

Penale

CAPTATORE INFORMATICO

Il captatore informatico: riflessioni sulla recente sentenza della Cassazione

giovedì 03 dicembre 2020

di Filippi Leonardo - Avvocato e Professore ordinario di procedura penale nell'Università di Cagliari
Suraci Leonardo - Dottore di ricerca in diritto processuale penale presso l'Università La Sapienza di Roma

- Intercettazioni



Per approfondire

IL QUOTIDIANO GIURIDICO

- [Davvero possibili le intercettazioni c.d. a strascico attraverso l'uso del captatore informatico per i reati comuni?](#)
martedì 22 settembre 2020
- [Prova informatica e diritti fondamentali: a proposito di captatore e non solo](#)
mercoledì 19 settembre 2018
- [Intercettazioni con captatore informatico: parere del Garante sullo schema di decreto](#)
venerdì 10 agosto 2018

PRODOTTI



- Ebook - Legge 7/2020: la riforma delle intercettazioni



- Speciale Procedura penale: Commentario + Guida



• Giurisprudenza Italiana

EDICOLA PROFESSIONALE

• Il duplice volto del captatore informatico tra usi pubblici e privati
Diritto Penale e Processo n. 10/2020

• Davvero possibili le intercettazioni c.d. a strascico attraverso l'uso del captatore informatico per i reati comuni?
Diritto Penale e Processo n. 8/2020

• Intercettazioni: habemus legem!
Diritto Penale e Processo n. 4/2020

[Leggi dopo e Annota](#)



Captatore informatico e obbligo di motivazione. Riflessioni su [Cass. pen., Sez. V, 18 novembre 2020, n. 32428](#)

di Leonardo Suraci

Il captatore informatico

Il **tema** delle intercettazioni di conversazioni e comunicazioni, si è detto più volte, è **tra i più delicati e complessi della procedura penale**, trattandosi di un mezzo di ricerca della prova in relazione al quale gli effetti del progresso tecnologico – inarrestabilmente prolifico sul terreno degli strumenti e delle metodologie di captazione – si scontrano con le esigenze di protezione del diritto dei singoli individui alla libertà e segretezza delle loro comunicazioni.

Va detto subito che l'approccio giurisprudenziale alle questioni che lo strumento investigativo pone appare più o meno "liberalizzante", tendendosi a restringere quanto più possibile – alla luce, tra l'altro, di una normativa che riferisce a pochissimi profili dell'operazione captativa l'apparato sanzionatorio – i margini di operatività delle sanzioni processuali e, molto spesso, a collocare all'esterno del perimetro normativo le nuove metodologie consentite dall'evoluzione della tecnologia.

Le problematiche che negli ultimi anni hanno attratto l'attenzione degli interpreti – e giustamente, considerato che si discute di una novità tecnologica capace di influire come mai si era visto prima sulla sfera di libertà della persona costituzionalmente presidiata – ruotano intorno al c.d. **captatore**

informatico, strumento il quale soltanto di recente, dopo tanto tergiversare e non pochi aggiustamenti, ha trovato spazio nella disciplina codicistica.

Il mezzo investigativo di cui si discute presenta **caratteristiche tecniche del tutto peculiari** ed una portata invasiva della sfera di riservatezza, come già detto, del tutto nuova ed eccezionalmente penetrante. L'intercettazione, nel caso in esame, viene effettuata mediante il ricorso ad un *software* il quale viene installato in un dispositivo del tipo *target* a distanza ed in modo occulto tramite l'invio con una *mail*, un *sms* o un'applicazione di aggiornamento.

Il software è costituito da due moduli principali: il primo (*server*) è un programma di piccole dimensioni che infetta il dispositivo bersaglio; il secondo (*client*) è l'applicativo utilizzato dal *virus* per controllare siffatto dispositivo.

Lo strumento tecnologico in argomento consente di svolgere diverse attività, permettendo l'acquisizione di dati che, trasmessi a mezzo della rete *internet* ad un sistema informativo nella disponibilità degli investigatori, vengono dagli stessi acquisiti e fruiti per finalità investigative.

