizzare le svariate attività di indagine derivanti dall'impiego del malware e che risultano diverse e/o aggiuntive rispetto alla "mera" intercettazione di conversazioni e comunicazioni tra presenti[89].

Non vanno, tuttavia, sottaciuti i rischi che possono derivare da un simile approccio "attivista", fondato, cioè, sulla convinzione per cui la positivizzazione dell'istituto rappresenti la soluzione ai mali del sistema.

Come sempre accade quando il processo penale si confronta con i nuovi ritrovati della scienza e della tecnica, il pericolo è di intervenire su una materia già diventata obsoleta, perché – si sa – i tempi delle riforme non coincidono con la velocità propria del progresso e dell'evoluzione tecnologica, condannando la legge ad una obsolescenza precoce.

Così, probabilmente, si potrebbe preferire una soluzione meno rigorosa ma assolutamente efficace in punto di "certezza del diritto". Si potrebbe pensare alla predisposizione di una norma "aperta", sulla falsariga del dictum di cui all'art. 189 c.p.p., che, subordinando gli strumenti di ricerca della prova a condizioni tassative, consente di vincolare l'ingresso di nuove e sempre più evolute tecniche di indagine e di investigazione al rispetto delle garanzie fondamentali costituzionalmente riconosciute, in modo tale da ripristinare un sistema informato al principio di legalità della prova.

Seguendo una simile impostazione, «il legislatore non dovrebbe soffermarsi sulla disciplina dei singoli strumenti informatici – sempre potenzialmente in evoluzione e dunque suscettibili di creare un vuoto di tutela in caso di mancato tempestivo intervento legislativo – ma dovrebbe piuttosto identificare le garanzie fondamentali che devono essere sempre tutelate indifferentemente dallo strumento impiegato»[90].

In realtà, questa soluzione non appare del tutto soddisfacente. Da una parte, non si può negare la circostanza per cui al variare delle tecniche intrusive varia inevitabilmente anche il complesso di garanzie nelle quali si possono iscrivere i nuovi ritrovati della tecnologia, con ciò determinando l'insorgere di nuove criticità poste proprio dai progressi tecnici. Dall'altro, se è vero che l'esperimento delle attività di perquisizione occulta da remoto – mai disciplinata da alcuna norma giuridica – determina un vulnus ai principi fondanti

CamminoDiritto.it
ISSN 2532-9871

l'assetto costituito, in questi casi il rischio da scongiurare è consentire alla prassi giurisprudenziale di ricorrere all'atipicità per giustificare e legittimare il compimento di attività che, per converso, risultano ai limiti della costituzionalità.

Al fine di arginare simili pericula, si potrebbe propendere per l'introduzione di un nuovo mezzo di ricerca della prova ("intrusione informatica", potrebbe definirsi) per regolare le attività di accesso, osservazione e acquisizione di dati e informazioni da remoto, esperibile mediante l'impiego di sempre più sofisticate tecniche di indagine.

In questi casi, non sarebbe tipizzato lo strumento con cui condurre le indagini informatiche quanto piuttosto le regole cui ricorrere ogni qual volta si proceda ad attività di sorveglianza occulta e continuativa da remoto, predisponendo le garanzie fondamentali che devono essere sempre riconosciute all'indagato e ai soggetti terzi occasionalmente coinvolti, a prescindere dalla tecnica investigativa impiegata.

In altre parole, l'obiettivo potrebbe essere quello di introdurre una nuova categoria probatoria, con la quale verrebbero individuati i "casi" e i "modi" dell'ingerenza nella sfera privata degli individui, così da ritenere il sacrificio dei diritti inviolabili assolutamente rispettoso del principio di stretta legalità e del principio di proporzione.

Con ciò non si intende "imbrigliare" in un eccessivo formalismo giuridico le attività di polizia ma solo rendere conforme ai principi propri di uno Stato di diritto un sistema che, ad oggi, è ancora orfano di regole[91].

La previsione di un intervento legislativo in materia non rappresenta, tuttavia, l'unico rimedio alla capacità intrusiva del malware. Alle carenze normative, infatti, si aggiungono anche le disfunzioni di ordine pratico derivanti dall'uso di strumenti di indagine dalla portata dirompente e che, si pronostica, non possono che acuirsi in ragione dell'avanzamento della tecnologia.

Proprio in ragione del carattere ubiquitario e totalizzante che caratterizza le nuove tecniche di indagine, al di là della formalistica sanzione comminata alle acquisizioni ultra moenia (art. 270, comma 1 bis c.p.p.) e ultra vis (art. 271, comma 1 bis c.p.p.) già predisposta dal legislatore con riferimento al captatore informatico, occorre soffermarsi sui rivolti prasseologici che l'atto inutilizzabile produce sul procedimento, a partire dalle indagini preliminari fino a condizionare la decisione giudiziale.

Nonostante l'intento encomiabile del legislatore – che rimodula la portata delle patologie, sia con riguardo all'inutilizzabilità delle informazioni apprese tramite un'intercettazione

CamminoDiritto.it
ISSN 2532-9871

illegittima (art. 271 c.p.p.), che in rapporto al divieto di trasmigrazione del captato (art. 270 c.p.p.) – sembra indispensabile tratteggiare i futuribili risultati della nuova normativa, interrogandosi sugli effetti che l'atto illegittimo produce sulla prova ulteriore di cui ha favorito l'acquisizione.

Senza entrare nel merito del complesso dibattito relativo alla "portata" della c.d. "teoria dei frutti dell'albero avvelenato"[92], occorre circoscrivere – seppur brevemente – il convulso contesto giurisprudenziale e dottrinale in cui si insinua la questione.

Sul punto, si delineano due orientamenti contrastanti: nonostante una parte minoritaria della giurisprudenza e della dottrina ammetta il propagarsi dell'invalidità in questione[93], sostenendo la tesi della c.d. inutilizzabilità derivata[94], le tendenze maggioritarie spingono sul versante opposto. Infatti, nel rispetto degli insegnamenti della Consulta[95], si ammette che per la prova inutilizzabile non possa operare il principio dell'estensione del vizio agli atti consecutivi e dipendenti[96], posto che il legame tra la prova inutilizzabile e quella successiva sarebbe meramente psicologico e non giuridico e il vizio colpisce i risultati dell'atto e non l'atto in sé[97].

Lo stesso principio – si è detto – trova applicazione nel caso delle intercettazioni mediante Trojan, per cui sarebbe impensabile una «propagazione illimitata del vizio dell'inutilizzabilità»[98].

