35010-20

REPUBBLICA ITALIANA
In nome del Popolo Italiano
LA CORTE SUPREMA DI CASSAZIONE
QUINTA SEZIONE PENALE

Composta da:

MARIA VESSICHELLI	- Presidente -	Sent. n. sez. 683/2020
BARBARA CALASELICE		CC - 30/09/2020
IRENE SCORDAMAGLIA		R.G.N. 14172/2020
ELISABETTA MARIA MOROSINI		
MATILDE BRANCACCIO	- Relatore -	

ha pronunciato la seguente

SENTENZA

sul ricorso proposto da:
MONACO STEFANO nato a LECCE il 04/07/1990

avverso l'ordinanza del 20/03/2020 del TRIBUNALE DEL RIESAME di LECCE

udita la relazione svolta dal Consigliere MATILDE BRANCACCIO;

sentite le conclusioni del Sostituto Procuratore Generale TOMASO EPIDENDIO che ha concluso per il rigetto del ricorso.

udito il difensore, avvocato ALESSANDRO STOMEO, che si riporta ai motivi di ricorso ed insiste per l'accoglimento dello stesso.

RITENUTO IN FATTO

1. Il Tribunale del Riesame di Lecce, con provvedimento del 20.3.2020, ha confermato l'ordinanza del GIP del Tribunale di Lecce del 12.2.2020 emessa nei confronti di Vito Penza per il reato di partecipazione ad associazione finalizzata al traffico di stupefacenti, confermando, altresì, la misura cautelare già disposta dal GIP della custodia cautelare in carcere.

2. Avverso l'ordinanza del Riesame propone ricorso l'indagato, tramite il difensore avv. Pantaleo Cannoletta, deducendo quattro diversi motivi con cui censura il provvedimento.

2.1. Il primo argomento eccepito evidenzia violazione di legge processuale in relazione all'inutilizzabilità delle intercettazioni sulle quali si fonda l'intera costruzione della gravità indiziaria in fase cautelare.

La difesa ribadisce due profili di illegittimità delle intercettazioni realizzate tramite captatore informatico installato sui telefoni cellulari di Stefano Monaco e Antonio Leto, già prospettati nei motivi di riesame.

Anzitutto, si evidenzia la fraudolenza della modalità di installazione del virus cd. *trojan* attraverso il quale è stato possibile attuare l'intercettazione, fraudolenza che ha richiesto la collaborazione dello stesso soggetto intercettato, inconsapevole ed ingannato.

Tale modalità ingannevole e subdola risulta illegittima poiché ciò che l'ordinamento consente è solo l'attività occulta di apprensione del flusso di informazioni (l'intercettazione in sé delle conversazioni) mentre non può ritenersi liceizzata la frode strumentale all'attivazione dell'intercettazione, pena la violazione degli artt. 2 e 15 della Costituzione e dei diritti fondamentali da tali disposizioni garantiti.

I risultati delle intercettazioni adottate con tali modalità fraudolente funzionali all'installazione del captatore informatico sono, pertanto, inutilizzabili.

Un secondo profilo di illegittimità delle intercettazioni che hanno coinvolto il ricorrente, da cui discenderebbero analogamente conseguenze di inutilizzabilità dei risultati ottenuti, si individua nell'illecito utilizzo del dispositivo telefonico degli stessi indagati e dell'energia da questi acquistata di volta in volta per la ricarica delle batterie del cellulare in loro possesso, beni di esclusiva proprietà dei "bersagli" delle operazioni investigative, con conseguente violazione del diritto di proprietà costituzionalmente tutelato dall'art. 42 della nostra Carta fondamentale.

2.2. Il secondo motivo di censura argomenta violazione di legge processuale in relazione agli artt. 191 e 271 cod. proc. pen., nonché manifesta illogicità della motivazione del provvedimento impugnato.

