BREVI NOTE SUL RAPPORTO TRA TROJAN HORSE E LIBERTÀ DI AUTODETERMINAZIONE

Emanuele Salvatore Murone

Cass., Sez. V, 30 settembre 2020, (dep. 11 novembre 2020), n. 31604

VESSICCHELLI Presidente, MOROSINI Relatore, EPIDENDIO P.G.

Con la pronuncia in oggetto, la Corte di legittimità ribadisce che il captatore informatico non costituisce un autonomo mezzo di ricerca della prova, ma solo una particolare modalità tecnica per effettuare l'intercettazione delle conversazioni tra presenti. Di conseguenza, il *trojan horse* non può rientrare tra i metodi il cui utilizzo, per l'effetto di pressione sulla libertà fisica e morale della persona, sia vietato dall'art. 188 c.p.p., atteso che non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità.

With the current judgment, the Supreme Court reaffirms that cyber capturer is not an independent means of proof, but just one particular technical way of intercepting conversations between presents. Consequently, may not be one of the methods whose use, as a result of pressure on the person's physical and moral freedom, is prohibited by law.

SOMMARIO: 1. Il caso di specie. – 2. Il captatore informatico tra pronunce di legittimità e modifiche normative. – 2.1. L'evoluzione di legittimità e la sentenza a sezioni unite Scurato. - 2.2. La c.d. riforma Orlando (d.lgs. n. 216/2017). - 2.3. L'adozione del d.l. n. 161/2019. - 3. La giurisprudenza più recente in tema di captatore informatico. – 4. Considerazioni conclusive.

1. **Il caso di specie.**

Con l'arresto in esame, i giudici della Quinta Sezione Penale della Corte di Cassazione hanno rigettato il ricorso avverso l'ordinanza con la quale il Tribunale del Riesame di Lecce aveva confermato la misura della custodia cautelare in carcere nei confronti del ricorrente, partecipe in associazione mafiosa.

Avverso la pronuncia della Corte di merito, l'imputato ha articolato le proprie doglianze in quattro motivi di ricorso, eccependo l'inutilizzabilità dei risultati delle intercettazioni effettuate mediante l'istallazione del captatore informatico.

In particolare, secondo la prospettazione del ricorrente, l'utilizzo del captatore informatico sarebbe stato illegittimo poiché rientrante tra gli strumenti di pressione sulla libertà fisica e morale della persona, il cui uso sarebbe vietato dall'articolo 188 c.p.p.. Nello specifico, si evidenziava come il trojan horse fosse uno strumento «subdolo» di acquisizione della prova, poiché indurrebbe il soggetto intercettato all'autoinstallazione del virus, così violando il principio di autodeterminazione.

La questione viene risolta dalla Suprema Corte ritenendo che il *trojan horse* non esercita alcuna pressione

sulla libertà fisica e morale della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità.

2. Il captatore informatico tra pronunce di legittimità e modifiche normative.

Prima di analizzare la soluzione adottata dalla Corte di Cassazione, appare utile precisare brevemente quali siano i tratti caratterizzanti il c.d. *trojan horse*, anche definito «captatore informatico» o «agente intrusore».

Il c.d. *trojan horse* è un virus informatico che viene inoculato da remoto in maniera occulta nel sistema operativo di apparati informatici e che, mediante comandi a distanza, acquisisce una molteplicità di dati archiviandoli nel server cui è collegato[1].

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 che il virus usa per controllare detto dispositivo. I dati raccolti sono trasmessi, per mezzo della rete internet, in tempo reale o a intervalli prestabiliti ad altro sistema informatico in uso agli organi inquirenti.

Se le potenzialità operative dello strumento sono innegabili – rendendo di fatto possibile ascoltare tutte le conversazioni, telefoniche ed ambientali, captare il flusso di dati in entrata e in uscita, attivare il microfono, mettere in funzione la fotocamera e finanche controllare gli spostamenti – il tema dei limiti di ammissibilità si appalesa piuttosto delicato. Se appare legittimo, a prima vista, nutrire preoccupazioni per le accresciute potenzialità acquisitive dei virus informatici, suscettibili di ledere la riservatezza, la dignità e la libertà delle persone, è del pari legittimo ricordare che «solo siffatti strumenti sono, oggi, in grado di penetrare i canali criminali di comunicazione o di scambio d'informazioni (di matrice mafiosa o terroristica) utilizzati per la commissione di perniciosissimi reati contro la persona e la libertà» [2].

2.1. L'evoluzione di legittimità e la sentenza a sezioni unite Scurato.

Una compiuta disamina sul tema dei presupposti applicativi e dei limiti all'impiego del captatore informatico deve necessariamente prendere le mosse dalla pronuncia a Sezioni Unite del 28 aprile 2016, n. 26889, Scurato[3].

Nel caso di specie, la Corte di Cassazione era stata chiamata, prima delle modifiche apportate al codice di rito dal d. lgs. 216/2017, a pronunciarsi sulla necessità, o meno, di indicare nel decreto autorizzativo

dell'intercettazione a mezzo di captatore informatico i luoghi in cui sarebbe stata disposta la captazione. Per quanto qui di interesse, i motivi di doglianza risiedevano in una presunta violazione dell'art. 266, comma 2, c.p.p., posto che le intercettazioni erano state effettuate in luoghi di privata dimora[4], all'interno dei quali non vi era fondato motivo di ritenere che si stesse svolgendo l'attività criminosa, e poiché non erano stati indicati, nel provvedimento autorizzativo, i luoghi in cui l'attività captativa si sarebbe svolta. Tale ultimo motivo di doglianza trovava supporto in una pronuncia di poco precedente, a sensi della quale *«il decreto autorizzativo deve individuare, con precisione, i luoghi nei quali dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, non essendo ammissibile un'indicazione indeterminata o addirittura l'assenza di ogni indicazione al riguardo»*, al fine di non incorrere in una lettura incostituzionale dell'art. 266 c.p.p. per violazione dell'art. 15 Cost.[5]