Seguendo una simile impostazione, considerato che l'inutilizzabilità colpisce l'idoneità della prova a produrre risultati conoscitivi valutabili dal giudice per la formazione del suo libero convincimento, i risultati inutilizzabili a fini probatori non perderanno valore a fini investigativi[99], potendo comunque essere utilizzati dagli inquirenti come "spunti" per l'avvio di ulteriori indagini.

Da tale assunto dipendono scenari assai inquietanti circa la possibilità di aggirare il divieto consentendo un ingresso "forzato" delle informazioni non utilizzabili, come dati "per" la formazione della notitia criminis, oppure per motivare il ricorso ad altri atti investigativi considerati legittimi anche se causalmente originati da intercettazioni ex se inutilizzabili[100]. Ad esempio, rischia di essere ammesso il ricorso a detto materiale per autorizzare ulteriori intercettazioni o per disporre una perquisizione.

Di qui, sulla base delle informazioni acquisite, la polizia giudiziaria potrà compiere tutti quegli atti "atipici" di indagine per i quali non è prevista una «possibile partecipazione del difensore al compimento dell'atto»[101] ed il pubblico ministero potrà fare ricorso agli «strumenti più appropriati, modellati sulla struttura degli atti di indagine che vengono compiuti durante le attività amministrative o procedimentali»[102].

CamminoDiritto.it
ISSN 2532-9871

La questione diventa ancor più preoccupante nel caso di investigazioni atipiche esperite tramite Trojan.

In effetti, a ben riflettere, il divieto di utilizzo dei risultati inerisce solo al contenuto delle conversazioni e delle comunicazioni apprese mediante il virus, non estendendosi al ben più ampio novero di operazioni che possono essere esperite tramite il captatore che, si ribadisce, non trovano alcuna regolamentazione nell'articolato legislativo.

Di conseguenza, i divieti posti dal legislatore contemporaneo sono come sterilizzati al di fuori della disciplina delle intercettazioni, dal momento che i dati appresi con tecniche non riconducibili, neppure lato sensu, alla captazione rischiano di avere ingresso nel processo penale attraverso i "tradizionali" canali di acquisizione delle prove atipiche.

Sulla base di simili premesse, sembra doveroso proporre un ripensamento, almeno in materia di inutilizzabilità delle conversazioni carpite mediante virus, dell'opzione tradizionale secondo cui le uniche conseguenze della fattispecie dovrebbero prodursi esclusivamente in àmbito probatorio. Tale impostazione poteva forse essere sostenuta in un mondo in cui la pervasività della raccolta era già capillare, ma non ancora totalizzante: nel caso delle intercettazioni telefoniche non era possibile carpire conversazioni al di fuori della chiamata, eccezion fatta per i marginali casi delle captazioni "a cornetta sollevata"; in quello delle intercettazioni ambientali, il ricorso alle "tradizionali" microspie esauriva la loro portata operativa al solo ambiente di collocazione. Ancora più problematico, invece, accettare il medesimo ragionamento quando le comunicazioni (ma non solo) possono essere incamerate grazie a dispositivi informatici da cui ormai ogni cittadino è accompagnato in ogni momento della vita quotidiana, pronti a divenire sentinelle al servizio dell'autorità giudiziaria; in questo senso, peraltro, il Trojan è solo il più conosciuto tra numerosi strumenti che consentono una raccolta indiscriminata e illimitata di informazioni[103].

D'altra parte, le recenti pronunce della Consulta lasciano aperti alcuni spiragli per prevedere regimi differenziati di invalidità in rapporto alla tipologia di atti investigativi[104] ; il che significa che «ad un "massimo" di illegalità dell'atto probatorio, perché compiuto in violazione di divieti di elevato spessore deve corrispondere dunque una equivalente "estensione" dell'area di inutilizzabilità processuale»[105].

In tale contesto, a tutela dei fondamentali diritti della persona, è opportuno chiedersi se sia necessario far cadere alcuni tabù[106]. Nel tema che qui occupa, là dove riconducibili alla categoria dell'inutilizzabilità, potrebbe essere opportuno precludere qualsiasi impiego dei risultati delle intercettazioni eseguite mediante captatore informatico: le conseguenze

CamminoDiritto.it
ISSN 2532-9871

derivanti dal divieto di utilizzo non dovrebbero, quindi, essere scontate dalla sola prova ma dall'intero novero di attività procedimentali che da quegli elementi possa trarre beneficio.

Da ultimo, sembra doveroso confrontarsi con un dato – a nostro avviso inconfutabile – derivante dall'imprinting che l'inesauribile compendio probatorio (ottenuto proprio mediante il ricorso a strumenti investigativi itineranti) ha sulle logiche decisionali dell'autorità giudiziaria.

Seppur non utilizzabili formalmente ai fini dell'emanazione della sentenza, la mole di informazioni risultanti dalle investigazioni tramite captatore informatico inevitabilmente plasmano, forgiano e modellano il giudicante e il suo convincimento che da "libero" diventa "prigioniero" di bias cognitivi derivanti dagli effetti che il materiale spurio raccolto ha sulla mente dell'organo giudiziario.

Di qui, si ritiene necessario non solo ridefinire i ruoli tra i diversi protagonisti delle indagini preliminari, ma anche propendere per l'istituzione di specifici organi con competenze riservate alla sola fase di selezione del materiale probatorio rilevante ai fini processuali, funzionale a garantire la legittimità della procedura esecutiva e, al contempo, evitare ingressi "indiretti" del materiale probatorio acquisito contra legem.

In questi casi, si potrebbe paventare la possibilità di attribuire ad un giudice diverso il compito di procedere alla selezione del materiale "rilevante" ai fini investigativi, depurandolo dagli orpelli di cui si arricchisce grazie alla forza intrusiva ubiquitaria e continuativa del malware.

Si supererebbero in tal modo le criticità di natura più strettamente operativa, determinate dai possibili condizionamenti investigativi di un organo che, dismessi i panni di "controllore" della regolarità dell'attività investigativa, una volta iniziato il processo penale dirige le indagini "tradizionali" con un background di informazioni che ne condizionano le scelte investigative e, quindi, gli esiti processuali.

Nonostante gli sforzi profusi per tentare di fornire adeguati rimedi ai problemi posti dall'impiego del captatore informatico nel processo penale, l'indagine non consente di addivenire ad una soluzione condivisa.

