DIRITTO PENALE CONTEMPORANEO

IL CAPTATORE INFORMATICO IN ATTESA DELLA RIFORMA (*)

di Manfredi Bontempelli

SOMMARIO: 1. Il captatore informatico come strumento tecnico dell'intercettazione. – 2. L'intercettazione di comunicazioni domiciliari tramite captatore informatico. – 3. Superamento della teoria giurisprudenziale della c.d. "intercettazione ambientale itinerante". – 4. Attuale regime d'uso del captatore ai fini d'intercettazione. – 5. Profili di utilizzabilità probatoria del captatore informatico come strumento della perquisizione.

1. Il captatore informatico come strumento tecnico dell'intercettazione.

Appare riduttivo, ma scontato, l'inquadramento del captatore informatico come strumento tecnico dell'intercettazione, e quindi come componente eventuale di questo mezzo probatorio[1]. Scontato, innanzitutto, per una ragione empirica, dato il crescente utilizzo giudiziario del congegno in discorso, e dell'intercettazione in sé intesa come «la prova principe del processo penale del ventunesimo secolo»[2].

C'è, poi, un'ovvia ragione normativa, costituita dalla disciplina delle "intercettazioni mediante inserimento di captatore informatico", ad opera dell'art. 4 d.lgs. n. 216/2017, con cui è stata attuata la delega contenuta nella legge n. 103/2017 (c.d. legge Orlando). La novella fornisce una sistemazione legislativa della specifica materia, nel più ampio contesto delle indagini informatiche[3], che risulta per un verso organica, poiché detta le condizioni e i limiti di utilizzabilità processuale dell'intercettazione tramite captatore, in autonomia rispetto alla soluzione fornita

(*) Il contributo costituisce il testo della relazione presentata alla *Digital Transformation Law Conference* (DTLC, 2018), Università degli Studi di Milano – 12, 13 e 14 dicembre 2018.

[1] Si veda l'impostazione di O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, p. 25, che così definisce la «componente» dello «strumento di prova», il cui intervento «nell'impiego dei mezzi di prova è per alcuni loro esemplari necessario e per altri eventuale»: «essa consiste in apparati conoscitivi (principi e metodologie della scienza teorica, metodiche della scienza applicata, tecnologie, procedure di indagini tecniche e di valutazioni costruite sulla scorta di esperienze pratiche specializzate, apparecchiature con cui queste risorse di conoscenza sono utilizzate) che esorbitano dal sapere comune quanto a competenza teorica o pratica e richiedono perciò il ricorso a un esperto». Proprio al novero delle «apparecchiature tecniche» appare riconducibile il captatore informatico, quale «componente ulteriore rispetto a quelle individuate nelle previsioni del catalogo» codicistico (v. ancora O. DOMINIONI, *op. loc. cit.*).

[2] O. MAZZA, *Introduzione*, in *Le nuove intercettazioni*, a cura di O. MAZZA, Torino, 2018, p. XI.

[3] Per una ricostruzione sistematica, v. il recente contributo di S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Padova, 2018.

dall'attuale "diritto vivente". Per altro verso, si tratta di una sistemazione parziale, in quanto il decreto non contiene disposizioni circa l'utilizzo dei c.d. *trojan* ad altri fini, e in particolare come strumento per effettuare videoriprese, oppure le perquisizioni *on line*[4]. Va verificato se, alla luce delle nuove norme, il problema dell'utilizzabilità del captatore debba essere reimpostato su questi ulteriori versanti, ed eventualmente in che termini[5]. Resta da dimostrare l'ipotesi interpretativa che, in mancanza di disposizioni di legge che ne sanciscano espressamente l'ammissibilità, sia radicalmente precluso l'utilizzo del virus *trojan* al di fuori delle intercettazioni[6].

Inoltre, la disciplina del d.lgs. n. 216/2017 non è sfuggita alle opzioni legislative compiute dal sopravvenuto governo, che ha modificato le disposizioni introdotte con la "riforma Orlando" «ancora nel mezzo del guado (caso estremo: alcune di quelle disposizioni erano in regime di *vacatio legis*)»[7]. Anche per il captatore le nuove disposizioni si applicheranno (salvo ulteriori ripensamenti del legislatore) "alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019", in base alla disciplina transitoria di cui all'art. 9 comma 1 d.lgs. n. 216/2017, come modificata dal d.l. n. 91/2018, conv. in l. n. 108/2018.

Peraltro, ai sensi del citato art. 9 comma 1, le disposizioni dell'art. 6 d.lgs. n. 216/2017 risultano applicabili a far data dal 26 gennaio 2018 (momento di entrata in vigore del decreto stesso)[8], con la conseguenza che il sistema di governo processuale del captatore informatico già ora deve essere ricostruito tenendo conto delle norme di "semplificazione delle condizioni per l'impiego delle intercettazioni delle conversazioni e delle comunicazioni telefoniche e telematiche nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione" (così la rubrica

---

[4] Per una panoramica sui potenziali usi processuali del captatore informatico alla luce delle sue caratteristiche tecniche v., ad es., R. BRIGHI, *Funzionamento e potenzialità investigative del malware*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. GIOSTRA e R. ORLANDI, Torino, 2018, pp. 221 ss.; O. CALAVITA, *L'odissea del* trojan horse, in questa *Rivista*, fasc. 11/2018, p. 45 ss. Con precipuo riguardo al tema delle perquisizioni *on-line*, v., ad es., L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, *ivi*, pp. 289 ss., la quale ritiene che «la poliedrica figura delle "perquisizioni *on-line*" [sia] destinata […] ad accogliere in via residuale quanto rimanga fuori dalla sfera delle intercettazioni *stricto sensu* e dagli altri mezzi di ricerca della prova tipici».

[5] Secondo L. PARLATO, *op. cit.*, p. 290, «il lato "nascosto", su cui la novella è rimasta silente, crea difficoltà interpretative ancor maggiori di quelle direttamente legate alla lettura del testo».

[6] V. i rilievi anche metodologici di F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. brasileira dir. proc. pen.*, 2017, pp. 485-486, alla luce del fatto che «nel codice di procedura penale italiano manca una specifica regolamentazione della materia. Va tuttavia immediatamente precisato che ciò non significa che le attività investigative di cui si discute debbano ritenersi vietate, e, come tali, insuscettibili di fornire materiali probatori utilizzabili in giudizio (art. 191 c.p.p.). Ciò per due ragioni. In primo luogo, perché alcune di tali attività […] sono riconducibili a strumenti di ricerca della prova già disciplinati dalla legge (segnatamente, l'intercettazione di comunicazioni). In secondo luogo, 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.)».