Le Sezioni Unite si erano soffermate sul tema delle intercettazioni ambientali esclusivamente sulla base delle definizioni fornite sul punto dalla dottrina e dalla giurisprudenza, attesa l'assenza di qualsivoglia riscontro testuale nel codice di rito. Invero, l'art. 266 c.p.p. disciplinava le «intercettazioni tra presenti» senza alcun espresso riferimento all'ambiente che, invece, assumeva rilievo nel secondo periodo dell'ultimo comma del medesimo articolo, a mente del quale le intercettazioni in luogo di privata dimora erano consentite solo se ivi si stesse svolgendo attività criminosa. Mentre le intercettazioni tra presenti non necessitavano di alcuna indicazione del luogo in cui avrebbero dovuto essere svolte, dal momento che né l'art. 266 c.p.p. né la giurisprudenza della CEDU parevano orientarsi in tal senso, le intercettazioni tra presenti nei luoghi di privata dimora, invece, sarebbero state ammissibili solo se vi fosse stato motivo di ritenere che all'interno del domicilio si stesse svolgendo attività criminosa, trovando applicazione la disciplina derogatoria prevista dall'art. 13 della l. 23 luglio 1991, n. 203 [6].

Tale ultima normativa, introdotta per garantire una maggiore efficacia dell'attività investigativa in un terreno delicato quale è quello del crimine organizzato[7], avrebbe permesso di effettuare l'intercettazione domiciliare anche se non vi fosse stato motivo di ritenere che nei luoghi predetti si stesse svolgendo l'attività criminosa, in deroga al limite di cui all'art. 266, comma 2, c.p.p., a patto che il decreto autorizzativo delle intercettazioni motivasse adeguatamente il ricorso a tale modalità.

A fortiori, poi, le Sezioni Unite pongono in evidenza come l'indicazione specifica dei luoghi sia sempre risultata superflua nei delitti di criminalità organizzata, utile solamente a fini pratici per consentire agli organi di polizia giudiziaria di installare fisicamente la cimice. Non così, invece, per i restanti reati che seguono la disciplina ordinaria, relativamente ai quali l'indicazione della tipologia di ambienti è *conditio sine qua non* della legittimità delle operazioni investigative di intercettazioni in luogo di privata dimora[8].

Le ragioni di questa deroga alla disciplina ordinaria in materia di intercettazioni devono essere ricercate nella circostanza che i delitti di criminalità organizzata vengono perpetrati da associazioni criminose che si

avvalgono di una pressante forza intimidatrice e della piaga del fenomeno omertoso che rendono inattendibili le fonti di prova testimoniali, spingendo gli inquirenti a ricorrere a mezzi di ricerca della prova «a sorpresa» come le intercettazioni[9].

Con un altro passaggio, la Suprema Corte è giunta a sostenere che le caratteristiche tecniche delle intercettazioni mediante virus informatico prescindono dal riferimento al luogo, trattandosi di un'intercettazione ambientale «itinerante», e perciò ontologicamente incompatibile con l'indicazione del luogo, non potendosi imporre la captazione nel momento in cui il soggetto entra in un luogo di privata dimora. Secondo il Supremo Collegio, *«muovendo da tali premesse e volendo giungere ad un primo approdo ermeneutico, deve escludersi - de iure condito - la possibilità di intercettazioni nei luoghi indicati dall'art. 614 c.p., con il mezzo del captatore informatico, al di fuori della disciplina derogatoria di cui alla l. n. 203/1991, art. 13»*.

Quanto ai procedimenti di criminalità organizzata, precisava peraltro la Corte, che l'installazione del captatore informatico in un dispositivo itinerante, con provvedimento di autorizzazione adeguatamente motivato e nel rispetto delle disposizioni generali in materia di intercettazione, costituiva *«una delle naturali modalità di attuazione delle intercettazioni al pari della collocazione di microspie all'interno di un luogo di privata dimora»*.

La sentenza Scurato, pertanto, se da un lato ha efficacemente ritenuto che il captatore informatico fosse solo una *species* del più ampio *genus* delle intercettazioni tra presenti e non, piuttosto, un autonomo mezzo di ricerca della prova, dall'altro non è riuscita a sopire definitivamente i dubbi interpretativi sull'ammissibilità del captatore informatico: in dottrina, infatti, si temeva che l'ufficio del pubblico ministero potesse strumentalizzare l'iscrizione per il delitto associativo al solo fine di legittimare, *ex post*, l'utilizzo del mezzo di ricerca della prova[10].

2.2. La c.d. riforma Orlando (d. lgs. n. 216/2017).

Con il d. lgs. 29 dicembre 2017, n. 216 il Governo ha dato seguito alla delega legislativa attribuitagli dall'art. 1, comma 84, l. 23 giugno 2017, n. 103, i cui criteri della direttiva, almeno secondo parte della dottrina, erano così dettagliati «*da far pensare ad una veste normativa pressoché definitiva*»[11]. Si era preso atto, infatti, della lacuna normativa, e della assoluta insufficienza della disciplina codicistica in materia di intercettazioni ambientali, che rispecchiava un bilanciamento di interessi risalenti ad un momento storico nel quale si disponeva di strumenti rudimentali a confronto con le tecnologie oggi sperimentabili[12]. La disciplina in oggetto nasceva quindi da una ponderazione di interessi in gioco completamente ricalcolata, anche alla luce del principio di proporzionalità, che presidia la correttezza nel misurare il rapporto fra il grado di intrusività della specifica misura di controllo capace di incidere negativamente sui diritti di libertà dei singoli, e il livello di intensità delle garanzie legali [13].