Rispettando i crismi propri di qualsivoglia ricerca, l'analisi lascia ancora imbattute e inesplorate diverse rotte. L'irrefrenabile velocità con cui gli strumenti investigativi si evolvono apre, infatti, la strada all'impiego di ulteriori tecniche di indagini (intelligenza

CamminoDiritto.it
ISSN 2532-9871

artificiale, droni, robot) che, spingendosi assai oltre i confini legislativi previsti in relazione all'uso del captatore informatico, sono destinati a comprimere – inevitabilmente – fondamentali diritti degli individui, nel frattempo privati di adeguate forme di tutela nell'assenza di una normativa che li contempli. Ecco allora, che le riflessioni condotte – che sembravano poter rappresentare il punto di arrivo nella materia delle investigazioni tramite Trojan – non possono che essere il nuovo punto di partenza per un sistema processuale penale "informatizzato" ancora allo stato embrionale.

CamminoDiritto.it
ISSN 2532-9871

Note e riferimenti bibliografici

[1] Il Tribunale del riesame aveva qualificato tale attività quale intercettazione di atti comunicativi, dal momento che il file era stato fotografato nel corso della sua stessa formazione.

[2] Sulle funzionalità del virus in rapporto alle potenzialità investigative, ex multis, M. TORRE, Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali, Milano, 2017, 12 s. Si consenta, inoltre, il rinvio a W. NOCERINO, Il captatore informatico nelle indagini penali interne e transfrontaliere, Padova, 2021.

[3] In questo senso D. CURTOTTI- W. NOCERINO, Le intercettazioni tra presenti con captatore informatico, in AA. VV., Le recenti riforme in materia penale, a cura di G.M. Baccari-C. Bonzano-K. La Regina- E.M. Mancuso, Milano, 2017, 560.

[4] Così C. CONTI-M. TORRE, Spionaggio digitale nell'àmbito dei social network, in AA. VV., Le indagini atipiche, II ed., Torino, 2019, 562.

[5] Sul punto, per tutti, S. ATERNO, La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screen shot, in Dir. pen. proc., 2018, f. 8, 1065 ss.

[6] Cfr. § 5.

[7] Come meglio si dirà (cfr. § 4), l'intercettazione ambientale rappresenta l'unica attività normata dal legislatore contemporaneo. Come precisa M. BONTEMPELLI, Il captatore informatico in attesa della riforma, in Dir. pen. cont., 20 dicembre 2018, 3, «[A]ppare riduttivo, ma scontato, l'inquadramento del captatore informatico come strumento tecnico dell'intercettazione».

[8] In argomento R. ORLANDI, Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici, in Arch. pen., 25 luglio 2016.

[9] In questo senso L. FILIPPI, L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico), in Arch. pen., 2016, f. 2, 349 s. Si consenta, inoltre, il rinvio a W. NOCERINO, Il captatore informatico: un giano bifronte. Prassi operative vs risvolti giuridici, in Cass. pen., 2020, f. 2, 826.

[10] F. GIUNCHEDI, Captazioni "anomale" di comunicazioni: prova incostituzionale o mera attività di indagine?, in Proc. pen. giust, 2014, f. 5, 134.

[11] Sul punto, esaustivamente, L. PARLATO, voce Perquisizioni on-line, in Enc. dir., Annali, vol. X, Milano, 2017, 603 ss. Ma già S. MARCOLINI, Le cosiddette perquisizioni on line (o perquisizioni elettroniche), in Cass. pen., 2010, f. 7-8, 2855 ss.; M. TROGU, Sorveglianza e "perquisizioni" on-line su materiale informatico, in AA. VV., Le indagini atipiche, Torino, 2014, I ed., 431.

[12] L'espressione appartiene a S. SIGNORATO, Le indagini digitali. Profili strutturali di una metamorfosi investigativa, Torino, 2018, 292,

[13] Così P. TONINI-C. CONTI, Il diritto delle prove penali, Milano, 2014, 482.

[14] Ex multis P. FELICIONI, Le fattispecie "atipiche" e l'impiego processuale, in AA. VV., L'intercettazione di comunicazioni, a cura di T. Bene, Bari, 2018, 315 ss.; EAD., L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma, in Proc. pen. giust., 2016, f. 5, 118.

[15] Cass., sez. un., 28 aprile 2016, n. 26889, in Arch. pen., 2016, f. 2, 348 ss. Diversi sono i commenti alla pronuncia in esame. Tra i tanti, si vedano, T. ALESCI, L'intercettazione di comunicazioni o di conversazioni tra presenti con il Trojan horse è ammissibile anche nei luoghi di privata dimora per i reati di criminalità organizzata, in Proc. pen. giust., 2016, f. 5, 28 ss.; A. CAMON, Cavalli di Troia in Cassazione, in Arch. nuova proc. pen., 2017, f. 1, 91; W. NOCERINO, Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel

CamminoDiritto.it
ISSN 2532-9871

processo penale, in Cass. pen., 2016, f. 12, 3589.

[16] S. ATERNO, voce Digital forensics (investigazioni informatiche), in Dig. disc. pen., Agg., vol. III, Torino, 2014, 217; F. CAPRIOLI, Il "captatore informatico" come strumento di ricerca della prova in Italia, in Rev. Bras. de Direito Processual Penal, 2017, f. 2, 483 ss.; D. CURTOTTI, Il captatore informatico nella legislazione italiana, in Jusonline, 2017, f. 3, 385; S. SIGNORATO, Le indagini digitali, cit., p. 239; A. TESTAGUZZA, I sistemi di controllo da remoto: tra normativa e prassi, in Dir. pen. proc., 2014, f. 6, 759 ss.; M. TORRE, Il captatore informatico, cit., 18.

[17] Cfr. J. BENTHAM, An Introduction to the Principles of Morals and Legislation, in AA. VV., The Collected Works of Jeremy Bentham, a cura di J. H. Burns - H. L. A. Hart Athlone Press, 1970.

[18] Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[19] Volendo W. NOCERINO, Il captatore informatico: un giano bifronte. Prassi operative vs risvolti giuridici, cit., 828.

[20] Così C. PELOSO, La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo, in Dir. pen. cont., 2017, f. 1, 150.

[21] Sul tema, ex multis, A. CAPONE, Intercettazioni e costituzione. Problemi vecchi e nuovi, in Cass. pen., 2017, f. 3, 1263 ss.; M. GRIFFO, Una proposta costituzionalmente orientata per arginare lo strapotere del captatore, cit., 43; O. MAZZA, Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni, in Proc. pen. giust., 2018, f. 4, 684 ss.; S. SIGNORATO, Le indagini digitali, cit., 69; G. SPANGHER, Le criticità della disciplina delle intercettazioni telefoniche, in Dir. pen. proc., 2016, f. 3, 921 ss.