È così possibile, dunque:

- captare il traffico dati dal dispositivo infettato;
- attivare il microfono e, quindi, apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo;
- mettere in funzione la *web camera* e, dunque, carpire immagini;
- perquisire l'*hard disk* e fare copia, in tutto o in parte, delle unità di memoria del sistema informatico oggetto di intrusione;
- decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema e visualizzare ciò che appare sullo schermo del dispositivo;
- sfuggire agli antivirus.

Utilizzando il programma informatico appena descritto, quindi, è possibile captare i dialoghi che si svolgono tra persone presenti e la correlata attività dà luogo ad un'intercettazione di tipo ambientale che può avvenire ovunque sia localizzato l'apparecchio interessato, sia pure nei limiti della capacità di percezione del microfono.

Lo strumento, è evidente ed il dato è del tutto saliente, consente l'apprensione delle conversazioni tra presenti – mediante l'attivazione, attraverso il *virus* informatico, del microfono di un dispositivo elettronico (personal computer, tablet, smart-phone) – ovunque si svolgano dal momento che l'attività di captazione segue tutti gli spostamenti nello spazio dell'utilizzatore dell'apparecchio, eventualmente anche le situazioni di permanenza in luoghi qualificabili come domicilio e, pertanto, tutelati dalla previsione rafforzativa di cui all'[art. 266, co. 2](#) c.p.p.

La consapevolezza della **capacità eccezionalmente intrusiva** del captatore è stata fin da subito colta dalla comunità giuridica e, nel silenzio del codice processuale, è stata rimessa alla giurisprudenza la definizione dei limiti di impiego del mezzo percettivo.

La Corte di cassazione, occupandosi della materia ed alla luce delle caratteristiche della innovativa tecnica di captazione, ha **rimesso alle Sezioni unite** una pluralità di questioni, trattandosi di stabilire:

1. se il decreto che dispone tale metodica di intercettazione debba indicare, a pena di inammissibilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione;

2. se, in mancanza di tale indicazione, l'eventuale sanzione di inutilizzabilità riguardi in concreto soltanto le captazioni che avvengono in luoghi di privata dimora al di fuori dei presupposti indicati dall'[art. 266, comma 2](#) c.p.p.;

3. se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata ([Cass. pen., Sez. VI, ordinanza 6 aprile 2016, n. 13884](#)).

La rimessione della questione alle Sezioni unite era stata determinata da una precedente presa di posizione della Suprema Corte la quale, nell'occasione, si era espressa nel senso dell'illegittimità di siffatta metodologia investigativa ([Cass. pen., Sez. VI, 26 maggio 2015, n. 27100](#)).

In particolare, la Corte aveva ritenuto giuridicamente inammissibile la stessa in quanto, consentendo la captazione di comunicazioni in qualsiasi luogo si rechi il soggetto portando con sé l'apparecchio, permette l'apprensione di conversazioni senza limitazione di luogo e, quindi, contrasta non soltanto con la normativa codicistica, ma ancora prima con il precetto costituzionale di cui all'[art. 15](#) Cost. dal momento che l'unica opzione interpretativa compatibile con il richiamato dettato costituzionale è quello secondo cui l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati *ab origine* e non in qualunque luogo si trovi il soggetto.