Nonostante gli originali propositi, tuttavia, il legislatore ha dettato una disciplina piuttosto scarna e minimalista del captatore informatico, circoscrivendo l'intervento riformatore esclusivamente alle funzioni di intercettazione ambientale itinerante di cui era dotato il *trojan horse* [14].La novella in oggetto ha introdotto un nuovo periodo nell'art. 266, comma 2, c.p.p. in virtù del quale era possibile procedere all'intercettazione di comunicazioni tra presenti «*anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*»[15]. In dottrina, diversamente da quanto disposto dal legislatore delegato, si era ipotizzato di introdurre *ex novo* un art. 266-*ter* c.p.p., dedicato esclusivamente alla funzione di intercettazione virale di comunicazioni o conversazioni tra presenti[16]. Allineandosi al *dictum* delle Sezioni Unite Scurato, il legislatore ha sopito il dibattito dottrinale e giurisprudenziale che era sorto in relazione alla sussunzione dell'intercettazione itinerante nel più ampio *genus* delle intercettazioni tra presenti, dilatandone notevolmente, tuttavia, l'orizzonte applicativo. Le Sezioni Unite, infatti, avevano circoscritto «diffusamente» l'ambito di operatività del captatore informatico ai soli reati di criminalità organizzata, la cui nozione era tale da ricomprendere ogni delitto sussumibile nel modulo di incriminazione di cui all'art. 416 c.p.[17] Il legislatore, non modificando in alcun modo l'art. 266, comma 1, c.p.p. - che racchiude l'elencazione dei delitti in ordine ai quali è possibile procedere con il mezzo di ricerca della prova «tradizionale» - e non specificando alcuna deroga nel comma 2 del medesimo articolo, ha ritenuto preferibile estendere il catalogo dei reati per i quali era possibile procedere alla captazione itinerante, allargando così l'ambito applicativo dell'istituto in esame rispetto al regime previgente[18].

Il legislatore si discosta dal solco tracciato dal Supremo Collegio anche in relazione alla possibilità di effettuare intercettazioni ubiquitarie in luogo di privata dimora, al di fuori della disciplina derogatoria prevista per i delitti di criminalità organizzata di cui all'art. 13 d. l. n. 152/1991. Invero, secondo la Cassazione non sarebbe stato possibile per il giudice delle indagini preliminari predeterminare i luoghi di privata dimora in cui il dispositivo elettronico sarebbe andato a trovarsi e, di conseguenza, elencarli nel decreto autorizzativo. Il legislatore, al contrario, effettua una scelta diametralmente opposta, dal momento che ritiene ammissibile la captazione domiciliare nel caso in cui vi sia fondato motivo di ritenere che ivi si stesse svolgendo attività criminosa[19]. L'art. 266, comma 2, c.p.p. non ha subito infatti alcuna variazione ed è posto in continuità con il precedente periodo che ammette l'intercettazione captativa.

In netta cesura con quanto sancito dalla sentenza Scurato, la novella legislativa prevede l'indicazione, anche indiretta, da parte del giudice dei luoghi e del tempo in cui è consentita l'attivazione del microfono. La suddetta pronuncia, infatti, riteneva che l'indicazione del luogo fosse una mera modalità attuativa, volta a fornire indicazioni per l'esecuzione dell'intercettazione. Al contrario, il legislatore ha ritenuto preferibile l'indicazione del luogo - insieme a quella del tempo - tra i presupposti del provvedimento autorizzativo (art. 267, comma 1, c.p.p.), i quali sono garantiti da un'espressa comminatoria di inutilizzabilità del risultato intercettivo (art. 271, comma 1, c.p.p.): il tutto al verosimile fine di effettuare un bilanciamento tra le esigenze

investigative e quelle private, garantendo un controllo successivo da parte del soggetto destinatario ignaro della captazione.

Le considerazioni appena svolte, tuttavia, non trovavano applicazione ai casi in cui si procedesse per uno dei gravi delitti elencanti nell'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., ai quali si applicava la disciplina derogatoria di cui all'art. 13 del d.l. 152/1991. Invero l'art. 266, comma 2-*bis*, c.p.p., consentiva in ogni caso l'intercettazione itinerante, anche se avveniva in un luogo di privata dimora, se si fosse proceduto per uno dei reati testé citati, circoscrivendo così l'ambito applicativo in precedenza disegnato dalle Sezioni Unite Scurato, che comprendeva qualsiasi delitto riconducibile al protocollo di tipicità soggettiva dell'art. 416 c.p.

Infine, ai sensi della modifica introdotta nell'art. 267 c.p.p., sono stati equiparati ai suddetti reati di anche quelli commessi contro la pubblica amministrazione (per i quali è prevista la pena della reclusione non inferiore nel massimo a 5 anni), per i quali sarebbero state applicabili le disposizioni di cui all'art. 13 del d.l. 13 maggio 1991, n. 152. La *ratio* andrebbe presumibilmente rintracciata nell'opacità che caratterizza tali crimini, nei quali il rischio di punizione generale, che coinvolge maggiori concorrenti, crea, proprio come accade per le associazioni a delinquere, una rigida impenetrabilità nel crimine, perforabile solo mediante una forte intrusività[20].