[22] Prima delle Sezioni Unite "Scurato" (Cass., sez. un., 28 aprile 2016, n. 26889, cit.), cfr. Cass., sez. VI, 10 marzo 2016, n. 13884, in Dir. inf. e informatica, 2016, f. 1, 81; Id., sez. VI, 26 maggio 2015, n. 27100, in Guida dir., 2015, f. 41, 83 s.; Id., sez. VI, 8 aprile 2015, n. 27536, inedita; Id., sez. VI, 12 marzo 2015, n. 24237, inedita. Ma già Cass., sez. VI, 27 novembre 2012, n. 15009, in C.E.D. Cass., n. 254865; Id., sez. V, 14 ottobre 2009, n. 16556, ivi, n. 246954. Poi, dopo la pronuncia, nelle more dell'entrata in vigore della riforma, Id., sez. I, 25 giugno 2019, n. 50972, in Sist. pen., 20 ottobre 2020; Id., sez. V, 30 settembre 2020, n. 31604, in Giur. pen., 11 novembre 2020; Id., Sez. V, 30 settembre 2020, n. 35010, in C.E.D. Cass., n. 280398; Id., sez. V, 28 settembre 2020, n. 31849, ivi, n. 279769; Id., sez. V, 28 settembre 2020, n. 33138, ivi, n. 279841; Id., sez. VI, 13 giugno 2017, n. 36874, in Dir. pen. cont., 27 settembre 2017.

[23] L'espressione appartiene a M. GIALUZ, L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare, in Sist. pen., 1 maggio 2020. Come precisato da L. FILIPPI, Intercettazioni: habemus legem!, in Dir. pen. proc., 2020, f. 4, 453, «[L]a lunga gestazione della riforma [...] si è poi conclusa, tra le doglie, con un aborto spontaneo». Secondo F. RUGGIERI, La nuova disciplina delle intercettazioni: alla ricerca di una lettura sistematica, in Proc. pen. giust., 2020, f. 4, 933, «[S]e a questa circostanza si aggiunge che anche la recente legge 28 febbraio 2020 n. 7 di conversione del d.l. 30 dicembre 2019 n. 161 ha a sua volta novellato e modificato l'articolato del codice di rito relativo a tale mezzo di ricerca della prova contenuto nel provvedimento d'urgenza, prima facie non sembra possibile offrire una visione sistematica e soprattutto coerente dell'istituto».

[24] Cfr. d.lgs. 29 dicembre 2017, n. 216, recante "Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103", in Gazz. uff., 11 gennaio 2018, n. 8.

[25] L. 23 giugno 2017, n. 103, recante "Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario", in Gazz. uff., 4 luglio 2017, n. 154.

[26] Ex art. 1, comma 1139, lett. a della l. 30 dicembre 2018, n. 145, recante "Bilancio di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021", in Gazz. uff., 31 dicembre 2018, n. 302.

[27] Secondo il disposto dell'art. 9, comma 2, d.l. 14 giugno 2019, n. 53, recante "Disposizioni urgenti in materia di ordine e sicurezza pubblica", convertito, con modificazioni, dalla l. 8 agosto 2019, n. 77, in Gazz. uff., 9 agosto 2019, n. 186.

[28] D.l. 30 dicembre 2019, n. 161, recante "Disposizioni urgenti in materia di intercettazioni", in Gazz. uff., 31

CamminoDiritto.it
ISSN 2532-9871

dicembre 2019, n. 305, convertito, con modificazioni, dalla l. 28 febbraio 2020, n. 7, in Gazz. uff., 28 febbraio 2020, n. 50.

[29] La divergenza di vedute tra l'ex Ministro della Giustizia del Partito Democratico, Andrea Orlando, e il suo successore del Movimento Cinque Stelle, Alfonso Bonafede, era nota ai più: tra il mese di giugno e luglio 2018, subito dopo il varo del primo Governo di Giuseppe Conte, il Ministro aveva già espresso pubblicamente l'intento di avviare una "riforma della riforma" in tempi brevi quale correttivo al contuso sistema giudiziario. Infatti, il 22 giugno 2018, intervenendo a un convegno organizzato dal Consiglio Superiore della Magistratura, il Ministro della Giustizia Alfonso Bonafede aveva dichiarato: «il mio impegno prioritario è capire le linee della riscrittura del provvedimento e su questo avvierò un confronto già la prossima settimana con procure e avvocati». Sui contenuti delle dichiarazioni, v. F. CACCIA, Bonafede all'Anm: intercettazioni, bloccherò la riforma, in Corriere della Sera, 23 giugno 2018, 11.

[30] M. GIALUZ, L'emergenza nell'emergenza, cit., 3.

[31] Sul punto G. SPANGHER, La riforma sconta due mesi di proroga, in vigore dal 1° maggio, in Guida dir., 2020, f. 13, 34.

[32] Con queste motivazioni era stato giustificato lo slittamento dell'entrata in vigore alla fine di febbraio: v. Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019, reperibile al sito www.senato.it., p. 7. Assai interessanti al riguardo appaiono le riflessioni di G. AMATO, Un differimento per ragioni tecniche e organizzative, in Guida dir., 2020, f. 6, 65.

[33] D.l. 30 aprile 2020, n. 28, recante "Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19", in Gazz. uff., 30 aprile 2020, n. 111, convertito, con modificazioni, dalla l. 25 giugno 2020, n. 70, ivi, 29 giugno 2020, n. 162. Per una panoramica delle questioni legate ai tempi di adattamento ed esecuzione dei dicta normativi, per tutti, E. MARZADURI, L'applicazione delle disposizioni nel tempo, in Legislaz. pen. (Speciale sulle nuove intercettazioni), 24 novembre 2020, 156 ss.

[34] L'innesto è avvenuto ad opera dell'art. 4, comma 1, lett. a, punto 2 d.lgs. 216/2017.

[35] Art. 1, comma 4, lett. a, l. 3/2019. Più precisamente, il comma 3 della medesima novella abroga il secondo comma dell'art. 6, d.lgs. 216/2017, il quale stabiliva che «[L']intercettazione di comunicazioni tra presenti nei luoghi indicati dall'art. 614 del codice penale non può essere eseguita mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile quando non vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

[36] Art. 2, comma 1, lett. f, punto 1, d.l. 161/2019.