Il ricorrente, in sostanza, censura l'interpretazione della disciplina autorizzatoria delle intercettazioni mediante captatore informatico per i reati di criminalità organizzata, che, dalla sentenza delle Sezioni Unite n. 26689 del 2016, Scurato, in poi, si è diffusa nella giurisprudenza, avuto riguardo alla non necessità di indicare il luogo ove avverranno le conversazioni "obiettivo".

A giudizio della difesa, le disposizioni vigenti, ed in particolare l'art. 266, comma 2, cod. proc. pen. e l'art. 13 d.l. n. 152 del 1991, conv. in legge n. 203 del 1991, non consentono di leggere l'autorizzazione all'intercettazione tramite "trojan" in modo così ampio, tale da far derivare dalla necessaria "dinamicità" del mezzo di captazione – che segue costantemente l'obiettivo – la non necessità di offrire indicazioni sui luoghi nei quali si svolgeranno le conversazioni che si andranno ad intercettare.

Il sistema, invece, libera l'autorizzazione all'intercettazione ambientale, anche mediante virus informatico, solo dall'obbligo di motivare sul fatto che nei luoghi di privata dimora si stia svolgendo l'attività criminosa, ma non da quello di indicare quali siano tali luoghi.

La peculiarità dello strumento di intercettazione andava, dunque, meglio considerata e rapportata alle disposizioni vigenti e il provvedimento impugnato non ha offerto una motivazione congrua e convincente all'analoga eccezione sollevata in sede di riesame.

2.3. Il terzo motivo eccepito lamenta violazione di legge processuale ed inutilizzabilità delle intercettazioni disposte nel procedimento tramite captatore informatico, strumento non ancora consentito dal legislatore.

Nonostante gli sforzi ricostruttivi della giurisprudenza, infatti, la possibilità di disporre intercettazioni tramite captatore informatico non era contemplata dal legislatore prima dell'entrata in vigore della legislazione del 2017 (legge delega n. 103 del 2016 e d. lgs. n. 216 del 2017), avvenuta, per quanto riguarda le modifiche di disciplina collegate all'utilizzo del "trojan", solo per i procedimenti penali, da ultimo, iscritti dopo il 31 agosto 2020. Ciò prova, a giudizio della difesa, che per i procedimenti penali precedentemente iscritti non era affatto autorizzabile l'utilizzo del captatore informatico per disporre l'intercettazione di conversazioni degli indagati, con conseguente inutilizzabilità di quelle autorizzate nel procedimento a carico del ricorrente.

Inoltre, la difesa ripercorre la giurisprudenza costituzionale e delle Sezioni Unite sulle limitazioni alla segretezza della corrispondenza "fisica" rappresentata da lettere e messaggi scritti, la rapporta alla sentenza Scurato sul captatore informatico ed alla legislazione che, solo successivamente a tale pronuncia, ha inteso prevedere dettagliatamente disposizioni sulle modalità esecutive delle intercettazioni tramite virus informatico (si pensi al nuovo testo dell'art. 271 cod. proc. pen. ed agli innesti operati sull'art. 89 delle disposizioni di attuazione al codice di rito, fondamentali per assicurare la correttezza delle intercettazioni tramite un mezzo così invasivo di ingerenza investigativa); infine, giunge a contestare apertamente la soluzione adottata dalle

Sezioni Unite nella sentenza Scurato che non si è preoccupata di verificare l'idoneità a supportare il nuovo "tipo" di intercettazioni della disciplina previgente a quella poi oggetto di novella.

2.4. La quarta ragione di censura proposta dal ricorrente attiene al difetto di motivazione dei decreti autorizzativi e di quelli di proroga circa l'indispensabilità di procedere ad intercettazione tramite captatore informatico, con violazione, quindi, dell'art. 267 cod. proc. pen.
L'obbligo di un'adeguata motivazione, idonea a supportare uno strumento di indagine così invasivo, è stato previsto sia dalla novella del 2017 (cfr. il secondo periodo dell'art. 267 cod. proc. pen.), sia dalle stesse Sezioni Unite nella sentenza Scurato del 2016.
Ed invece, i decreti autorizzati relativi ai RIT 109/2018, 454/2018, 790/2018 sono privi di tale motivazione specifica sulla necessità di far ricorso all'intercettazione tramite *trojan* e sull'impossibilità che agli stessi risultati investigativi potesse giungersi con le tradizionali e meno invasive intercettazioni telefoniche o ambientali.