L'ordinanza di rimessione si è posta in radicale dissenso con siffatte conclusioni, facendo in primo luogo osservare che l'esigenza di predeterminare le situazioni ambientali oggetto di captazione risulta estranea all'intercettazione a mezzo di virus informatico, in quanto la caratteristica tecnica di siffatta modalità di captazione prescinde dal riferimento al luogo, trattandosi in ipotesi di un'intercettazione ambientale "itinerante", di talché ciò che rileva è che il decreto autorizzativo sia adeguatamente motivato per giustificare le ragioni per le quali si ritiene debba utilizzarsi la metodica dell'istallazione da remoto, consentendo così una captazione dinamica. Sul versante normativo, poi, l'ordinanza ha evidenziato come un problema di compatibilità si sarebbe posto comunque soltanto rispetto al domicilio ed ai luoghi di privata dimora presi in considerazione dall'[art. 614](#) c.p. e richiamati dall'[art. 266, co. 2](#) c.p.p., per cui lo stesso sarebbe rimasto escluso dall'area operativa delineata dall'[art. 13](#), d.l. 13 maggio 1991, n. 152, convertito in [l. 12 luglio 1991, n. 203](#), dal momento che l'intercettazione tra presenti che sia disposta nell'ambito di procedimenti di criminalità organizzata è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'[art. 614](#) c.p. si stia svolgendo l'attività criminosa. Le Sezioni unite della Corte di cassazione (il riferimento è, ovviamente, a [Cass. pen., Sez. un., 1 luglio 2016, n. 26889](#)), approfondendo gli spunti tratti dall'ordinanza di rimessione e dopo avere ribadito la correttezza della qualificazione giuridica dell'attività investigativa svolta tramite agente intrusore come intercettazione di tipo "ambientale", hanno enunciato principi di diritto ben noti.

Difatti, la Corte ha statuito che:

a. deve escludersi la possibilità di compiere intercettazioni nei luoghi indicati dall'[art. 614](#) c.p., con il mezzo costituito dal captatore informatico, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'[art. 13](#), d.l. 13 maggio 1991, n. 152, convertito in [l. 12 luglio 1991, n. 203](#), non

potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'[art. 266, co. 2 c.p.p.](#), che in detto luogo "si stia svolgendo l'attività criminosa";

b. è invece consentita la captazione nei luoghi di privata dimora *ex* [art. 614 c.p.](#), pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'[art. 13d.l. 13 maggio 1991, n. 152](#).

La Corte di cassazione ha colto l'occasione per ribadire l'**adesione ad una interpretazione ampia della nozione di "criminalità organizzata"**, definizione la cui precisazione non costituisce – dicono le Sezioni unite – un mero esercizio teorico poiché da essa dipende l'applicazione delle norme processuali che si riferiscono alla categoria di reati ad essa correlata.

Ha chiarito, pertanto, che per procedimenti relativi a delitti di criminalità organizzata devono intendersi non soltanto quelli elencati nell'[art. 51](#), commi 3-*bis* e 3-*quater* c.p.p., ma anche quelli comunque facenti capo a un'associazione per delinquere *ex* [art. 416 c.p.p.](#), con esclusione del mero concorso di persone nel reato.

Si tratta di una presa di **posizione che ha destato non poche perplessità** sul versante dell'effettiva protezione dei valori di rango costituzionale che la disciplina delle intercettazioni di conversazioni e comunicazioni si presta a ledere, dal momento che la nozione estesa del concetto di criminalità organizzata, coniugandosi con l'orientamento secondo il quale i risultati delle intercettazioni telefoniche disposte per un reato rientrante tra quelli indicati nell'[art. 266 c.p.p.](#) sono utilizzabili anche relativamente ai restanti reati per i quali si procede nel medesimo procedimento, pur se per essi le intercettazioni non siano consentite, e ciò indipendentemente dal successivo esercizio dell'azione penale anche in relazione al primo reato (v., infatti, [Cass. pen., Sez. V, 29 aprile 2014, n. 17939](#)), rischia[va] di rendere agevoli forzature finalizzate a configurare la ricorrenza dei presupposti legittimanti il ricorso all'incursore informatico anche in relazione ad ipotesi solo formalmente escluse.

Grande assente nel contesto di una sentenza dai notevoli risvolti sistematici, il dovere motivazionale del giudice non ha subito rimaneggiamenti in chiave rafforzativa, essendosi la sentenza limitata a sottolineare, da un lato, l'esigenza che, nel rispetto dei canoni di proporzione e ragionevolezza a fronte della forza intrusiva del mezzo usato, la qualificazione, pure provvisoria, del fatto come inquadrabile in un contesto di criminalità organizzata, risulti ancorata a sufficienti, sicuri e obiettivi elementi indiziari che ne sorreggano, per un verso, la corretta formulazione da parte del pubblico ministero e, per altro verso, la successiva, rigorosa, verifica dei presupposti da parte del giudice chiamato ad autorizzare le relative operazioni intercettative; dall'altro lato, la generica necessità che l'installazione del captatore informatico in un dispositivo "itinerante" avvenga in forza di un provvedimento di autorizzazione – la quale, dunque, è stata ritenuta indispensabile e ricondotta alla sfera di legittimazione del giudice – adeguatamente motivato e nel rispetto delle disposizioni generali in materia di intercettazione, precisando altresì che essa costituisce una delle naturali modalità di attuazione delle intercettazioni al pari della collocazione di microspie all'interno di un luogo di privata dimora.