[37] Si ricordi che l'estensione dell'area operativa del captatore informatico, infatti, era stata delimitata da queste norme con riferimento ai «procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni».

[38] Si tratta dei reati compresi negli artt. 314 e 335 bis c.p., i quali, peraltro, sono delitti che possono essere commessi sia da pubblici ufficiali, sia da incaricati di pubblico servizio, con esclusione di alcune fattispecie penali, come, ad esempio, la turbata libertà degli incanti (art. 353 c.p.) e la turbata libertà del procedimento di scelta del contraente (art. 353 bis c.p.).

[39] Relazione dell'Ufficio del Massimario della Corte di Cassazione sulla legge 28 febbraio 2020, n. 7, conversione in legge con modificazioni del decreto legge 30 dicembre 2019, n. 161, Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni, n. 35, 23 marzo 2020, 8.

[40] Si tratta, più precisamente, dei procedimenti facenti capo ad un'associazione per delinquere, ex art. 416 c.p., correlate alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato, per cui si applicano le disposizioni di cui all'art. 13, d.l. n. 152/91 in forza di quanto indicato da Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[41] Sul punto M. GRIFFO, Rilievi sull'impiego del trojan nei procedimenti per i reati contro la pubblica amministrazione, in Proc. pen. giust., 2020, f. 2, 482 ss.

CamminoDiritto.it
ISSN 2532-9871

[42] Cfr. art. 1, comma 1, l. 7/2020, che modifica l'art. 2, comma 1, lett. c, d.l. 161/2019.

[43] Relazione dell'Ufficio del Massimario della Corte di Cassazione, cit., 10.

[44] Così D. PRETTI, La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019, in Sist. pen., 2 marzo 2020, 8.

[45] Secondo l'art. 2, comma 2, lett. a, d.l. 161/2019, le comunicazioni intercettate dovevano essere trasferite esclusivamente nell'archivio digitale di cui all'art. 269, comma 1 c.p.p.; disposizione, poi, modificata in sede di conversione.

[46] Art. 2, comma 2, lett. a, {https/URL}

[47] Invero, l'utilizzabilità dei risultati delle intercettazioni in procedimenti diversi è un tema "caldo" nel panorama giuridico dottrinale e giurisprudenziale. Di recente, la S.C., nella sua composizione più autorevole, interviene per chiarire la portata del dettato di cui all'art. 270, comma 1 c.p.p. In quell'occasione, la Corte chiarisce che il divieto in esame non opera, oltre che nel caso di reati successivamente emersi che siano ricompresi tra quelli per cui è previsto l'arresto obbligatorio in flagranza, anche con riferimento ai risultati relativi ai reati che sono connessi ex art. 12 c.p.p., sempre che rientrino nei limiti di ammissibilità previsti dalla legge. Cass., sez. un., 28 novembre 2019, n. 51, in Sist. pen., 30 gennaio 2020, con commento di G. ILLUMINATI, Utilizzazione delle intercettazioni in procedimenti diversi: le sezioni unite ristabiliscono la legalità costituzionale.

[48] L. 7/2020, che modifica l'art. 2, comma 1, lett. g, d.l. 161/2019, attraverso l'interpolazione di un nuovo punto "01".

[49] Cass., sez. un., 28 novembre 2019, n. 51, cit.

[50] In questo senso D. PRETTI, La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019, cit., 10.

[51] Cfr. il parere della Commissione permanente Affari Costituzionali del Senato della Repubblica del 19 febbraio 2020 relativamente all'emendamento n. 2.219. In questo senso anche Relazione dell'Ufficio del Massimario della Corte di Cassazione, cit., 13.

[52] Per dovere di completezza, si precisa che in sede di conversione del d.l. 161/2019, viene introdotto una nuova fattispecie nel catalogo dei reati intercettabili ex art. 266, comma 1 c.p.p., rappresentata dai «delitti commessi avvalendosi delle condizioni previste dall'art. 416 bis c.p. ovvero al fine di agevolare l'attività delle associazioni previste nello stesso articolo» (art. 266, comma 1, lett. f quinquies, c.p.p.).

[53] Ex art. 270, comma 1 c.p.p.

[54] Cfr. art. 2, comma 1, lett. g, punto 1, d.l. 161/2019.

[55] L. 7/2020, che modifica l'art. 2, comma 1, lett. g, d.l. 161/2019.

[56] Cass., sez. un., 28 novembre 2019, n. 51, cit.

[57] Per cui, è bene precisarlo nuovamente, non opera il divieto di cui all'art. 270, comma 1, c.p.p., non trattandosi di "reati diversi". Cfr. Cass., sez. un., 28 novembre 2019, n. 51, cit.

[58] Per i profili di criticità derivanti dalla possibilità di impiego "indiretto" delle informazioni, più in generale, A. CAMON, Le intercettazioni telefoniche nel processo penale, Milano, 1996, p. 44. Più di recente e con riferimento alla normativa modificata nel 2017, P. BRONZO, Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori, in AA. VV., Nuove norme in tema di intercettazioni Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche, a cura di G. Giostra-R. Orlandi, Torino, 2018, 255 ss.

[59] Cfr. § 3.

[60] Lo definiscono in tal modo D. CURTOTTI- W. NOCERINO, Le intercettazioni tra presenti con captatore informatico, cit., 560.

CamminoDiritto.it
ISSN 2532-9871

[61] Parla di un'intercettazione atipica priva di una sua autonomia concettuale, S. LORUSSO, Digital evidence, cybercrime e giustizia penale 2.0, in Proc. pen. giust., 2019, f. 4, 823.

[62] In questo senso R. ORLANDI, Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma, in Riv. it. dir. proc. pen., 2018, f. 2, 538 ss.; S. SIGNORATO, Le indagini digitali, cit., p. 299 ss.; M. TROGU, Intrusioni segrete nel domicilio informatico, in AA. VV., Le indagini atipiche, a cura di A. Scalfati, 2019, II ed., 579.

[63] P. BRONZO, L'impiego del trojan horse informatico nelle indagini penali, in. Riv. it. sc. giur., 2017, f. 8, 347 s.; F. CAPRIOLI, Il "captatore informatico" come strumento di ricerca della prova in Italia, cit., 485 ss. Secondo tali Autori, anche nel caso del Trojan dovrebbe seguirsi l'impostazione di F. CORDERO, Tre studi sulle prove, Milano, 1963, 153, per cui «tutto ciò che non è vietato dalla legge è permesso». In questo modo, le altre attività sono utilizzabili nei limiti delle regole di cui all'art. 189 c.p.p.