2.3. L'adozione del d. l. n. 161/2019.

Il 1° settembre 2020, dopo due successivi interventi riformativi (il d. lgs. 29 dicembre 2017, n. 216 ed il d.l. 30 dicembre 2019, n. 161 convertito dalla l. 28 febbraio 2020, n. 7) ed una lunga serie i rinvii (da ultimo, al 31 agosto 2020) è entrata in vigore la tanto attesa riforma delle intercettazioni telefoniche.

Sottolineando solo gli aspetti che interessano nel caso di specie, l'utilizzazione del captatore informatico è stata estesa a tutti i reati per i quali è possibile eseguire le intercettazioni. Il legislatore, dunque, con l'introduzione del comma 2-*bis* nell'art. 268 c.p.p., ha dato copertura normativa all'utilizzo di tale strumento di captazione finora non disciplinato, sia rispetto alle conversazioni telefoniche e ambientali, che alla messaggistica non vocale.

Tre sono i regimi applicativi dello strumento di cui si tratta a seconda che si proceda: a) per i reati previsti dall'art. 51, comma 3-*bis* e 3-*quater*, c.p.p.; b) per i reati con pena massima non inferiore a cinque anni contro la pubblica amministrazione commessi da pubblici ufficiali o incaricati di pubblico servizio; c) per i reati comuni.

Con riferimento ai reati di cui ai commi 3-*bis* e 3-*quater* dell'art. 51 c.p.p., il legislatore ha sostanzialmente recepito le indicazioni fornite dalla citata sentenza Scurato. Premesso che le intercettazioni tramite captatore

informatico su dispositivo mobile sono assimilabili ad una intercettazione ambientale, nessun limite particolare è previsto per questa categoria di reati dall'art. 266, comma 2-*bis*, c.p.p. La nuova tecnologia, in particolare, potrà essere usata anche qualora il dispositivo mobile capti conversazioni nei luoghi di cui all'art. 614 c.p., trovando applicazione la disciplina di cui all'art. 13 del d.l. n. 151/1991 che, in deroga ai presupposti fissati dall'art. 266, comma 2, c.p.p., permette l'acquisizione di conversazioni che si svolgano nei luoghi di privata dimora senza richiedere necessariamente che in essi vi sia attività criminosa in atto. Tuttavia, ai sensi dell'art. 267, comma 1, c.p.p., il decreto autorizzativo deve indicare i motivi che rendono necessaria tale modalità per lo svolgimento delle indagini. Dal confronto tra la nuova disciplina e quella previgente, emerge come il rigido rinvio operato dall'art. 268, comma 2-*bis*, c.p.p. ai soli reati di cui ai commi 3-*bis* e 3-*quater* dell'art. 51 c.p.p., non sembrerebbe contemplare il reato associativo non qualificato di cui all'art. 416 c.p.

Quanto, invece, ai reati contro la pubblica amministrazione è ora possibile eseguire le intercettazioni di comunicazioni tra presenti mediante captatore informatico anche luoghi indicati dall'art. 614 c.p.[21] ed anche qualora in essi non vi sia un'attività criminosa in atto. In questa ipotesi, tuttavia, il decreto autorizzativo deve indicare tanto le motivazioni che, ai sensi dell'art. 267, comma 1, c.p.p., rendono necessaria tale modalità per lo svolgimento delle indagini, quanto quelle che, ai sensi dell'art. 266, comma 2-*bis*, c.p.p., ne giustificano l'utilizzo nei citati luoghi di privata dimora.

Infine, per quanto concerne i reati comuni, il captatore informatico potrà sempre essere impiegato a condizione che le conversazioni non avvengano nei luoghi di privata dimora di cui all'art. 614 c.p. altrimenti l'intercettazione è consentita - in forza del principio contenuto nell'art. 266, comma 2, c.p.p. - solo se vi sia fondato motivo di ritenere che ivi si stia svolgendo attività criminosa. In ogni caso, il decreto del giudice che autorizza l'intercettazione tra presenti mediante captatore informatico deve contenere, ai sensi dell'art. 267, comma 1, c.p.p., oltre l'indicazione delle ragioni che rendono necessaria tale modalità di svolgimento delle indagini, anche quella dei luoghi e del tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono. Lo scopo della previsione è quello di evitare l'utilizzo del nuovo strumento tecnologico possa eludere quanto statuito dall'art. 266, comma 2, c.p.p. che - si ribadisce - per la legittimità delle captazioni in luoghi domiciliari presuppone che sia in atto attività criminosa.

3. **Il captatore informatico quale prova tipica.**

Effettuata questa doverosa e sintetica premessa circa l'evoluzione normativa che ha interessato la materia delle intercettazioni effettuate tramite captatore informatico, si può affermare che la Suprema Corte, con la pronuncia in oggetto, ha condivisibilmente respinto le censure sollevate dal ricorrente, allineandosi ai principi espressi dalla sentenza Scurato.

L'importanza della pronuncia si desume dalla delicatezza della questione trattata: per la prima volta, infatti, si è ipotizzato che il *trojan horse* possa essere qualificato come strumento idoneo ad influire sulla libera determinazione del soggetto.

Appare utile preliminarmente richiamare il disposto di cui all'art. 188 c.p.p., ai sensi del quale «*non possono esser utilizzati, neppure con il consenso della persona interessata, metodi o tecniche idonei ad influire sulla libertà di autodeterminazione o ad alterare la capacità di ricordare e valutare i fatti*». La *ratio* di tale norma va rintracciata nell'intento del legislatore di delimitare l'ambito di operatività delle prove atipiche, ritenendo inammissibili procedure o mezzi che confliggano con la libertà morale della persona. La dottrina ha individuato la ragion d'essere di tale divieto probatorio osservando che non solo occorre distinguere tra «giusto processo» e «giusto procedimento», ma occorre focalizzarsi anche (e soprattutto) su un «giusto metodo probatorio», atteso che metodi di accertamento probatorio particolarmente invasivi possono alterare le capacità di valutare i fatti o la capacità di ricostruzione degli avvenimenti[22].