Il [d.l. 30 dicembre 2019, n. 161](#)

La **riforma delle intercettazioni**, come è noto, trova **applicazione rispetto ai procedimenti iscritti dall'1 settembre 2020** e, come si è già avuto modo di dire, alla luce dei plurimi differimenti e dei continui

rimaneggiamenti che hanno condotto alla definitiva veste assunta a seguito del [d.l. 30 dicembre 2019, n. 161](#) e della [legge di conversione 28 febbraio 2020, n. 7](#), il prodotto normativo consegna un assetto complessivo certamente molto meno innovativo rispetto a quello introdotto dal [d.lgs. 29 dicembre 2017, n. 216](#).

I profili di particolare novità della riforma si rinvencono proprio nella disciplina delle intercettazioni mediante il ricorso al captatore informatico.

Infatti, andando oltre la impostazione restrittiva delineata da [Cass. pen., Sez. un., 28 aprile 2016, n. 26889](#), l'[art. 266, co. 2](#) c.p.p. precisa che nei casi previsti dal co. 1 – le ipotesi di reato, cioè, rispetto alle quali è ammesso il ricorso al mezzo di ricerca della prova – è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita – negli stessi casi, quindi, e dunque in termini di generalità – anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile.

È stato mantenuto in relazione ai reati c.d. “comuni” – categoria ottenibile mediante lo scorporo dalle ipotesi generali di quelle particolari previste dall'[art. 266](#), co. 2-*bis* c.p.p. – il limite previsto rispetto ai luoghi indicati dall'[art. 614](#) c.p., di talché l'intercettazione è consentita in siffatta evenienza solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

L'[art. 266](#), co. 2-*bis* c.p.p. liberalizza invece il regime relativo alle specifiche tipologie di reati ivi compendiate, disponendo che l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre – dunque, a prescindere dalla ricorrenza del presupposto di cui al comma precedente – consentita nei procedimenti – si potrebbero definire “casi speciali” – per i delitti di cui all'[art. 51](#), co. 3-*bis* e 3-*quater* c.p.p. e, previa indicazione delle ragioni – dovrebbe trattarsi di esigenze investigative non dissimili da quelle previste dall'[art. 267, co. 1](#) c.p.p. – che ne giustificano l'utilizzo anche nei luoghi indicati dall'[art. 614](#) c.p., per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni.

Un **regime diversificato**, quindi, che subisce ulteriori articolazioni rispetto alle ipotesi di intercettazione domiciliare ed il cui elevatissimo tasso di invasività è – a stento, si è già evidenziato – bilanciato innanzitutto dal presidio garantistico costituito dall'obbligo di motivazione rinforzata che connota – anche qui in termini variegati – il contenuto del provvedimento autorizzativo del gip.

Infatti, l'[art. 267, co. 1](#) c.p.p. dispone che il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile deve indicare, qualunque sia il reato oggetto del procedimento, le ragioni che rendono necessaria – non, dunque, assolutamente indispensabile, ragione per cui il ricorso allo strumento captativo non deve costituire l'*extrema ratio* nemmeno nell'ambito dei procedimenti relativi a reati “comuni” – tale modalità per lo svolgimento delle indagini.

Se si procede per delitti diversi da quelli “speciali”, invece, l'obbligo di motivazione si estende all'indicazione dei luoghi e del tempo – anche rispetto a siffatto profilo, però, emerge la consapevolezza delle difficoltà che possono caratterizzare indicazioni correlate al carattere itinerante del supporto, di talché se ne consente una onnicomprensiva “indiretta determinazione” – in relazione ai quali è consentita l'attivazione del microfono.