CONSIDERATO IN DIRITTO

1. Il ricorso è complessivamente infondato, a tratti anche inammissibile, e deve essere, pertanto, rigettato.
Il ricorrente, infatti, in parte, non si confronta con la motivazione dell'ordinanza del Tribunale del Riesame di Lecce con cui si è adeguatamente risposto alle eccezioni sull'utilizzabilità delle intercettazioni avuto riguardo sia alla loro legittimità, a prescindere dall'entrata in vigore della riforma sulla possibilità di utilizzare il captatore informatico tramite virus *trojan*, trattandosi di reati di associazione mafiosa e finalizzata al traffico di stupefacenti, secondo le affermazioni della giurisprudenza di legittimità in tema, sia alla loro specifica motivazione; per altra parte pone questioni prive di fondamento.

2. Il primo ed il terzo motivo di ricorso, che possono essere trattati in maniera unitaria, attenendo alla legittimità delle intercettazioni tramite *trojan* sotto diversi aspetti e risolvendosi, in ultima analisi, entrambi, in una richiesta di revisione degli approdi della giurisprudenza di legittimità da ultimo pronunciatasi sul tema, sono infondati.

3.1. È bene premettere che sul tema delle intercettazioni tramite captatore informatico (un software-virus conosciuto come *trojan*) la giurisprudenza di legittimità nella sua massima espressione ha già avuto modo di compiere alcune affermazioni importanti, culminate nella sentenza delle Sezioni Unite n. 26886 del 28/4/2016, Scurato, Rv.

266905-06, pronuncia che ha affrontato il problema rilevando come, in tema di intercettazioni ambientali, fosse legittima l'utilizzazione di tale innovativo strumento tecnologico e come la possibilità di tale suo utilizzo derivasse direttamente dalle disposizioni normative vigenti ed in particolare dall'art. 13 del d.l. n. 152 del 1991, convertito in l. n. 203 del 1991, in tal modo limitandone l'utilizzo ai reati di "criminalità organizzata", offrendo anche la corretta nozione di tale categoria criminologica secondo la *ratio* della disciplina dettata nel 1991.

Quanto alla natura di tale captatore informatico, le Sezioni Unite, così come la giurisprudenza successiva, hanno sottolineato il suo essere costituito, appunto da un software, del tipo definito simbolicamente *trojan horse* (chiamato "captatore informatico" già nelle prime pronunce sul tema - cfr. Sez. 5, n. 16556 del 14/10/2009, dep. 2010, Virruso, Rv. 246954 - oppure "agente intrusore": cfr. Sez. 6, n. 27100 del 26/05/2015, Musumeci, Rv. 265654). Tale programma informatico, viene installato in un dispositivo-obiettivo (il *target*, che può essere un computer, un tablet o uno smartphone), di norma a distanza e in modo occulto, per mezzo del suo invio con una e-mail, un sms o un'applicazione di aggiornamento, attivata dallo stesso dispositivo obiettivo.

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.

La peculiarità di tale strumento è quella che attraverso il suo utilizzo si riesce a captare l'intero flusso di informazioni provenienti da un dispositivo elettronico in cui il virus informatico è stato inoculato, permettendo di farne copia attraverso l'ispezione anche dell'hardware; si possono registrare le conversazioni in presenza attivando il microfono del dispositivo "infettato"; si può mettere in funzione la web-camera, carpendo le immagini visualizzabili; si può decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (screenshot).

In sostanza, il *trojan* consente di seguire costantemente il bersaglio con un'attivazione continua e l'apprensione di tutti i dati in esso contenuti, sfuggendo eventualmente anche alle protezioni antivirus, nonchè di trasmettere via internet i dati in tempo reale, ovvero ad intervalli prestabiliti, ad altro sistema informatico in uso agli investigatori.