La portata applicativa dell'art. 188 c.p.p., tuttavia, può essere colta appieno esclusivamente se letta, in combinato disposto, con il successivo art. 189 c.p.p., il quale impone al giudice di ritenere illegittima la prova atipica che sia idonea a pregiudicare la libertà morale senza, tuttavia, dettare alcuna «*aprioristica preclusione*»[23] ma, al contrario, permettendo un continuo adeguamento del processo penale allo sviluppo tecnologico. Pertanto, quando nel processo penale sussiste la necessità di confrontarsi con una prova atipica, spetterà al giudice il compito di valutarla alla stregua dei due parametri indicati dall'art. 189 c.p.p.: l'idoneità della prova a garantire l'accertamento dei fatti e l'assenza di un pregiudizio alla libertà morale della persona.

Il ricorrente, con il primo motivo di ricorso, ha dedotto l'illegittimità delle intercettazioni effettuate tramite captatore informatico, sostenendo che si tratti di una modalità «subdola» di acquisizione poiché indurrebbe il soggetto intercettato all'autoinstallazione, con costi – peraltro - a carico del suddetto. Ad avviso del ricorrente, dunque, l'utilizzazione del *trojan horse* violerebbe il principio di autodeterminazione scolpito nell'art. 188 c.p.p.

La Corte ha ritenuto infondata la doglianza. Il giudice di legittimità, *in primis*, ha colto l'occasione per ripercorrere i principi giurisprudenziali consolidatisi in materia, a partire dalla sentenza Scurato, con la quale è stato chiarito che «*il fondamento normativo cui fare riferimento, de iure condito, va rinvenuto nella disciplina delle intercettazioni "tra presenti" e, specificamente, negli artt. 266, 267 e 271 c.p.p. con le deroghe previste, per i reati di criminalità organizzata, dal d.l. n. 152/1991, art. 13, convertito dalla l. n. 252/1991*»[24]. La Corte, pertanto, allineandosi all'orientamento giurisprudenziale espresso nella sentenza Scurato, non solo conclude che la disciplina in tema di intercettazioni ambientali è omogenea a quella delle intercettazioni disposte tramite captatore informatico, ma correttamente afferma che tale ultima disciplina trovava cittadinanza

all'interno del nostro ordinamento già prima della modifica codicistica operata dalla riforma Orlando.

Affermazione di centrale importanza, nell'economia della sentenza in commento, è quella per cui «*il captatore informatico non è altro che uno strumento messo a disposizione dalla moderna tecnologia, attraverso il quale è possibile effettuare un'intercettazione ambientale*».

Ma esclude la Corte che l'utilizzo del captatore informatico costituisca una prova atipica o un aggiramento delle regole dalla prova tipica, «*poiché, già prima dell'entrata in vigore della specifica disciplina contenuta nel D.Lgs. n. 216 del 2017 (che invece ne estende l'applicabilità, a determinate condizioni, anche ai reati comuni), l'impiego del trojan horse, quale mezzo per eseguire la captazione delle conversazioni tra presenti, era regolamentato dagli artt. 266, 267 e 271 c.p.p. – interpretati in senso restrittivo dalle Sezioni Unite Scurato, che hanno bandito tale strumento per tutti i reati comuni, al fine di scongiurare in radice il pericolo di una incontrollabile intrusione nella sfera privata delle persone – con la speciale deroga, nella specie operante, di cui al D. L. n. 152 del 1991, art. 13*».

Sul piano giuridico, la Corte di legittimità ha statuito la tipicità del captatore informatico quale mezzo di prova, affermando che «*lungi dal costituire un autonomo mezzo di prova, è solo una particolare modalità tecnica per effettuare l'intercettazione delle conversazioni tra presenti*».

A conferma della correttezza di tale esegesi, le considerazioni svolte dal ricorrente in ordine alla riconducibilità del captatore informatico nel novero delle prove atipiche, osserva la Corte, sarebbero smentire proprio dal dettato normativo di cui all'art. 266, comma 2, c.p.p., il quale rende evidente come il *trojan horse* sia solo uno dei possibili modi attraverso il quale si può effettuare l'intercettazione di conversazioni tra presenti.

Sul punto, attenta dottrina ha osservato che l'assenza di una precisa regolamentazione della materia non consente di ritenere 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.) [25]. Ciò per due ordini di ragioni. In primo luogo, perché talune attività sono riconducibili a strumenti di ricerca della prova già disciplinati dalla legge (segnatamente, l'attivazione tramite virus informatico della telecamera di cui è dotato un dispositivo elettronico è riconducibile alla videoripresa, consentita nei limiti specificati dalla nota sentenza Prisco [26]; l'acquisizione delle comunicazioni che passano attraverso dispositivi elettronici collegati a sistemi di messaggistica *online* è invece riconducibile alla intercettazione telematica disciplinata dall'art. 266-bis c.p.p.) [27]. 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.).

La Cassazione ha dunque ritenuto che «*il trojan horse non esercita alcuna pressione sulla libertà fisica e morale*

della persona, non mira a manipolare o forzare un apporto dichiarativo, ma, nei rigorosi limiti in cui sono consentite le intercettazioni, capta le comunicazioni tra terze persone, nella loro genuinità e spontaneità», così escludendo la riconducibilità del captatore informatico tra i metodi e le tecniche idonee ad influire sulla libertà di determinazione del soggetto, rientranti nell'operatività del divieto di cui all'art. 188 c.p.p.