[7] *Prefazione* alla Sesta edizione di O. DOMINIONI ed altri, *Procedura penale*, Torino, 2018.

[8] Al riguardo, ad es., M. GAMBARDELLA, *Entrata in vigore e profili di diritto transitorio*, in *Nuove norme in tema di intercettazioni*, cit., p. 160.

dell'art. 6 cit.). Senza tralasciare la difficoltà di dover considerare attualmente applicabile una disposizione riguardante le intercettazioni eseguite con il captatore, il comma 2 dell'art. 6, che non solo è speciale rispetto al comma 1 del medesimo articolo, riguardante le intercettazioni "tradizionali", ma si raccorda anche alle disposizioni generali sul captatore, contenute nell'art. 4 e allo stato inapplicabili *ex* art. 9 comma 1 in quanto in regime di *vacatio*. Si noti, fra l'altro, che il 31 maggio 2018 è stato pubblicato il regolamento ministeriale contenente i "requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore" (art. 4 del D.M. 20 aprile 2018)[9], senza che ne sia stata posticipata l'operatività come per le disposizioni sul captatore inserite nel codice. La disciplina regolamentare attua l'art. 7 d.lgs. n. 216/2017, peraltro assoggettato al periodo di *vacatio* ai sensi del citato art. 9 comma 1.

È evidente l'importanza di chiarire se la legge processuale già preveda l'uso del captatore, e in che limiti, tanto più se si aderisce alla tesi della dottrina secondo cui sarebbero ammissibili soltanto gli usi dello strumento probatorio previsti dalla legge processuale. Si pensi, ad esempio, alla «duplice limitazione» ricavata dall'art. 266 comma 2 c.p.p., nuovo testo (non ancora applicabile), che consente l'esecuzione dell'intercettazione di comunicazioni fra presenti "anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile": si è osservato, incisivamente, che «il captatore può essere usato solo come mezzo di intercettazione ambientale e soltanto su dispositivi portatili. Non sono previsti (*e, pertanto, si direbbe, non sono ammessi*) usi diversi da quello appena ricordato, come ad esempio, perquisizioni *on-line* o intercettazioni di messaggi in uscita con il controllo a distanza del *software* di comunicazione (es. programmi *e-mail*, *Messenger*, *WhatsApp*). Né possono essere controllati con captatori informatici i *computer* fissi. Il discorso è quindi circoscritto ai *computer* portatili, ai *tablet*, agli *smartphone*»[10].

---

[9] Cfr. al riguardo M. TORRE, *D.M. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico*, in *Dir. pen. proc.*, 2018, p. 1255. V. anche, in linea generale, G. ZICCARDI, *Il captatore informatico nella "Riforma Orlando": alcune riflessioni informatico-giuridiche*, in *Arch. pen.*, 2018, *Speciale Riforme*, pp. 5 ss., 10 ss.

[10] R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, pp. 544-545 (corsivo aggiunto). Cfr. anche P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, in *Le nuove intercettazioni*, cit., p. 119; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit., p. 291. Per un'impostazione più articolata, v. P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in *Nuove norme in tema di intercettazioni*, cit., pp. 237-238, che distingue tra impieghi ammissibili del captatore («nelle ipotesi in cui l'inoculazione del *virus* costituisca solo una particolare metodica di attività investigative già conosciute e regolamentate: ad esempio, l'attivazione tramite *virus* informatico della telecamera di cui è dotato un dispositivo elettronico è riconducibile alla videoripresa, consentita nei limiti specificati dalla giurisprudenza delle Sezioni Unite; l'acquisizione delle comunicazioni che passano attraverso dispositivi elettronici collegati a sistemi di messaggistica *on-line* è invece riconducibile alla intercettazione telematica disciplinata dall'art. 266-*bis* c.p.p.») e gli altri, inammissibili, impieghi del *trojan* («anche ove i meccanismi "assomiglino" a quelli propri di mezzi investigativi consentiti: ad esempio, le cosiddette perquisizioni *on-line* (*on-line search*) o l'accesso, con facoltà di copia, ai dati memorizzati nei dispositivi o in *cloud*»).

2. L'intercettazione di comunicazioni domiciliari tramite captatore informatico.

È significativo il fatto che, per i procedimenti di cui all'art. 6 d.lgs. n. 216/2017, il legislatore abbia graduato il regime d'impiego delle intercettazioni con il captatore, rendendolo più restrittivo quanto alle comunicazioni domiciliari, rispetto a quelle extradomiciliari. Il comma 2 dell'art. 6 cit. esclude, infatti, l'uso dello strumento probatorio in discorso al fine di eseguire "l'intercettazione di comunicazioni tra presenti nei luoghi indicati dall'articolo 614 del codice penale", quando non vi è "motivo di ritenere che ivi si stia svolgendo l'attività criminosa".

Ne consegue, per un verso, il dovere del giudice di indicare nel provvedimento autorizzativo delle intercettazioni di comunicazioni domiciliari eseguite tramite captatore, «lo specifico luogo (l''ambiente') in cui si svolgerà l'attività investigativa»[11], a dimostrazione della correttezza dell'assunto sostenuto dalla giurisprudenza di legittimità prima dell'intervento delle Sezioni Unite della Corte di cassazione nel 2016[12]. Secondo tale assunto, «l'unica opzione interpretativa compatibile con il dettato costituzionale è quella secondo la quale l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati *ab origine* e non in qualunque luogo si trovi il soggetto»[13]. Si pone sulla stessa linea, in sostanza, la disposizione contenuta nell'art. 4 comma 1, lett. b), d.lgs. n. 216/2017, di modifica dell'art. 267 comma 1 c.p.p. e attualmente in regime di *vacatio*, in forza della quale devono essere indicati nel decreto autorizzativo "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono", sempre che si proceda "per delitti diversi da quelli di cui all'articolo 51, commi 3-*bis* e 3-*quater*" del codice.