[64] Si esprime così S. SIGNORATO, Le indagini digitali, cit., 301. Secondo R. ORLANDI, Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma, cit., 544 s., «[U]si diversi da quelli espressamente regolati dall'art. 266, comma 2 e comma 2 bis c.p.p. non sono ammessi, proprio perché limitano un diritto fondamentale di una persona [...], del quale è però doveroso affermare l'esistenza [...]».

[65] F. CAPRIOLI, Il "captatore informatico" come strumento di ricerca della prova in Italia, cit., 485 ss.

[66] Cass., sez. V, 21 novembre 2017, n. 1822, in Giur. it., 2018, f. 7, 1817 ss., con nota di M. MINAFRA, Sul giusto metodo acquisitivo della corrispondenza informatica "statica". (Prove e messaggi telematici remoti); Id., sez. IV, 28 giugno 2016, n. 40903, in C.E.D. Cass., n. 268228.

[67] Cass., sez. IV, 28 giugno 2016, n. 40903, cit. Sul punto, M. GRIFFO, Una proposta costituzionalmente orientata per arginare lo strapotere del captatore, in Dir. pen. cont., 2018, f. 2, 23.

[68] Si esprime così L. GIORDANO, Dopo le Sezioni Unite sul "captatore informatico" avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo, in Dir. pen. cont., 2017, f. 3,188.

[69] In questo senso M. GRIFFO, Una proposta costituzionalmente orientata per arginare lo strapotere del captatore, cit., 28 s.

[70] Cass., sez. V, 20 ottobre 2017, n. 48370, in Giur. it., 2017, f. 2, 2498 ss.

[71] Secondo S. ATERNO La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screen shot, cit., 1069, «[S]e con lo screen shot si riesce a captare una conversazione via chat o una comunicazione tra due soggetti in tempo reale ovvero in corso di svolgimento non si ravvedono differenze con una telecamera o una macchina fotografica che riprende il contenuto comunicativo (qualsiasi) di un soggetto che dialoga o che scrive con un altro soggetto situato anche fuori dal luogo in cui è ripreso». Di qui, sarebbe più logico sussumere tali attività nell'àmbito delle intercettazioni ambientali domiciliari condotte mediante il supporto di strumenti atipici.

[72] S. ATERNO La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screen shot, cit., 1069.

[73] Come sostenuto, tali attività potrebbero essere definite come ispezioni on-line. In questo senso, P. FELICIONI, L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma, in Proc. pen. giust., 2016, f. 5, 124.

[74] Cfr. C. CONTI-M. TORRE, Spionaggio digitale nell'àmbito dei social network, in AA. VV., Le indagini atipiche, II ed., cit., 562.

[75] Così S. RODOTÁ, Una scommessa impegnativa sul terreno dei nuovi diritti, Discorso del presidente del Garante per la protezione dei dati personali tenuto l'8 maggio 2001alla presentazione della Relazione per il 2001, 15 maggio 2002, in www.privacy.it

[76] C. CONTI-M. TORRE, Spionaggio digitale, cit., 564.

[77] Sulla distinzione tra comportamenti comunicativi e non, da ultimo, Cass., sez. III, 22 luglio 2020, n. 31515, in

CamminoDiritto.it
ISSN 2532-9871

C.E.D. Cass., n. 280039.

[78] La giurisprudenza ha ridefinito i termini dei "luoghi pubblici" e di quelli "aperti al pubblico". Cfr. Cass., sez. VI, 21 novembre 2017, n. 595, in C.E.D. Cass., n. 271763, secondo cui «l'area antistante un condominio, recintata ma priva di cancello, costituisce luogo aperto al pubblico, in quanto consente l'accesso ad una categoria indistinta di persone a non solo ai condomini». Così come sono considerati tali «la cella e gli ambienti penitenziari [...] non essendo nel "possesso" dei detenuti, ai quali non compete alcuno "ius excludendi alios"; tali ambienti, infatti, si trovano nella piena e completa disponibilità dell'amministrazione penitenziaria, che ne può fare uso in ogni momento per qualsiasi esigenza d'istituto». Nello stesso senso Id., sez. VI, 15 maggio 2018, n. 26028, in C.E.D. Cass., n.273417.

[79] Nei luoghi riservati manca la stabilità dello ius excudendi alios (esistendo il diritto solo se l soggetto è presente sul luogo) ma sussiste un'aspettativa di riservatezza maggiore rispetto ai luoghi pubblici». Cass., sez. un., 28 luglio 2006, n. 26795, cit. Nello stesso senso, Id., sez. V, 3 marzo 2009, n. 11522, in C.E.D. Cass., n. 244199.

[80] In base all'evoluzione giurisprudenziale, può dirsi che i luoghi "domiciliari" sono quei luoghi in cui il titolare possiede uno ius excludendi alios stabile, ovvero azionabile anche quando il soggetto non sia fisicamente presente. Cfr. Corte cost., 16 maggio 2008, n. 149, in Giur. cost., 2008, 1825. Tale profilo era già emerso nella giurisprudenza di legittimità. Come precisato, il carattere di "stabilità" del diritto risulta, ai fini della determinazione del concetto di domicilio, assolutamente necessario (Cass., sez. IV, 20 giugno 2018, n. 32245, in C.E.D. Cass., n. 273458). Rientrano, pertanto, nella nozione di domicilio solo i luoghi che assolvono in concreto alla finalità di proteggere la vita privata del loro possessore, durante lo svolgimento delle sue attività professionali, di svago, di alimentazione, di riposo. In questo senso, G. VARRASO, Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione, in AA. VV., Le nuove intercettazioni, a cura di O. Mazza, Torino, 2018, 139 s. La delicata quaestio sembra aver trovato una stabilità ermeneutica grazie al recente apporto delle Sezioni Unite che accoglie un'interpretazione maggiormente restrittiva alla nozione de qua. Cfr. Id., sez. un., 23 marzo 2017, n. 31345, in Dir. pen. cont., 2017, f. 7-8, 227 ss., con nota di S. BERARDI, Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624 bis c.p., secondo cui «rientrano nella nozione di privata dimora di cui all'art. 624 bis c.p. esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare».

[81] Sottolinea A. CAMON, voce Captazione di immagini, in Enc. dir., VI, Milano, 2013, 143 s., che «la distinzione tra comportamenti comunicativi e non ha qualcosa di artificioso [...], in quanto spezza in due uno strumento investigativo in realtà unitario quanto a tipologia, natura, grado e modalità di compressione del bene tutelato».