Tale assunto della Suprema Corte si allinea a quanto sostenuto dalla dottrina maggioritaria, secondo cui l'inoculazione del *trojan horse* nel dispositivo bersaglio soddisfa pienamente i requisiti disposti nell'art. 189 c.p.p. Il captatore informatico, infatti, permette di raccogliere una pluralità di elementi probatori la cui utilità per l'accertamento dei fatti è indubbia e, inoltre, per quanto concerne la tutela dell'integrità morale della persona, proprio la natura ingannevole del virus trojan garantisce che il processo volitivo dell'indagato si formi in assenza di alcun condizionamento esterno[28]. Pertanto, proprio l'essenza «subdola», perché segreta, del captatore informatico rappresenta la maggior 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.

Secondo altra dottrina, invece, l'inoculazione del captatore grazie alla collaborazione inconsapevole del destinatario, che viene tratto in inganno, violerebbe 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, compromettendo inevitabilmente la libertà morale dell'individuo[29].

Né può ritenersi, prosegue il Supremo Collegio, che nell'eventualità in cui lo strumento captativo in oggetto consentisse l'intercettazione di conversazioni presidiate dalla sanzione dell'inutilizzabilità (come quelle intercorrenti tra l'imputato ed il suo difensore) o producesse esiti lesivi per la dignità umana, tali situazioni possano incidere «a monte» sulla legittimità del decreto autorizzativo, quanto, piuttosto, «a valle», poiché altrimenti si rischierebbe di far ricadere nell'onere motivazione del giudice un requisito non previsto dalla legge. D'altro canto, sostiene la Corte, tali situazioni patologiche ricevono adeguata e puntale protezione nell'art. 271 c.p.p., a mente del quale non sarebbero utilizzabili le risultanze di specifiche intercettazioni che abbiano violato precisi divieti di legge o che, nelle loro modalità di attuazione o nei loro esiti, ledano i diritti della persona o la sua dignità.

Esaurito dunque il percorso logico-argomentativo, la Corte enuncia il seguente principio di diritto: *«va escluso che il captatore informatico possa inquadrarsi tra i metodi o le tecniche idonee ad influire sulla libertà di determinazione del soggetto, come tali vietati dall'art. 188 c.p.p.».*

La sentenza affronta poi due ulteriori questioni.

Con il secondo motivo di ricorso il ricorrente sosteneva che il decreto autorizzativo avrebbe dovuto indicare, a pena di inammissibilità, i luoghi in cui l'intercettazione doveva avvenire, condizione, tuttavia, che non

sarebbe stata assolta nel caso di specie.

Tale doglianza, osservano i giudici di legittimità, non è condivisibile poiché *«la necessità dell'indicazione di uno specifico luogo – quale condizione di legittimità dell'intercettazione – non risulta imposta né dall'art. 266 c.p.p., 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 dalla giurisprudenza della Corte EDU»*.

Ne consegue, dunque, che debbano ritenersi legittime le intercettazioni «tra presenti» eseguite a mezzo di captatore informatico installato su un dispositivo portatile, nell'ambito dell'attività investigativa svolta in relazione a procedimenti di criminalità organizzata e ciò prescindendo dalla preventiva individuazione ed indicazione dei luoghi in cui la captazione deve essere espletata. Il legislatore, infatti, in relazione ai delitti di criminalità organizzata ha dato una precisa e significativa indicazione laddove ha escluso, per le intercettazioni tra presenti in luogo di privata dimora, l'operatività del requisito autorizzativo che l'art. 266 c.p.p., comma 2, secondo periodo, richiede per tutte le altre tipologie di intercettazioni. A ben vedere, il comma 2 dell'art. 266 c.p.p. impone unicamente che le intercettazioni effettuate nei luoghi di privata dimora siano consentite «*solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa*»[30].

Con il terzo motivo, invece, il ricorrente affermava che le intercettazioni effettuate mediante captatore informatico non sarebbero consentite poiché non previste - all'epoca dei fatti - dal codice di rito. Tale strumento, infatti, sarebbe stato disciplinato per la prima volta con il d. lgs. n. 216 del 2017 attraverso norme non ancora entrate in vigore nel momento in cui vennero compiuti i fatti.

Tale doglianza è infondata. Da un punto di vista strettamente temporale, osserva il Collegio, è pacifico che al momento dell'esecuzione dell'attività di intercettazione, non era vigente la specifica disciplina dettata dal legislatore per il *trojan horse* con il d. lgs. n. 216/2017, applicabile ai soli procedimenti penali iscritti dal 1 settembre 2020. La Corte, trovando sicuro ancoraggio nel principio del *tempus regit actum*, esclude categoricamente che la riforma delle intercettazioni possa applicarsi in maniera retroattiva, ragion per cui, quando si procede per un reato di criminalità organizzata commesso antecedentemente al 1 settembre 2020, troverà applicazione la disciplina delle intercettazioni «tra presenti» di cui agli artt. 266, 267 e 271 c.p.p., con la specifica deroga prevista per i delitti di criminalità organizzata dal d. l. n. 151/1991, art. 13, convertito dalla l. n. 203/1991[31].

4. **Considerazioni conclusive.**

La tesi sostenuta dalla Suprema Corte per cui il captatore informatico è uno strumento di per sé lecito

appare condivisibile, attesa l'espressa riconducibilità delle conversazioni captate tramite *trojan horse* nell'alveo delle intercettazioni tra presenti di cui all'art. 266, comma 2, c.p.p..