Per altro verso, l'applicazione del citato art. 6 comma 2 d.lgs. n. 216/2017 non avrebbe senso, qualora non operasse per le intercettazioni eseguite con il captatore, la regola generale della limitazione dell'"intercettazione ambientale domiciliare" all'esistenza del requisito di cui all'art. 266 comma 2 c.p.p. Infatti, la norma speciale relativa al "captatore informatico su dispositivo elettronico portatile" deroga al regime di ammissibilità delle intercettazioni "tradizionali" fissato dall'art. 6 comma 1 d.lgs. n. 216/2017, che, a sua volta, deroga al più restrittivo regime di cui all'art. 266 c.p.p., equiparando i procedimenti per i richiamati delitti dei pubblici ufficiali contro la pubblica amministrazione ai procedimenti per i delitti di criminalità organizzata (art. 13 d.l. n. 152/1991, conv. in l. n. 203/1991). Come è noto, le intercettazioni di comunicazioni tra presenti "domiciliari" sono consentite in tali procedimenti "anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa". La norma speciale relativa al captatore informatico (art. 6 comma 2), facendo eccezione a una norma (art. 6 comma 1, di richiamo dell'art. 13 d.l. n. 152/1991) che è essa stessa speciale rispetto alla disciplina generale sulle intercettazioni di comunicazioni, riespande quindi, per i procedimenti di cui all'art. 6 d.lgs. n. 216/2017,

---

[11] Cass., Sez. VI, 26 giugno 2015, n. 27100, in *C.E.D. Cass.*, rv. 265654.

[12] Cass., Sez. Un., 28 aprile 2016, n. 26889, in *Dir. pen. cont.*, 7 ottobre 2016, con nota di G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*.

[13] Cass., Sez. VI, 26 giugno 2015, n. 27100, cit.

la portata della norma generale sulle intercettazioni domiciliari contenuta nell'art. 266 comma 2 c.p.p.[14].

È indubbio che, come si è affermato in dottrina, l'art. 6 comma 2 d.lgs. n. 216/2017 «pone una regola che limita il potere investigativo, vietando l'intrusione informatica su dispositivi portatili localizzati nel domicilio privato, quando non vi sia motivo di ritenere che lì si svolga l'attività presa di mira»[15]. Ed è vero, pertanto, come ha osservato la dottrina in discorso, che si tratta di una «regola priva di autonomia, destinata a combinarsi» sia «con la norma che ammette – in linea generale – l'uso dei captatori informatici»[16] sia, come si è visto, con la norma che limita – in linea generale – le intercettazioni di conversazioni in ambito domiciliare. Non c'è, quindi, alcun fenomeno di successione di leggi applicabili alle intercettazioni domiciliari nei procedimenti per i gravi reati contro la pubblica amministrazione. D'altra parte, è implicito all'art. 6 comma 2 cit. che le intercettazioni domiciliari eseguite con il captatore nei procedimenti per reati di "criminalità organizzata", *ex* d.l. n. 152/1991, esulino dalla regola generale di cui all'art. 266 comma 2 c.p.p. Quindi, l'art. 6 comma 2 va integrato in via interpretativa in senso, rispettivamente, restrittivo ed espansivo del potere investigativo di ricorrere al captatore.

3. Superamento della teoria giurisprudenziale della c.d. "intercettazione ambientale itinerante".

I richiamati indici normativi rendono in parte superato l'impianto concettuale della pronuncia delle Sezioni Unite del 2016, con particolare riferimento alla teoria della c.d. "intercettazione ambientale itinerante", impiegata dalla Suprema Corte al fine di escludere l'intercettazione di comunicazioni fra presenti con il captatore informatico, anche in ambiente non domiciliare, nei procedimenti per reati comuni, e di ammetterla anche in ambiente domiciliare, nei procedimenti per reati di criminalità organizzata[17]. Si può dire, in sintesi, che questa teoria giurisprudenziale sia caratterizzata dal particolare tipo di approccio – di metodo e interpretativo – seguito per argomentare la suddetta ripartizione.

Innanzitutto (profilo metodologico), la decisione delle Sezioni Unite ha posto al centro della teoria della "intercettazione ambientale itinerante" il tema della struttura

---

[14] Cfr., sul punto, 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 *Le nuove intercettazioni*, cit., p. 149.

[15] R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., p. 554.

[16] R. ORLANDI, *op. loc. ult. cit.*

[17] Per una critica sintetica e penetrante, v. 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, n. 2, p. 348.

tecnica del captatore[18], e lo ha ricollegato al tema della disciplina applicabile nei due tipi di procedimenti (per reati comuni e di criminalità organizzata), argomentando l'utilizzabilità del captatore stesso nel solo settore (quello dei procedimenti per reati di criminalità organizzata) in cui non opera il limite di ammissibilità delle intercettazioni domiciliari *ex* art. 266 comma 2 c.p.p. Esso imporrebbe l'indicazione del luogo *ex ante* e ciò, secondo tale giurisprudenza, sarebbe impossibile data la natura particolare dello strumento probatorio.

In secondo luogo (profilo interpretativo), la sentenza in discorso ha ribaltato l'opzione ermeneutica della necessaria individuazione (e indicazione) *ex ante* dei luoghi dell'intercettazione "ambientale", sostenendo che né la disciplina codicistica, né le garanzie CEDU prescriverebbero d'indicare i luoghi delle intercettazioni "tra presenti", mentre la legge processuale interna menzionerebbe l'"ambiente" al solo fine di tutelare il domicilio[19]. Peraltro, secondo la Suprema Corte, il riferimento al luogo, pur non integrando «un presupposto dell'autorizzazione» dell'intercettazione tra presenti, «compiuta con mezzi definibili "tradizionali"», avrebbe rilevanza «solo limitatamente alla motivazione del decreto nella quale il giudice deve indicare le situazioni ambientali oggetto della captazione, e ciò», prosegue la Corte, «solo ai fini della determinazione delle modalità esecutive del mezzo di ricerca della prova, che avviene mediante la collocazione fisica di microspie»[20]. Quindi, almeno considerazioni riguardanti le formalità assuntive del mezzo probatorio imporrebbero d'individuare il luogo di effettuazione delle intercettazioni "tradizionali" sin dal provvedimento autorizzativo.