L'intercettazione caratterizzata da tali modalità – come hanno messo in evidenza le Sezioni Unite – si configura come "*sostanzialmente di natura ambientale*" e può "*avvenire ovunque, quindi anche all'interno di un domicilio e non solo in luoghi pubblici o aperti al pubblico, senza dover affrontare i problemi pratici che implica la collocazione di una microspia, evitando dunque agli investigatori anche il rischio di essere scoperti*".

La sentenza Scurato argomenta ancora secondo una linea di omogeneità di disciplina tra le intercettazioni ambientali intercettazioni disposte tramite captatore informatico (a

pag. 11 della pronuncia del massimo collegio nomofilattico è dato leggere: "*..delineate le caratteristiche tecniche dello strumento di intercettazione in argomento* (quello tramite captatore informatico, n.d.r.), *appare evidente che, quanto alla "qualificazione giuridica" dell'attività d'indagine con esso svolta, non può che farsi riferimento alle intercettazioni c.d. "ambientali".*

Da tale omogeneità "*deriva che i parametri normativi - nonché i criteri interpretativi e le "linee-guida" elaborati dalla giurisprudenza - da tener presenti, nel procedere al vaglio della questione rimessa alle Sezioni Unite, non possono che essere quelli che a tale tipo di intercettazione si riferiscono*" (così ancora la pronuncia Scurato a pag. 11).

2.2. Alla luce di tale premessa sulla tipologia di strumento investigativo con cui ci si confronta, può essere analizzato il motivo di ricorso formulato dall'indagato e riferito alle fase dell'esecuzione delle operazioni di intercettazione.

Ebbene, seguendo le indicazioni delle Sezioni Unite e guardando alla giurisprudenza di legittimità formatasi in materia di intercettazioni ambientali - sia pur tenendo presente le peculiarità dello strumento di intercettazione costituito dal *trojan* – anzitutto deve rammentarsi come le operazioni esecutive di installazione degli strumenti tecnici atti a captare le conversazioni tra presenti siano state ritenute implicitamente autorizzate ed ammesse con il provvedimento che dispone l'intercettazione; e difatti si è affermato che la collocazione di microspie all'interno di un luogo di privata dimora, costituendo una delle naturali modalità attuative di tale mezzo di ricerca della prova, deve ritenersi implicitamente ammessa nel provvedimento che ha disposto le operazioni di intercettazione, senza la necessità di una specifica autorizzazione: cfr. Sez. 6, n. 14547 del 31/1/2011, Di Maggio, Rv. 250032; Sez. 1, n. 24539 del 9/12/2003, dep. 2004, Rigato, Rv. 230097.

Tale principio è diretta conseguenza del fatto che 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 della corrispondenza e di qualsiasi forma di comunicazione previsto dall'art. 15 Cost. devono coordinarsi, subendo la necessaria compressione (Sez. 2, n. 21644 del 18/02/2013, Badagliacca, Rv. 255541; Sez. 1, n. 38716 del 02/10/2007, Biondo, Rv. 238108; Sez. 4 n. 47331 del 28/09/2005, Cornetto, Rv. 232777; Sez. 6, n. 4397 del 10/11/1997, Greco, Rv. 210062).

Le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni, poi, costituiscono atti materiali rimessi alla contingente valutazione della polizia giudiziaria, non essendo compito del pubblico ministero indicare le modalità dell'intrusione negli ambiti e luoghi privati ove verrà svolta

l'intercettazione poiché la finalità di intercettare conversazioni telefoniche e/o ambientali consente all'operatore di polizia la materiale intrusione, per la collocazione dei necessari strumenti di rilevazione nei luoghi oggetto di tali mezzi di ricerca della prova; l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali (Sez. 6, n. 39403 del 23/6/2017, Nobile, Rv. 270941; Sez. 6, n. 41514 del 25/9/2012, Adamo, Rv. 253805).