[82] L'espressione appartiene a A. SCALFATI, Orientamenti in tema di videoriprese, cit., 93.

[83] Come precisato dalla giurisprudenza di legittimità, «[L]e videoriprese effettuate "da remoto", mediante l'attivazione attraverso un virus informatico della telecamera di un apparecchio telefonico smartphone, possono ritenersi legittime quali prove atipiche ai sensi dell'art. 189 c.p.p. salvo che siano effettuate all'interno di luoghi di privata dimora, e ferma la necessità di autorizzazione motivata dall'autorità giudiziaria per le riprese che, pur non comportando una intrusione domiciliare, violino la riservatezza personale». Così Cass., sez. VI, 26 maggio 2015, n. 27100, in Guida dir., 2015, f. 41, 83.

[84] R. ORLANDI, Una giustizia penale a misura di nemici?, in Riv. it. dir. proc. pen., 2020, f. 2, 718.

[85] Così Corte EDU, Grande Camera, 25 marzo 1998, Kopp c. Svizzera, n. 23224/94, § 53 s. Ma già Id., Grande Camera, 15 giugno 1992, Ludi c. Svizzera, n. 12433/86.

[86] D. CURTOTTI, Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole, in Proc. pen. giust., 2018, f. 3, 435.

[87] Così C. BECCARIA, Dei delitti e delle pene, Marco Coltellini ed., 1764, 33.

[88] Cfr. Cass., sez. V, 30 maggio 2017, n. 48370, cit., 2498 ss.

[89] In questo senso, per tutti, F. CAPRIOLI, Intercettazioni e tutela della privacy nella cornice costituzionale, in Cass. pen., 2021, f. 4, 1143.

[90] C. PELOSO, La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per

CamminoDiritto.it
ISSN 2532-9871

le intercettazioni tra presenti nei reati di terrorismo, in Dir. pen. cont., 1 giugno 2017.

[91] Così efficacemente D. CURTOTTI, Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole, cit., 438.

[92] La c.d. teoria dei frutti dell'albero avvelenato (anche definita inutilizzabilità derivata), si contrappone alla tesi del "male captum bene retentum". In base alla prima teoria, i vizi dell'atto inutilizzabile travolgono anche quello successivo; viceversa, chi propende per la seconda tesi, in assenza di un espresso richiamo normativo – sulla falsariga di quanto previsto dall'art. 185 c.p.p. in rapporto alle nullità) – l'invalidità non può in nessun caso propagarsi. Sul tema, esaustivamente, F. CORDERO, Il procedimento probatorio, in Tre studi sulle prove penali, Milano, 1963, 65 ss.; F.R. DINACCI, L'inutilizzabilità nel processo penale. Struttura e funzione del vizio, Milano, 2008, 91; N. GALANTINI, voce Inutilizzabilità (dir. proc. pen.), in Enc. dir., Agg. I, Milano, 1997, 700 ss.; G. PIERRO, Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali, Edizioni Scientifiche Italiane, 1992, 170; A. SCELLA, Prove penali e inutilizzabilità. Uno studio introduttivo, Torino, 2000, 134; G. SPANGHER, "E pur si muove": dal male captum bene retentum alle exclusionary rules, in Giur. cost., 2001, 2821. Più di recente, C. CONTI, Accertamento del fatto e inutilizzabilità nel processo penale, Cedam, 2007, 91 ss.; F.R. DINACCI, L'inutilizzabilità nel processo penale. Struttura e funzione del vizio, Milano, 2008, 62 ss.; V. FANCHIOTTI, Non c'è albero cattivo che dia frutti buoni, in Arch. nuova proc. pen., 2018, f. 3, 205; P. FERRUA, Prove illegittimamente acquisite: passato ed avvenire di un'illustre teoria, in Dir. pen. e proc., 2020, f. 9, 1256; N. GALANTINI, Inutilizzabilità della prova e diritto vivente, in Riv. it., dir. proc. pen., 2012, f. 1, 70 s.; G. ILLUMINATI, L'inutilizzabilità della prova nel processo penale italiano, ivi, 2010, f. 1, 534. Per ulteriori spunti in rapporto ai confini di utilizzabilità della prova scientifica, v. anche D. CURTOTTI, I rilievi e gli accertamenti tecnici, Cedam, 2013, 354 ss.

[93] Senza alcuna pretesa di completezza, Cass., sez. VI, 31 maggio 2011, n. 29666, in C.E.D. Cass., n. 250558; Id., sez. II, 8 aprile 2008, n. 19647, ivi, n. 239784; Id., sez. V, 13 marzo 1992, n. 899, in Riv. it. dir. proc. pen., 1992, 1197 ss. In questo senso anche una parte della dottrina per cui ci sarebbe una dipendenza giuridica e, quindi una contaminazione del vizio, in tutti i casi in cui la prova successiva non sarebbe stata scoperta senza la prova inutilizzabile. V., ex plurimis, F.M. GRIFANTINI, voce Inutilizzabilità, in Dig. disc. pen., vol. VII, Torino, 1999, 253. Nello stesso senso anche V. GREVI, Nemo tenetur se detegere, Milano, 1972, 192.

[94] Come sostenuto, quella derivata non è una specie autonoma di invalidità; «si tratta piuttosto di un effetto del vizio che affligge l'atto». Così G. CONSO, Il concetto e le specie di invalidità. Introduzione alla teoria dei vizi degli atti processuali, Milano, 1955, 79. Nello stesso senso anche C. CONTI, L'inutilizzabilità, in AA. VV., Le invalidità processuali, a cura di A. Marandola, Torino, 2015, 146 ss.

[95] Corte cost., 27 settembre 2001, n. 332, in Giur. cost., 2001, 2821 ss. Più di recente, Id., 26 novembre 2020, n. 252, in Riv. it. dir. proc. pen., f. 1, 2021, 297, con nota di A. ZAMPINI, La Corte costituzionale nuovamente alle prese con le perquisizioni, tra male captum e legittimità dell'iter autorizzativo; Id., 3 ottobre 2019, n. 219, in Giur. cost., 2019, 2581 ss., con nota di P. FERRUA, Perquisizioni illegittime e sequestro, 2595. V. anche i commenti di C. IASEVOLI, La funzione 'dissuasiva' del processo penale, in AA. VV., Scenari e trasformazioni del processo penale. Ricordando Massimo Nobili, a cura di C. Iasevoli, 2020, 346. Per una visione più generale del trend seguito dalla Consulta nelle pronunce in esame, N. GALANTINI, Alla ricerca della "inutilizzabilità derivata", in Sist. pen., 2021, f. 3, 151 ss.