È noto come la giurisprudenza delle Sezioni Unite abbia escluso la possibilità di intercettazioni domiciliari con lo strumento del captatore, «al di fuori della disciplina derogatoria di cui all'art. 13 della legge n. 203 del 1991»[21], in base alla «caratteristica tecnica di tale modalità di captazione» che, secondo la stessa giurisprudenza, «prescinde dal riferimento al luogo, trattandosi di una intercettazione ambientale per sua natura "itinerante"»[22]. Infatti, solo per l'intercettazione ordinaria, date le «modalità esecutive» richiamate (uso di microspie in luoghi circoscritti sin dall'inizio), opererebbe il «requisito autorizzativo delle intercettazioni tra presenti» domiciliari, *ex* art. 266

---

[18] Ribadisce la «connotazione "itinerante" del captatore informatico, che per sua natura "segue" lo strumento elettronico su cui è stato inoculato», di recente, P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 123.

[19] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 5 motivazione, secondo cui «l'art. 266, comma 2, cod. proc. pen., si limita ad autorizzare "negli stessi casi" previsti dal comma primo della stessa norma, "l'intercettazione delle comunicazioni tra presenti": il riferimento all'ambiente è presente solo nella seconda parte della disposizione, in relazione alla tutela del domicilio. La necessità dell'indicazione di uno specifico luogo – quale condizione di legittimità dell'intercettazione – non risulta inserita né nell'art. 266, comma 2 (in cui, con riferimento all'intercettazione di comunicazioni tra presenti, vi è solo la previsione di una specifica condizione per la legittimità dell'intercettazione se effettuata in un luogo di privata dimora), né nella giurisprudenza della Corte EDU».

[20] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 5 motivazione.

[21] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 6 motivazione.

[22] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 5 motivazione.

comma 2 c.p.p., «in tutta la sua pienezza, non consentendo eccezioni di alcun genere»[23]. Al contrario, per l'intercettazione mediante "intrusore" il giudice non potrebbe «prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico (*smartphone, tablet, computer*) verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale»[24]. In altre parole, nell'intercettazione tramite captatore mancherebbe il presupposto "tecnico" per applicare l'art. 266 comma 2 c.p.p., vale a dire la collocazione fisica di una microspia in luogo determinato (in grado di consentire la predeterminazione dei luoghi dell'operazione). Sarebbero, quindi, considerazioni sulla struttura del mezzo probatorio a fare emergere un profilo d'incompatibilità fra l'uso dello strumento tecnico del captatore e l'applicazione della disciplina sulle intercettazioni riguardante i procedimenti per reati comuni. Di conseguenza, ecco la conclusione del ragionamento della Corte di cassazione, sarebbe legittimo intercettare con il captatore nelle sole indagini di criminalità organizzata «a prescindere dalla preventiva individuazione ed indicazione dei luoghi in cui la captazione deve essere espletata»[25]; e senza che rilevi «che il dispositivo portatile, al cui interno è stato installato il "captatore informatico", possa (in quanto per natura "itinerante") intercettare conversazioni "tra presenti" dovunque»[26].

Ora, è proprio l'asserita incompatibilità – motivata da ragioni tecniche – fra uso del captatore e applicazione della disciplina codicistica ad essere superata dal d.lgs. n. 216/2017 che, innanzitutto, ammette l'inserimento del captatore informatico nei dispositivi elettronici portatili, ai fini d'intercettazione delle comunicazioni fra presenti, anche nei procedimenti per reati comuni e non solo di criminalità organizzata (art. 266 comma 2, primo periodo, c.p.p., nuovo testo). Inoltre, la nuova disciplina estende al captatore la distinzione di regime fra intercettazioni domiciliari ed intercettazioni extradomiciliari, ammettendo le prime solo quando ricorra una condizione analoga a quella di cui all'art. 266 comma 2 c.p.p. (il motivo di ritenere che nei luoghi domiciliari si stia svolgendo l'attività criminosa); a meno che non si proceda per i reati di cui

---

[23] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 6 motivazione.

[24] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 6 motivazione. E, di seguito, nel par. 7: «è impensabile, per tale mezzo di indagine, una preventiva individuazione ed indicazione dei luoghi di interesse, data la natura itinerante dello strumento di indagine da utilizzare». Anche in dottrina si è affermato che «all'atto di autorizzare un'intercettazione a mezzo di captatore informatico installato su di un apparecchio portatile, il giudice […] non sarà in grado di prevedere e predeterminare a priori i luoghi di privata dimora nei quali il congegno verrà introdotto e quindi non potrà controllare, né sotto il profilo oggettivo né sotto il profilo soggettivo, l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari». Così, S. LONATI, *I criteri direttivi contenuti nella delega in materia di intercettazioni di conversazioni o comunicazioni*, in *Le nuove intercettazioni*, cit., p. 25.

[25] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 10.1 motivazione.

[26] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 10.1 motivazione.

all'art. 51 commi 3-*bis* e 3-*quater* c.p.p., nel qual caso l'uso del captatore è sempre consentito (nuovo comma 2-*bis* dell'art. 266 c.p.p.)[27].

Ciò dimostra l'equivoco in cui era caduta la Suprema Corte quando, nella decisione a Sezioni Unite del 2016, aveva concluso per l'inapplicabilità dell'art. 266 comma 2 c.p.p. all'intercettazione mediante captatore, sul rilievo (peraltro giusto) dell'imprevedibilità (e incontrollabilità) dei luoghi in cui l'apparecchio "infettato" verrà introdotto. Il che, si poteva obiettare, non impedisce di limitare l'operatività del captatore (e quindi di tutelare il domicilio), attraverso l'attivazione e la disattivazione del microfono con cui vengono captati i dialoghi in prossimità del dispositivo portatile. Su questa linea è stato elaborato il criterio direttivo della lett. e), n. 1, della legge delega n. 103/2017, basato sull'"attivazione del microfono" e non sul "solo inserimento del captatore informatico" nell'apparecchio-bersaglio[28].

In attuazione di tale criterio, il d.lgs. n. 216/2017 richiede in ogni caso di indicare "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono", nei procedimenti per reati comuni (art. 267 comma 1 c.p.p., come modificato dall'art. 4 d.lgs. n. 216/2017): anche se non si tratta di intercettazioni domiciliari, e non è applicabile l'art. 266 comma 2 c.p.p., e quindi senza una correlazione con la tutela del domicilio, a dimostrazione della prioritaria *ratio* di garanzia della segretezza delle comunicazioni rivestita dalla regola processuale anzidetta. Come si vede, il d.lgs. n. 216/2017 determina un allargamento dello spazio operativo del captatore, rispetto alla precedente ricostruzione giurisprudenziale della materia, solo parzialmente controbilanciato da una disciplina più restrittiva sul piano delle "forme del provvedimento" autorizzativo, implicanti l'indicazione dei "luoghi" e del "tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono".