La Quinta Sezione, pertanto, dirime la questione portata alla sua attenzione sostenendo che il *trojan horse*, lungi dal costituire un autonomo mezzo di ricerca della prova, costituisce solo una particolare modalità tecnica per effettuare l'intercettazione delle conversazioni tra presenti, la cui cittadinanza all'interno del nostro ordinamento è da rinvenire in un momento antecedente alla sua esplicita previsione da parte del legislatore, dapprima con la riforma Orlando, e, da ultimo, con il d.l. 30 dicembre 2019, n. 161.

Parte della dottrina non ha mancato di osservare che il Supremo Collegio, propendendo per la tipicità del captatore informatico, si sarebbe svincolata dall'affrontare il delicato tema dei connessi limiti costituzionali della prova atipica: riserva di legge, riserva di giurisdizione e la tutela del domicilio informatico, quest'ultimo sussumibile sotto il catalogo delle libertà fondamentali di rilievo costituzionale[32].

L'equilibrio, dunque, cui sarebbe pervenuta la Corte presenterebbe il carattere della precarietà, in considerazione della crescente difficoltà che si riscontra nel coniugare le esigenze investigative oramai digitali con i diritti costituzionalmente rilevanti, primo fra tutti l'art. 14 Cost..

Tale assunto, tuttavia, si espone ad una serie di rilievi critici, atteso che la correttezza del bilanciamento tra valori costituzionali dipende dall'effettiva possibilità di comprimere le libertà fondamentali.

Nell'ambito dei procedimenti aventi ad oggetto i c.d. «reati comuni» sono proprio le considerazioni sulla struttura del mezzo probatorio a fare emergere un profilo di incompatibilità fra l'utilizzo dello strumento tecnico del captatore informatico e l'applicazione della disciplina sulle intercettazioni, atteso che nell'ambito di tali procedimenti non si riuscirebbe a dare attuazione alla clausola prevista dall'art. 266, comma 2, c.p.p. a tutela del domicilio e posto che, se anche fosse tecnicamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione ove quest'ultimo facesse ingresso in luogo di privata dimora, ne risulterebbe comunque impedito il controllo dell'organo giudicante al momento dell'autorizzazione.

Lo scenario, tuttavia, cambia decisamente in relazione ai delitti di criminalità organizzata. Per tali più gravi delitti, infatti, è certamente ragionevole pensare che il legislatore - in considerazione dell'eccezionale gravità e pericolosità delle minacce derivanti alla società e ai singoli dalle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di ingenti risorse finanziare - abbia voluto operare uno specifico bilanciamento di interessi, optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio.

In definitiva, da tali considerazioni discende che l'attuale disciplina del *trojan horse* non lede i diritti inviolabili sanciti nella carta costituzionale (art. 2, 14 e 15 Cost; art. 8 C.E.D.U.), ma garantisce, nell'ambito della rigorosa

cornice dei delitti di criminalità organizzata, il rapporto di proporzionalità diretta fra il grado di intrusività della specifica misura e il livello di intensità delle garanzie legali. Tale principio, del resto, è diretta conseguenza della circostanza per cui le intercettazioni di comunicazioni sono un mezzo di ricerca della prova funzionale al soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost., con il quale il principio di inviolabilità del domicilio previsto dall'art. 14 Cost. e quello di segretezza di qualsiasi forma di comunicazione previsto dall'art. 15 Cost., devono coordinarsi, subendo una necessaria compressione [33].

[1] P. TONINI, *Diritto processuale penale*, Milano, 2020, p. 276.

[2] GIUSEPPE LA CORTE, "*Il trojan: le intercettazioni nell'era digitale a contrasto con la criminalità organizzata*", in Giurisprudenza Penale, 2017.

[3] Cass. Pen., S. U. 28.4.2016, n. 26889, Scurato, in *CED Cass.* n. 266905-266906.

[4] Sulla nozione di «privata dimora» si veda da ultimo Cass., S.U., 22.6.2017, n. 31345, in CED n. 270076, che, chiamata a pronunciarsi sull'estensione della detta locuzione in un caso di furto in abitazione ex art. 624 bis c.p., ha sottolineato come detti luoghi siano quelli "*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, compreso quelli destinati ad attività lavorativa o professionale*".

[5] Cass. pen., Sez. VI, 26.5.2015, n. 27100, Musumeci, in C.e.d. Cass., Rv. 265655. Questa pronuncia adduceva a conforto della soluzione, la giurisprudenza che ammette la variazione del luogo in cui si devono svolgere le intercettazioni «solo se rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata» (tra le molte, cfr. Cass. pen., 11.12.2007, Sitzia, in C.e.d., n. 239634).

[6] C. PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di Stato"*, in Dir. pen. cont. riv. trim., 2017 (1), p. 80. Secondo l'Autore, la disciplina derogatoria prevista dall'art. 13 d.l. 152/1991 offre "un aggancio normativo sufficientemente solido", tuttavia le ingerenze nella sfera intima del soggetto, con l'utilizzo del virus di Stato, sono ben maggiori rispetto a un'intercettazione "classica" tra presenti. Inoltre, vi sarebbe in ogni caso un problema di compatibilità costituzionale dell'interpretazione giurisprudenziale con il principio della riserva di legge.

[7] La sentenza Scurato ha limitato la portata del captatore informatico ai reati di criminalità organizzata, ed in particolare ha fornito una nozione ampia di "criminalità organizzata" ovvero ha chiarito che l'utilizzo del mezzo di ricerca della prova è consentito "*...non solo ai delitti elencati nell'art. 51 c. 3 bis e 3 quater c.p.p. ma anche quelli comunque facenti capo a un'associazione per delinquere ex art. 416 bis c.p., correlata alle attività più*

diverse, con esclusione del mero concorso di persone".

[8] Si veda, *ex multis*, Cass. pen., Sez. I, 25.2.2009, n. 11506, Molè; Cass. pen., Sez. II, 8.4.2014, n. 17894, Alvaro.