Tanto ciò è vero che di recente una pronuncia ha ritenuto utilizzabili le intercettazioni acquisite tramite la collocazione di microspie anziché mediante l'impiego di un software spia, così come invece era originariamente disposto nel decreto autorizzativo del giudice; ciò perché – si è detto - la modifica delle modalità esecutive delle captazioni, concernendo un aspetto meramente tecnico, può essere autonomamente disposta dal pubblico ministero, non occorrendo un apposito provvedimento da parte del giudice per le indagini preliminari (Sez. 6, n. 45486 del 8/3/2018, Romeo, Rv. 274934).

In altre parole, l'autorizzazione a disporre le operazioni di intercettazioni rende superflua l'indicazione delle modalità da seguire nell'espletamento dell'attività materiale e tecnica da parte della polizia giudiziaria, mentre la prova delle operazioni compiute nel luogo e nei tempi indicati dal giudice stesso e dal pubblico ministero è offerta dalla registrazione delle conversazioni intercettate (sul tema, in motivazione, vedi - oltre che Sez. 2, n. 21644 del 18/02/2013, Badagliacca, Rv. 255541; Sez. 1, n. 38716 del 02/10/2007, Biondo, Rv. 238108; Sez. 4 n. 47331 del 28/09/2005, Cornetto, Rv. 232777 - anche Sez. 6, n. 36874 del 13/06/2017, Romeo).

Dunque, è possibile affermare che:

- le questioni relative all'installazione degli strumenti tecnici per l'intercettazione – come nella specie il virus *trojan* – in relazione all'obiettivo da intercettare non attengono alla fase autorizzativa dell'attività investigativa demandata al giudice per le indagini preliminari, né alla verifica dei presupposti di legittimità delle intercettazioni, bensì alla fase esecutiva, già coperta dall'autorizzazione a disporre le stesse intercettazioni;
- la fase esecutiva è consegnata alle prerogative del pubblico ministero che può delegare la polizia giudiziaria alle operazioni materiali di installazione tecnica degli strumenti (software, hardware, trojan) idonee a dar vita, in concreto, alle intercettazioni; eventuali modifiche degli strumenti già indicati nel decreto autorizzativo del GIP come quelli da utilizzare per eseguire le captazioni possono essere disposte dallo stesso pubblico ministero;
- le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni, anche tramite virus *trojan*, costituiscono atti materiali rimessi alla contingente valutazione della polizia giudiziaria, consentiti dalla finalità pubblica di procedere ad attivare il mezzo di ricerca della prova anche quando consistono in

un'intrusione da parte degli agenti incaricati dell'esecuzione in luoghi privati o altrui o, come nel caso del captatore informatico, in dispositivi informatici tramite inserimento di un software spia; l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali.