4. Attuale regime d'uso del captatore ai fini d'intercettazione.

Il regime attualmente operante, in forza del combinato disposto degli artt. 6 comma 2 e 9 comma 1 d.lgs. n. 216/2017, postula la medesima distinzione fra intercettazioni domiciliari ed extradomiciliari (altrimenti non si spiegherebbe il regime speciale di cui al citato art. 6 comma 2)[29], ma anche la distinzione fra procedimenti per reati comuni e per reati di criminalità organizzata (non operando allo stato, invece, il riferimento dell'art. 266 comma 2-*bis* c.p.p. ai procedimenti per i delitti previsti dall'art. 51 commi 3-*bis* e 3-*quater* c.p.p.). Inoltre, per le intercettazioni domiciliari eseguite tramite captatore, nei procedimenti per reati comuni, dovrà essere indicato, nel

[27] Parla, al riguardo, di una presunzione legale assoluta di «continuità della condotta criminosa», R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., p. 554.

[28] Più precisamente, il criterio citato prevede che "l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice".

[29] V., *supra*, par. 2.

provvedimento autorizzativo, il luogo di attivazione del microfono (per accertare la condizione di cui all'art. 266 comma 2 c.p.p.), mentre non vi sono espliciti dati normativi per ritenere che il luogo dell'intercettazione debba essere individuato (ed indicato) *ex ante* anche per le intercettazioni extradomiciliari, secondo la nuova prescrizione di cui all'art. 267 comma 1 c.p.p. (non ancora applicabile ai sensi dell'art. 9 comma 1 d.lgs. n. 216/2017).

Peraltro, si potrebbe ritenere che la regola in questione sia implicita alla disciplina processuale di ogni tipo di intercettazione di comunicazioni fra presenti effettuate mediante l'inserimento di un captatore informatico in un dispositivo elettronico portatile, dal momento che, se così non fosse, non si potrebbe prevenire a monte l'effettuazione di intercettazioni in ambito domiciliare in violazione dell'art. 266 comma 2 c.p.p. (sempre che non ne sia esclusa l'applicazione come accade nel settore regolato dal d.l. n. 152/1991). Insomma il captatore, non avendo un raggio d'azione fisso in quanto destinato a operare su apparecchi mobili, richiederebbe una cautela aggiuntiva, rispetto alle tradizionali intercettazioni di comunicazioni fra presenti, nel caso in cui sia utilizzato in procedimenti che ammettono le intercettazioni domiciliari alla condizione di cui all'art. 266 comma 2 c.p.p.

Beninteso, l'individuazione (e indicazione) *ex ante* potrebbe avvenire quantomeno "per ambienti", in caso di intercettazioni extradomiciliari, riprendendo la ricostruzione operata dalle Sezioni Unite nel 2016 (sostanzialmente condivisa dal d.lgs. n. 216/2017, con il nuovo comma 1 dell'art. 267 c.p.p.). Seppur nella diversa ottica di ancorare l'uso del captatore all'inapplicabilità della disciplina codicistica (confinandolo dunque ai procedimenti per reati di criminalità organizzata *ex* art. 13 d.l. n. 152/1991, conv. in l. n. 203/1991), la Suprema Corte aveva valorizzato gli «ulteriori punti fermi» traibili, «*de iure condito*», dalla disciplina codicistica e speciale, implicanti il dovere giudiziale di: a) indicare specificamente il luogo della captazione in caso di intercettazioni domiciliari[30]; b) indicare il luogo della captazione non specificamente, ma per «tipologia di ambienti» in caso di intercettazioni non domiciliari[31]; c) indicare il luogo della captazione nei soli casi in cui occorra applicare l'art. 266 comma 2 c.p.p.[32].

---

[30] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 9 motivazione, secondo cui: «a) di regola, il decreto autorizzativo delle intercettazioni "tra presenti" deve contenere la specifica indicazione dell'ambiente nel quale la captazione deve avvenire solo quando si tratti di luoghi di privata dimora, con la limitazione che, in detti luoghi, tali intercettazioni possono essere effettuate, in base alla disciplina codicistica, soltanto se vi è fondato motivo di ritenere che in essi si stia svolgendo attività criminosa».

[31] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 9 motivazione: «b) per le intercettazioni "tra presenti" da espletare in luoghi diversi da quelli indicati dall'art. 614 cod. pen. (come, ad esempio, carceri, autovetture, capanni adibiti alla custodia di attrezzi agricoli, luoghi pubblici, ecc.), deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti dove essa va eseguita: l'intercettazione resta utilizzabile anche qualora venga effettuata in un altro luogo rientrante nella medesima categoria».

[32] Cass., Sez. Un., 28 aprile 2016, n. 26889, cit., par. 9 motivazione: «c) l'indicazione del luogo o dell'ambiente della intercettazione "tra presenti" costituisce un indispensabile requisito autorizzativo nei soli casi in cui occorre fare applicazione della disciplina codicistica sulle limitazioni delle captazioni effettuate nei luoghi di privata dimora (vale a dire, la sussistenza del fondato motivo di ritenere che in essi si stia svolgendo l'attività criminosa)».

La regola della predeterminazione dei luoghi "per ambienti", pur costituendo una garanzia "debole" tenendo conto delle prassi invalse nella motivazione dei provvedimenti autorizzativi delle intercettazioni, sarebbe comunque in grado, se correttamente intesa, in termini di «progetto investigativo»[33], di evitare l'effettuazione di "intercettazioni itineranti". Di un tipo simile di intercettazione potrebbe continuare a parlarsi in considerazione, non della natura tecnica del captatore, ma della disciplina applicabile nei procedimenti per reati di criminalità organizzata.