[9] A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 150.

[10] 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., fasc. 3/2017, p. 177 ss.

[11] D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in Jusonline, 3, 2017, p. 383.

[12] P. BRONZO, *L'impiego del trojan horse informatico nelle indagini penali*, in Rivista italiana per le Scienze Giuridiche, (8) 2017, p. 333.

[13] M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in Dir. pen. cont., Riv. trim., 2014 (3/4), 144.

[14] G. SPANGHER, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in Giur. penale web, 2018, n.1. Si veda, inoltre, G. GIOSTRA - R. ORLANDI, *Nuove norme in tema di intercettazioni, Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p. 290. Sul punto anche 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, Padova, 2017, 571.

[15] Ai sensi del novellato art. 266, comma 2, c.p.p. *"negli stessi casi [di cui al primo comma] è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile".*

[16] D. CURTOTTI, op. cit., p. 383.

[17] *"Per reati di criminalità organizzata devono intendersi non solo quelli elencati nell'art. 51 c.p.p., commi 3-bis e 3-quater, ma anche quelli comunque facenti capo a un'associazione per delinquere, ex art. 416 c.p., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato"* (Cass. Pen., SS. UU. 28 aprile 2016, n. 26889, Scurato, § 16, in *CED Cass.* n. 266905-266906).

[18] In altre parole, «evidente, dunque, l'asimmetria tra ambito di ammissibilità che appaiono come cerchi intersecanti: da un lato, la scelta legislativa di restringere in numero di reati per l'accertamento dei quali è consentito il ricorso al captatore informatico [...]; dall'altro lato, tuttavia, il legislatore delegante fa rientrare dalla finestra ciò che le sezioni unite sembravano aver fatto uscire dalla porta principale, ossia la possibilità di impiegare il captatore informatico quando si procede per reati "comuni"» (M. TORRE, *Il captatore*

informatico nella legge delega 23 giugno 2017, n. 103, in Il captatore informatico, Nuove tecnologie investigative e rispetto delle regole processuali, Milano, 2017, p. 438).

[19] Precisa T. ALESCI, *Le intrusioni inter praesentes*, in L'intercettazione di comunicazioni, Cacucci, Bari, 2018, p. 77, che *"il fondato motivo di ritenere non postula che detta attività debba essere stata effettivamente sussistente, dovendosi considerare sufficiente, sulla base del dato normativo [...], che dell'attività in questione possa, con giudizio ex ante ragionevolmente ritenersi la sussistenza dell'emanazione del provvedimento di autorizzazione all'effettuazione delle operazioni".*

[20] L'art 6 d.lgs. n. 216/2017 dispone che *"nei procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p., si applicano le disposizioni di cui all'art. 13 del decreto-legge 13 maggio 1991, n.152, convertito con modificazioni dalla legge 12 luglio 1991, n. 203".*

[21] Si veda art. 2, comma 1, lett. c, d.l. 161/2019: all'articolo 266, al comma 2-bis, le parole "*e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4*" sono sostituite dalle seguenti: "*e 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, determinata a norma dell'articolo 4".*

[22] Come osservato da C. FANUELE, *"La ricostruzione del fatto nelle investigazioni penali"*, CEDAM, 2012, pag. 5.

[23] G. CONSO-V. GREVI-M. BARGIS, *Compendio di procedura penale*, VII ed., Padova, 2014, p. 326.

[24] Il captatore informatico è stato definito dalla giurisprudenza, pressoché unanime, quale strumento attraverso cui esperire un mezzo di ricerca della prova, ossia l'intercettazione di conversazioni tra presenti: Cass., S.U., 28.4.2020, n. 26889; Sez. V, 20.10.2017, n. 48370; Sez. VI, 13 giugno 2017, n. 36874.

[25] P. BRONZO, *L'impiego del trojan horse informatico nelle indagini penali*, in Rivista italiana per le Scienze Giuridiche, (8) 2017, p. 347. F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in Rev. brasile ira dir. proc. pen., 2017, p. 485 ss.

[26] Cass., S.U., 28.3.2006, PRISCO, *in Riv. it. dir. e proc. pen.,* 2006, 1537.

[27] Cass.pen., 10 novembre 2015, Guarnera, in *Arch. pen*., 2016 (1), p. 212 s., con nota di A. Testaguzza, Chat BlackBerry: *sistema* "pin-to-pin".

[28] M. TORRE, *Il captatore informatico, Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, p. 69.

[29] Così, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli,

Torino, 2018, p. 238.

[30] In P. BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, 2002, si sostiene che "*la disposizione in esame non richiede che la suddetta attività debba essere effettivamente sussistente ma che attraverso un giudizio ex ante, nel momento dell'emanazione del provvedimento autorizzativo delle intercettazioni, ragionevolmente può ritenersi che in uno dei luoghi di cui l'art. 614 c.p. si stia svolgendo l'attività criminosa*".

[31] Analogamente, si veda Cass. pen., Sez. V, 24.9.2020, n. 32426.

[32] *Ex plurimis*, si veda L. Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardai dei diritti fondamentali, Dalla Sentenza Scurato alla riforma delle intercettazioni*, in D.P.C., (1)/2018.

[33] Cass. pen., Sez. II, n. 21644 del 18.02.2013, Badagliacca, Rv. 255541; Cass. pen., Sez. II, n. 38716 del 02.10.2007, Biondo, Rv. 238108; Cass. pen., Sez. IV, n. 47331 del 28.09.2005, Cornetto, Rv. 232777; Cass. pen., Sez. VI, n. 4397 del 10.11.1997, Greco, Rv. 210062).