Si tratta di un tentativo di rafforzamento teso a salvaguardare l'inviolabilità del domicilio mediante una sorta di tracciabilità del percorso captativo, i limiti del quale sono però colti, appunto, dallo stesso legislatore laddove si accontenta di indicazioni indirette e, quindi, potenzialmente *omnibus*.

La delicatezza e l'invasività dello strumento di captazione in discorso ha giustificato, poi, il divieto di attivazione della procedura d'urgenza di cui all'[art. 267, co. 2](#) c.p.p. nei procedimenti per reati "comuni", di talché si configura in siffatte ipotesi una riserva di giurisdizione impositiva di un obbligo di verifica giudiziale che deve esplicarsi necessariamente in via preventiva.

Una disciplina derogatoria in termini restrittivi è stata prevista, infine, in relazione al regime di utilizzazione in procedimenti diversi delle risultanze ottenute mediante il ricorso al captatore informatico, al fine di arginare situazione di libera circolazione agevolate anche da una serie di prese di posizione "aperte" della giurisprudenza.

Infatti, se l'[art. 270](#), co. 1 c.p.p. dispone, in generale, che i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'[art. 266, co. 1](#) c.p.p., il nuovo co. 1-*bis* della medesima disposizione prevede che, fermo restando quanto previsto dal co. 1 – ossia, viene ribadita la regola del divieto di utilizzazione in procedimenti diversi, e dunque l'eccezionalità della deroga costituita dai casi di utilizzabilità – 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, ma soltanto qualora risultino indispensabili – ricorrendo siffatto requisito è ovvio che siano, allo stesso tempo, rilevanti – per l'accertamento (esclusivamente) dei delitti "speciali" indicati dall'[art. 266](#), co. 2-*bis* c.p.p.

Cass. pen., Sez. V, 18 novembre 2020, n. 32428. Motivazione, sovrapposibilità ed esecuzione delle operazioni

La sentenza in discorso esamina una **vicenda captativa** la quale si colloca **al di fuori dell'ambito applicativo della nuova disciplina delle intercettazioni**, trattandosi di un procedimento penale già pendente alla data indicata poco sopra ed avente ad oggetto delitti riconducibili alla nozione giurisprudenziale di "criminalità organizzata".

Non sembra potersi dubitare, dunque, della **legittimità del ricorso al trojan** nell'ambito della procedura in cui è intervenuta la pronuncia della Suprema Corte, così come non assume rilievo centrale nell'ambito della presente analisi il profilo motivazionale concernente la ricorrenza di sufficienti, sicuri e obiettivi elementi indiziari in ordine alla ricorrenza del fatto ed alla sua inquadrabilità in un contesto di criminalità organizzata.

In relazione ad esso e su un piano generale, merita di essere richiamata la giurisprudenza di legittimità secondo la quale la motivazione dei provvedimenti autorizzativi, stante la loro natura di decreti, può essere la "minima necessaria" a chiarire le ragioni del provvedimento in ordine sia all'indispensabilità del mezzo probatorio richiesto ai fini della prosecuzione delle indagini sia alla sussistenza dei gravi indizi e, in una tale ottica, è sufficiente che il giudice indichi i dati da lui ritenuti decisivi, senza necessità di operare uno specifico esame critico dell'intero contesto sottoposto al suo esame (Cass. pen., Sez. V, 27 maggio 2004, Scardamaglia).

La sentenza, poi, risolve correttamente (e comodamente, verrebbe anche da dire!) la questione relativa all'obbligo di motivazione inerente al profilo costituito dalla necessità del ricorso allo strumento captativo, ricorrendo al criterio intertemporale del *tempus regit actum* per escludere l'applicabilità della nuova disciplina e, dunque, adagiarsi sul generalissimo obbligo di "adeguata motivazione" del provvedimento di autorizzazione richiamato dalle Sezioni unite.