Si noti che l'operatività dell'art. 6 d.lgs. n. 216/2017 rende pure attuale una distinzione di regime dei due tipi di intercettazione ambientale nei procedimenti per gravi reati contro la pubblica amministrazione[34], salvo che si tratti di delitti associativi: quelle "tradizionali", eseguite tramite cimici o microspie, sono assoggettate alla più permissiva disciplina di cui al d.l. n. 152/1991, con conseguente necessità di accertare un quadro indiziario "sufficiente" e non "grave", mentre la durata è di novanta giorni prorogabile; quelle effettuate mediante inserimento di un captatore su dispositivo elettronico portatile, indubbiamente più invasive per quanto riguarda gli interessi costituzionali coinvolti, restano assoggettate alla disciplina ordinaria, richiedono pertanto l'accertamento dei "gravi indizi di reato" ed hanno una durata di quindici giorni, prorogabile su autorizzazione giudiziale.

5. Profili di utilizzabilità del captatore informatico come strumento della perquisizione.

Resta tuttora controverso stabilire se il captatore informatico possa o no essere impiegato al fine di effettuare le c.d. perquisizioni *on-line*, tema che, come si è visto, non è stato espressamente risolto dal d.lgs. n. 216/2017. Il punto di riferimento giurisprudenziale in materia è costituito da una pronuncia della Quinta Sezione della Corte di cassazione del 2009, che ha ricondotto alla categoria della prova atipica l'acquisizione – tramite captatore – «della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati»[35]. La Suprema Corte ha individuato l'oggetto di quest'attività acquisitiva in «"un flusso unidirezionale di

---

[33] 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*, cit., p. 147. Secondo S. SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in *Nuove norme in tema di intercettazioni*, cit., p. 269, l'indiretta determinazione «secondo un verosimile progetto investigativo rende del tutto incerta quella predeterminazione, a meno di non attribuire al giudice poteri divinatori».

[34] Per la analoga distinzione di regime nei procedimenti di criminalità organizzata, alla luce della disciplina del d.lgs. n. 216/2017 non ancora applicabile, v. R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., p. 554.

[35] Cass., Sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.*, rv. 246954 (massima).

dati" confinati all'interno dei circuiti del "computer"»[36]. La tesi, richiamata anche da un successivo arresto della stessa Quinta Sezione del 2017[37], è stata giustamente criticata dalla dottrina sul rilievo della lesione dei diritti costituzionali cagionata dall'operazione in discorso, in quanto non prevista dalla legge.

Si è osservato, in base a una prima tesi, che gli «atti di *online search* compiuti con l'ausilio dell'agente intrusore informatico […] rappresenterebbero una nuova e peculiare forma di violazione del domicilio, riconducibile a pieno titolo nell'orbita precettiva dell'art. 14 Cost.»[38]. Questa garanzia costituzionale tutelerebbe anche il c.d. "domicilio informatico": una vera e propria «proiezione *informatica* dell'individuo, destinata ad allargare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale»[39], e per definizione limitabile soltanto in base alla duplice riserva (di legge e di giurisdizione) presidiata dalla norma costituzionale anzidetta. Oppure, in base a una seconda tesi, sarebbe in gioco il «nuovo diritto fondamentale (alla libertà informatica)», che dovrebbe essere ricavato dall'art. 2 Cost. e «semplicemente riconosciuto quale manifestazione del libero sviluppo della personalità»[40]. Ciò significherebbe «esporre l'uso investigativo dei captatori informatici alla nota procedura che le costituzioni moderne esigono per la compressione di diritti considerati inviolabili: vale a dire, riserva di legge e autorizzazione giudiziale nel rispetto del principio di proporzionalità»[41]. A parte la diversa ricostruzione teorica, secondo entrambi gli approcci lo strumento in discorso sarebbe inutilizzabile, al fine di effettuare le perquisizioni *on-line*, data la comune premessa per cui «tutte le attività probatorie che comportano una violazione di questi tre fondamentali diritti dell'individuo», diritto alla libertà personale (art. 13 Cost.), diritto «all'intimità domiciliare» (art. 14 Cost.), diritto alla libertà e alla segretezza delle comunicazioni (art. 15 Cost.), «devono essere previste tassativamente dalla legge»[42].

---

[36] Cass., Sez. V, 14 ottobre 2009, n. 16556, cit.: «(Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non "un flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei cortocircuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prevista dagli artt. 266 ss. cod. proc. pen.)».

[37] Cass., Sez. V, 30 maggio 2017, n. 48370, in *C.E.D. Cass.*, rv. 271412.

[38] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., pp. 489 e 490.

[39] F. CAPRIOLI, *op. cit.*, p. 491: «un nuovo ed ulteriore spazio virtuale al cui interno – esattamente come nel domicilio e nei circuiti comunicativi riservati – ciascuno deve essere in grado di manifestare e sviluppare liberamente la propria personalità, al riparo da occhi e orecchi indiscreti».

[40] R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., p. 543 e, rispettivamente, p. 542.

[41] R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., p. 543. Secondo F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 491, invece, se si seguisse la strada di estrapolare dall'art. 2 Cost. «un nuovo diritto fondamentale alla "riservatezza informatica"», «rimarrebbero interamente da definire i contorni della tutela sovraordinaria: in particolare, non si tratterebbe di un diritto esplicitamente presidiato dalla doppia riserva di legge e giurisdizione».

[42] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 487. Nello stesso senso, R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., p. 543, secondo cui «le cosiddette perquisizioni *on-line* andrebbero considerate illegittime fino a che non saranno regolate da una norma

Sennonché, la tesi dell'inutilizzabilità dell'elemento probatorio «assunto in violazione di un diritto costituzionale in assenza di una espressa disciplina legislativa dei casi e dei modi» con cui restringere il diritto predetto[43], si espone all'obiezione di fondo secondo cui anche per la prova atipica l'inutilizzabilità deriverebbe dai divieti probatori ricavabili dal catalogo legale dei mezzi di probatori, con conseguente necessità di individuare i profili di «tipicità tassativa» di tale disciplina legale[44]. È significativo il limite espansivo dell'istituto dell'inutilizzabilità affermato da autorevole dottrina con riguardo alle «"notizie e immagini" ottenute con interferenze illecite nel domicilio»: si è osservato che «i canoni costituzionali operano indirettamente; finché l'art. 189 non sia dichiarato illegittimo "nella parte in cui" non esclude prove ottenute con interferenze indebite nella vita privata domestica, niente osterà all'uso processuale del documento foto- o cinematografico, dovunque sia situata l'immagine, nel domicilio o fuori, e comunque fosse avvenuta la ripresa (ad esempio, con un apparecchio ottico che veda attraverso i muri)»[45].