[96] In questo senso la giurisprudenza di legittimità. Ex plurimis, Cass., sez. V, 8 marzo 2018, n. 32009, in C.E.D. Cass., n. 273641; Id., sez. V, 20 novembre 2015, n. 12697, ivi, n. 263031; Id., sez. II, 29 novembre 2011, n. 44877, ivi, n. 251361; Id., sez. V, 11 marzo 2011, n. 21047, ivi, n. 250415; Id., sez. I, 2 marzo 2010, n. 16283, ivi, n. 246657; Id., sez. un., 27 marzo 1996, n. 5021, in Cass., pen., 1996, f. 11, 3272 ss.

[97] In dottrina M. CHIAVARIO, Limiti probatori nel vigente codice di procedura penale, in AA. VV., Garanzie ed efficienze della giustizia penale, a cura di M. Chiavario, Torino, 1998, 141. Ma già F. CORDERO, Prove illecite nel processo penale, in Jus, 1961, f. 1, 68. Sul punto, v. anche In tema anche N. TRIGGIANI, Sull'utilizzabilità a fini investigativi dei risultati di una intercettazione telefonica illegittima, in AA. VV., Percorsi di procedura penale, vol. IV, La revisione del codice di procedura penale agli albori del ventennio (1988-2008): riforma globale e tutela dei diritti della persona, a cura di V. Perchiunno, Giuffré, 2008, 63 ss. D'altra parte, non è nemmeno prospettabile procedere estendere alla inutilizzabilità la previsione dell'art. 185, comma 1 c.p.p. nel pieno rispetto del principio di tassatività che permea la materia delle invalidità. N. GALANTINI, L'inutilizzabilità della prova nel processo penale, Cedam, 1992 46 ss. In senso conforme, la giurisprudenza di legittimità nega l'applicabilità dell'art. 185, comma 1 c.p.p. per escludere il fenomeno della invalidità derivata della prova. a. V., tra le altre, Cass., sez. VI, 4

CamminoDiritto.it
ISSN 2532-9871

febbraio 2020, n. 9009 in C.E.D. Cass., n. 278563; Id., sez. VI, 30 aprile 2019, n. 4119, ivi, n. 27819; Id., sez. V, 29 ottobre 2019, n. 44114, ivi, n. 277432; Id., sez. VI, 22 ottobre 2019, n. 18125, ivi, n. 279555.

[98] Cfr. Cass., sez. VI, 28 luglio 2020, n. 22790, in Sist. pen., 11 settembre 2020.

[99] Come acutamente osservato con riferimento alla inutilizzabilità "tradizionale" «il principio [...] ex art. 191 comma 1 c.p.p. impedisce al giudice di valutare le prove acquisite in violazione dei divieti stabiliti dalla legge, ma non esclude che il pubblico ministero e la polizia giudiziaria possano trarre dagli atti vietati dalla legge spunti che ritengano utili per imbastire altre legittime investigazioni, i cui risultati potranno poi prospettare alla valutazione del giudice». Così N. TRIGGIANI, Sull'utilizzabilità a fini investigativi dei risultati di una intercettazione telefonica illegittima, in Cass. pen., 2005, f. 12, 3947.

[100] Si consideri che, in tema, la giurisprudenza di legittimità ha affermato che «le informazioni assunte attraverso mezzi di prova illegittimi, inutilizzabili per il giudice, possono essere utilizzate legittimamente dal pubblico ministero e dalla polizia giudiziaria per il prosieguo delle indagini». Così Cass., sez. III, 10 febbraio 2004, n. 16499, in Giur. it., 2004, f. 12, 2360 ss. Più di recente la Corte ha chiarito che «la sanzione dell'inutilizzabilità delle intercettazioni riguarda i risultati probatori conseguiti con quello specifico mezzo di prova, il che non esclude che il medesimo risultato possa essere ottenuto con altro diverso mezzo di prova previsto dall'ordinamento». Cfr. Cass., sez. IV, 7 novembre 2019, n. 1007, in C.E.D. Cass., n. 277586.

[101] Così C. FANUELE, L'utilizzazione delle denunce anonime per l'acquisizione della notizia di reato: condizioni e limiti delle attività pre-procedimentali alla luce delle regole sul "giusto processo", in Cass. pen., 2012, f. 8, 1555.

[102] L'espressione appartiene a R. APRATI, La notizia di reato nella dinamica del procedimento penale, Jovene, 2010, 52.

[103] Si pensi, ad esempio, al c.d. catcher, tecnica che consente controlli di massa, "parassitando" i collegamenti instaurati tra gli apparecchi riceventi, tipicamente cellulari, e le reti mobili. Sul punto, cfr. A. CAMON, Il cacciatore di IMSI. Archivio penale, 2020, f. 1, 1 ss.; W. NOCERINO, Il‌ ‌tramonto‌ ‌dei‌ ‌mezzi‌ ‌di‌ ‌ricerca‌ ‌della‌ ‌prova‌ ‌nell'era‌ ‌2.0, in Dir. pen. proc., 2021, 1017.

[104] Infatti, in Corte cost., 26 novembre 2020, n. 252, cit., la Consulta precisa che sussistono «peculiarità "funzionali" che caratterizzano il sistema delle inutilizzabilità e dei connessi divieti probatori in ragione dei valori che mirano a preservare, [per cui] esist[e] una gamma "differenziata" di regole di esclusione, alle quali corrisponde un altrettanto differenziato livello di lesione dei beni che quelle regole intendono tutelare».

[105] Così L. ANNUNZIATA, Questioni probatorie. Tra male captum bene retentum e theory of the fruit of the poisonous tree, Pacini, 2017, 152.

[106] Condivide la medesima impostazione N. GALANTINI, Alla ricerca della "inutilizzabilità derivata", cit., 157, per cui «[S]i potrebbe essere indotti a sostenere [...] azione che, a prescindere dall'inconferente e impraticabile meccanismo della nullità derivata, è il mezzo probatorio surrogato a non essere conforme in sé, nella sostanza, al suo stesso modello legale. [...] Lo schema dell'uso indiretto potrebbe così supportare la rivisitazione di alcune inutilizzabilità speciali, tra le quali dovrebbero essere ricompresi per coerenza i casi che, se non riconducibili propriamente alla tortura, sottendono il ricorso a pratiche lesive della libertà di autodeterminazione e risultano privi di un espresso effetto sanzionatorio».

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=8457