Che, cambiando per un attimo prospettiva, si tratti di obblighi giustificativi "non di molto diversi da quelli imposti dal legislatore della novella" appare un'affermazione non priva di forzature, dal momento che la previsione dell'obbligo di esporre le ragioni che rendono necessario il ricorso al captatore per lo svolgimento delle indagini – previsione contenuta nell'[art. 267, co. 1 c.p.p.](#) e che proietta i propri riflessi sulla fattispecie legittimante, rendendola più complessa – presenta tratti di specificità ben più ampi e marcati rispetto alla sopra richiamata indicazione di matrice giurisprudenziale, generica e tutt'altro che rafforzativa.

L'auspicio è che la precisazione della Suprema Corte non costituisca il primo passo di un percorso di sagomatura – per mano della giurisprudenza – verso il basso dello specifico obbligo di motivazione previsto dalla riforma, con conseguente ridefinizione – anche questa volta in termini restrittivi – dei margini operativi della sanzione prevista dall'[art. 271, co. 1 c.p.p.](#) in relazione all'[art. 267 c.p.p.](#)

La sentenza della Suprema Corte si occupa anche del tema costituito dalla **sovrapponibilità di provvedimenti autorizzativi di forme diversificate di captazione su medesimi obiettivi**, concludendo nel senso della piena legittimità dei decreti che autorizzano l'intercettazione tramite captatore di bersagli già interessati da attività di intercettazione (potremmo dire) tradizionale.

Mettendo da parte le difficoltà che caratterizzano il tentativo di ricostruire il pensiero della Corte circa i rapporti tra intercettazioni tradizionali e mediante captatore – si passa, infatti, da valutazioni di omogeneità a qualificazioni di autonomia tra mezzi di ricerca della prova – il pericolo che gli interpreti hanno paventato circa un surrettizio aggiramento dei termini di durata delle intercettazioni – correlati ad autonomi provvedimenti esecutivi, fondati (si auspica, essendo stato anche sul punto poco preciso il linguaggio utilizzato dalla Suprema Corte, la quale parla ora di autorizzazione, ora di esecuzione) su plurimi provvedimenti autorizzativi – ed un sovrabbondante attentato a beni di rilievo costituzionale – in ipotesi contestualmente attaccabili mediante forme diversificate di captazione – appare quantomeno meritevole di approfondite riflessioni.

Le problematiche poste dai ricorrenti in ordine alla legittimità della fase esecutiva delle intercettazioni sono state risolte facendo riferimento agli arresti giurisprudenziali che, nel corso degli anni, hanno definito variegate questioni afferenti al segmento procedurale successivo al provvedimento autorizzativo.

L'asse portante dell'argomentare della Suprema Corte è stato costituito dal principio di tassatività delle cause di invalidità – autorevolmente ribadito in relazione proprio all'inutilizzabilità, da ultimo, da [C. cost., 21 ottobre 2020, n. 252](#) – e, dunque, dalla non estensibilità del margine operativo riferibile all'[art. 271 c.p.p.](#)

D'altra parte, la stessa [Cass. pen., Sez. un., 1 luglio 2016, n. 26889](#) aveva chiarito che l'installazione del captatore informatico in un dispositivo "itinerante" costituisce "una delle naturali modalità di attuazione delle intercettazioni al pari della collocazione di microspie all'interno di un luogo di privata dimora".

Ed allora, se da un lato la ricostruzione della Suprema Corte appare difficilmente controvertibile alla luce del sistema normativo di riferimento, dall'altro essa rischia di creare nell'ambito dell'innovato assetto normativo – il quale compendia una specifica disciplina dei diversi profili correlati all'impiego di un diversificato mezzo captativo, tuttavia sprovvista di un sia pur timido apparato sanzionatorio – zone d'ombra proprio in un frangente della sequenza captativa che, invece, deve essere attentamente monitorato al fine di evitare che il mezzo di ricerca della prova, il ricorso al quale sia stato magari legittimamente autorizzato, divenga poi l'oggetto di un'attività gestionale oscura, difficilmente ricostruibile sia sul piano soggettivo che sul terreno delle dinamiche operative.

Ma, su questo terreno, l'alternativa ad una robusta attività giurisprudenziale di tipo manipolativo non può che essere l'intervento del legislatore.