Inoltre, è dubbia la stessa riconducibilità delle perquisizioni *on-line* alla categoria della prova atipica, considerando che la legge già prevede la perquisizione di "un sistema informatico o telematico, ancorché protetto da misure di sicurezza", finalizzata alla ricerca di "dati, informazioni, programmi informatici o tracce comunque pertinenti al reato" (art. 247 comma 1-*bis* c.p.p., introdotto dalla l. n. 48/2008). Non sembra contestabile che il captatore serva proprio per introdursi in un sistema informatico o telematico, eventualmente protetto, per raccogliere elementi dei suddetti tipi[46].

Contro l'ipotesi d'inquadrare nello schema tipico della perquisizione anche informatica le attività compiute tramite captatore «che consistono nel "perquisire l'*hard disk* e fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira"», si è espressa, anche di recente, la dottrina, articolando – indubbiamente con efficacia – le seguenti motivazioni: «In primo luogo, perché, a differenza delle perquisizioni regolate dalla legge, sono attività investigative occulte, svolte all'insaputa della persona che ha la disponibilità dell'oggetto da perquisire. In secondo luogo, perché sono attività investigative permanenti, destinate a protrarsi nel tempo. In terzo luogo, perché sono attività investigative funzionali all'acquisizione indiscriminata di dati (notizie di reato comprese) anziché alla ricerca selettiva di prova in ordine a un addebito preesistente»[47]. Ma, a ben guardare, anche le perquisizioni locali previste

---

volta ad attuare le accennate garanzie procedurali imposte dalla costituzione per la limitazione dei diritti inviolabili. E lo stesso vale per l'uso di captatori informatici quali mezzi di intercettazione alternativi a quelli già regolati dalla legge processuale».

[43] V. C. CONTI, *Accertamento del fatto e inutilizzabilità della prova nel processo penale*, Padova, 2007, p. 173, che ricava il divieto probatorio direttamente dall'art. 189 c.p.p.

[44] V., per questa tesi, O. DOMINIONI, *La prova penale scientifica*, cit., p. 91.

[45] F. CORDERO, *Procedura penale*, IX ediz., Milano, 2012, pp. 850-851.

[46] Per un inquadramento della c.d. "*on line search*" v., ad es., M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, pp. 56 ss.

[47] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 489. Secondo M. TORRE, *Il captatore informatico*, cit., p. 60, inoltre, un'altra differenza consisterebbe nel fatto che «l'attività di

dall'art. 247 c.p.p. possono svolgersi in modo occulto, cioè all'insaputa di chi abbia la disponibilità dei luoghi, ove sia assente (fermo restando l'avviso di deposito del decreto di perquisizione, a norma dell'art. 80 comma 2 n. att. c.p.p.)[48]. E si potrà trattare di operazioni diluite nel tempo, finalizzate ad acquisire una massa indistinta di cose pertinenti al reato (si pensi alla ricerca di documentazione nei locali di un'impresa di grandi dimensioni). Né è peregrina l'ipotesi che in tali contesti l'attività di ricerca probatoria faccia emergere la notizia di ulteriori reati. Le caratteristiche sopra enucleate non sarebbero pertanto decisive per escludere l'applicazione dell'art. 247 c.p.p. alle perquisizioni *on-line*[49].

Inoltre, il citato art. 247 comma 1-*bis* c.p.p., prevedendo che la perquisizione sia disposta "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" (analogamente dispone l'art. 244 comma 2 c.p.p., per quanto riguarda l'ispezione), demanda alla scienza e alla tecnica il compito d'individuare gli *strumenti* della ricerca probatoria, aprendo un varco normativo all'uso del captatore informatico concepito come apparecchiatura tecnica e, quindi, strumento probatorio[50] della perquisizione *on line*. Si pone, però, il problema della controllabilità giudiziale dell'uso delle misure tecniche anzidette in generale, e del captatore in particolare[51], in funzione di garantire l'attendibilità dell'accertamento, oltre che il diritto di difesa dell'imputato. Si è osservato, condivisibilmente, che «il ricorso alla *digital evidence* in questo contesto acutizza criticità intrinseche alla prova scientifica. In un ambito tecnologico tanto specialistico come è quello dei captatori informatici – e, più in generale, della *remote forensics* – il rischio di introdurre nel processo la *junk science* è elevato»[52].

---

captazione non sfocia nell'atto tipico del sequestro, bensì in un atto atipico, probabilmente un "verbale di operazioni compiute».

[48] È vero che, adottando l'impostazione in discorso, «dovendo consentire la partecipazione del difensore ai sensi degli artt. 356 e 365 c.p.p., le operazioni in questione perderebbero il loro carattere segreto e, dunque, buona parte della loro valenza conoscitiva. Inoltre esse sarebbero sottoposte all'autorizzazione del solo pubblico ministero anziché di un giudice, e senza alcuna limitazione quanto alla tipologia di reato oggetto del procedimento». Così, M. DANIELE, *Contrasto al terrorismo e captatori informatici*, in *Riv. dir. proc.*, 2017, p. 403 nt. 39.

[49] A. CAPONE, *Intercettazioni e Costituzione. Problemi vecchi e nuovi*, in *Cass. pen.*, 2017, pp. 1271 ss., dopo aver affermato che l'attività di *online search* compiuta tramite captatore informatico, «diretta alla ricerca e alla copia di documenti archiviati nella memoria del dispositivo bersaglio», è «senza dubbio assimilabile alle perquisizioni, almeno quando mira ad ottenere informazioni previamente individuate», avanza correttamente il quesito «se la perquisizione di un sistema informatico da remoto consenta tecnicamente l'adozione di tali misure e, laddove esistano, se esse siano adottate nella pratica».

[50] V., supra, nt. 1.

[51] In particolare, sulla essenzialità dei file di log al fine di verificare le azione compiute dal captatore v., ad es., G. ZICCARDI, *Il captatore informatico nella "Riforma Orlando"*, cit., p. 12.

[52] E. BRIGHI, *Funzionamento e potenzialità investigative del malware*, cit., p. 217. «Il problema di fondo è che il tema del captatore è "intrinsecamente tecnico"», afferma G. ZICCARDI, *Il captatore informatico nella "Riforma Orlando"*, cit., p. 3, che così prosegue: «Si tratta di uno di quei temi, quello dei captatori, che, per tradizione, andrebbero prima disciplinati nei loro aspetti tecnici e, solo successivamente, inseriti in un quadro normativo, anche per vincere la tradizionale segretezza circa il loro funzionamento che investe simili strumenti di indagini» (*ivi*, pp. 3-4).

Sulla scorta di questi rilievi, non pare insensato ricorrere ai criteri di ammissione dettati dall'art. 189 c.p.p. alla decisione se acquisire o no al processo i dati probatori assicurati tramite il captatore (ma anche al provvedimento con cui l'autorità giudiziaria disponga la perquisizione *on line*). È noto come la disciplina dell'art. 189 c.p.p. debba essere applicata per governare l'uso degli strumenti probatori nuovi o controversi e di elevata specializzazione, secondo la dottrina processuale che si è impegnata nel ricostruire organicamente il regime d'impiego processuale della nuova prova scientifica[53]. Qui in tanto la disciplina in discorso opererebbe, in quanto il captatore fosse considerato non un mezzo atipico di ricerca della prova o un mezzo d'indagine atipica, ma un apparato tecnico rientrante fra le componenti di un mezzo tipico di ricerca della prova, quale è la perquisizione[54].

Su questa linea, dovrebbe essere accertata in positivo, al momento della decisione acquisitiva, e non presunta, l'idoneità dei programmi d'impiego del captatore ad assicurare l'accertamento dei fatti, *ex* art. 189 c.p.p., a pena di esclusione dei dati probatori reperiti attraverso le perquisizioni *on line*[55]. Sotto questo profilo, sarebbe alquanto problematico l'uso dei programmi che non diano accesso ai c.d. "codici sorgente", senza i quali non è conoscibile come il *software* o il *malware* funzionino, né quindi è possibile controllare se l'uso del virus determini l'alterazione dei dati digitali[56] (in violazione dell'art. 247 comma 1-*bis* c.p.p.).

Inoltre, l'utilizzo del virus informatico non sarebbe praticabile nel caso in cui fosse accertata la lesione della libertà morale delle persone aventi la disponibilità del dispositivo elettronico portatile dove venga inoculato il captatore[57]. Si faccia il caso in cui l'attività di inoculazione del *trojan* avvenga con l'inganno. Va premesso che tale attività può essere svolta «secondo due modalità: o mediante installazione diretta da parte della polizia, quando riesce ad accedere al dispositivo, o tramite installazione remota»[58]. Qualora, «in quest'ultimo caso, l'inoculazione [avvenga] grazie alla collaborazione inconsapevole del destinatario, che viene tratto in inganno e, mentre accede ad esempio al *link* contenuto in una *e-mail* o effettua un aggiornamento di un *software* o di un'applicazione, scarica in realtà nel suo dispositivo informatico anche il

---

[53] O. DOMINIONI, *La prova penale scientifica*, cit., pp. 83 ss.

[54] Per una diversa impostazione, v. M. TORRE, *Il captatore informatico*, cit., pp. 58-59, che s'interroga, innanzitutto, sulla «verifica della effettiva "atipicità" dello strumento investigativo: individuare un modello tipico in cui ricondurre le perquisizioni *online*, infatti, significherebbe risolvere *ex lege* quella valutazione di legittimità dello strumento investigativo che, altrimenti, è rimessa totalmente all'interprete». Dopodichè l'A. afferma che «solo l'esito negativo di tale preliminare riscontro di tipicità consente di passare al livello successivo, consistente nella valutazione della possibilità di sfruttare, o meno, l'art. 189 c.p.p. per legittimare il mezzo atipico di ricerca della prova».

[55] V., invece, F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 486, secondo cui, «nel caso dei *Trojan horses*, è fuori discussione che si tratti di prove idonee ad assicurare l'accertamento di fatti». Cfr. anche M. TORRE, *Il captatore informatico*, cit., p. 69.

[56] Secondo G. ZICCARDI, *Il captatore informatico nella "Riforma Orlando"*, cit., p. 13, «il tema del codice sorgente alla base del *software* captatore e degli strumenti di *hacking* utilizzati si presenta come un argomento cruciale e, purtroppo, di non facile soluzione».

[57] V., invece, F. CAPRIOLI, *op. loc. ult. cit.*

[58] S. SIGNORATO, *Le indagini telematiche*, cit., p. 237.

captatore»[59], verrebbe violato «il principio del *nemo tenetur se detegere*, da intendersi in senso ampio, non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni autoincriminanti»[60], e dunque la libertà morale dell'individuo. Dovrebbe quindi parlarsi di impiego fraudolento del captatore, vietato *ex* art. 189 c.p.p., e per ritagliare spazi di legittimo utilizzo dello strumento ai presenti fini, dovrebbe naturalmente dimostrarsi che la tecnologia consenta l'inoculazione da remoto in modo occulto (senza collaborazione attiva del bersaglio investigativo).

Oppure l'inoculazione del captatore potrebbe avvenire «senza la collaborazione attiva, se pur involontaria, dell'utente bersaglio»[61]; anche in tal caso si potrebbe parlare di impiego occulto del captatore, consentito dalla legge. Si ricadrebbe, tuttavia, nell'ipotesi del "captatore fraudolento", qualora la polizia impiegasse un inganno per entrare in possesso del dispositivo elettronico portatile, che verrebbe materialmente consegnato tramite la collaborazione attiva del bersaglio investigativo, in violazione della sua libertà di autodeterminazione.

---

[59] S. SIGNORATO, *Le indagini telematiche*, cit., pp. 237-238. Cfr. anche R. BRIGHI, *Funzionamento e potenzialità investigative del malware*, cit., p. 219.

[60] Così, condivisibilmente, seppur in chiave dubitativa, S. SIGNORATO, *Le indagini telematiche*, cit., p. 238. V. la ricostruzione antitetica di M. TORRE, *Il captatore informatico*, cit., p. 69, che afferma con nettezza (ma sovrapponendo piani del discorso da distinguere) quanto segue: «ogni dubbio deve essere destituito di fondamento: proprio l'essenza "subdola", perché segreta, del captatore informatico rappresenta la maggiore garanzia dell'integrità del processo volitivo della persona, la quale, non sapendo di essere controllata, assumerà un comportamento del tutto naturale e svincolato da influenze esterne».

[61] R. BRIGHI, *Funzionamento e potenzialità investigative del malware*, cit., p. 220.