2.3. Orbene, quanto alla lamentata fraudolenza del mezzo utilizzato per carpire le conversazioni intercettate ed intromettersi nel dispositivo elettronico-obiettivo, e cioè del virus *trojan* inoculato ed attivato indebitamente e mediante la collaborazione del soggetto stesso intercettato, tratto in inganno informaticamente, è sufficiente richiamarsi a quanto sopra evidenziato ed in particolare sottolineare quanto segue.
Se la finalità di intercettare conversazioni telefoniche e/o ambientali consente all'operatore di polizia la materiale intrusione, per la collocazione dei necessari strumenti di rilevazione, negli ambiti e nei luoghi di privata dimora, oggetto di tali mezzi di ricerca della prova, senza che il pubblico ministero, delegato per l'esecuzione, sia tenuto a precisare le modalità di intrusione delle microspie in tali luoghi e senza che la relativa omissione determini alcuna nullità dell'atto (Sez. 6, n. 41514 del 25/9/2012, Adamo, Rv. 253805; cfr. anche le già citate Sez. 6, n. 14547 del 2011, Di Maggio e Sez. 1, n. 24539 del 2004, Rigato; nonché Sez. 6, n. 39403 del 2017, Nobile); allo stesso modo, la medesima finalità di intercettazione consente all'operatore di polizia, ovvero ad un suo delegato (di solito un privato, tecnico della società specializzata incaricata dell'esecuzione delle operazioni di inoculazione del software spia), di introdursi, anche da remoto, nel dispositivo elettronico-*target* indicato nel decreto autorizzativo del giudice e di installare il *trojan* mediante le modalità tecniche necessarie e utilizzando gli strumenti tecnologici opportuni.
Inoltre, argomentando ancora una volta *mutatis mutandis* dalla giurisprudenza relativa alle intercettazioni ambientali "classiche", può affermarsi che, in tema di intercettazioni tramite captatore informatico, la fraudolenza dell'intrusione nel dispositivo-*target* tramite virus *trojan*, poiché costituisce una delle naturali modalità attuative di tale mezzo di ricerca della prova, deve ritenersi implicitamente ammessa nel provvedimento che ha disposto le operazioni di intercettazione, senza la necessità di una specifica autorizzazione (cfr. Sez. 6, n. 14547 del 31/1/2011, Di Maggio, Rv. 250032; Sez. 1, n. 24539 del 9/12/2003, dep. 2004, Rigato, Rv. 230097) e pienamente legittima dal punto di vista del bilanciamento tra il 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 principio di inviolabilità della sfera di riservatezza e segretezza di qualsiasi forma di comunicazione previsto dall'art. 15 Cost. (cfr. in tema ancora di intercettazioni ambientali "classiche" e avuto riguardo anche all'inviolabilità del domicilio sancita dall'art. 14 Cost. : Sez. 2, n. 21644 del 18/02/2013, Badagliacca,

Rv. 255541; Sez. 1, n. 38716 del 02/10/2007, Biondo, Rv. 238108; Sez. 4 n. 47331 del 28/09/2005, Cornetto, Rv. 232777; Sez. 6, n. 6071 del 21/1/2004, Parisi, Rv. 227651; Sez. 6, n. 4397 del 10/11/1997, dep. 1998, Greco, Rv. 210062).

Tale bilanciamento e coordinamento del primo principio con la relativa necessaria compressione dei secondi, perfettamente legittima dal punto di vista della tenuta costituzionale, vale anche in riferimento al diritto di proprietà privata, previsto dall'art. 42 Cost. ed invocato dalla seconda parte del motivo di ricorso formulato dall'indagato, avuto riguardo alla lamentata, illecita utilizzazione - mediante l'intercettazione con virus *trojan* - dell'energia acquistata dagli stessi indagati per la ricarica delle batterie del dispositivo elettronico "infettato" ed all'utilizzo di quest'ultimo in quanto tale.

Ed infatti, è evidente che le conseguenze di "perdita" e "sottrazione" patrimoniale di una quota del proprio diritto di proprietà da parte del soggetto intercettato rimangono soccombenti, anche per la loro minima compressione, rispetto all'obiettivo, egualmente legittimo dal punto di vista costituzionale, del soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost.

La giurisprudenza della Corte costituzionale, anche più recente, non è di ostacolo alle opzioni alle quali si è appena aderito.

Invero, depone nel senso qui preferito la stessa pronuncia n. 20 del 2017 del giudice delle leggi, richiamata nel ricorso al fine di sostenere l'illegittimità dell'utilizzo del mezzo captatore informatico e l'impraticabilità di forme di controllo del diritto alla comunicazione non esplicitamente previste nelle modalità dalla legge, per il principio di non sostituibilità della prova e senza che possa essere applicato il concetto di prova atipica alle intercettazioni disposte tramite *trojan*, ancora una volta nel tentativo di smentire gli approdi delle Sezioni Unite nella sentenza Scurato.

I giudici delle leggi, in detta sentenza, hanno evidenziato come i diritti di «libertà» e «segretezza» della «corrispondenza e di ogni altra forma di comunicazione», oggetto del diritto «inviolabile» tutelato dall'art. 15 Cost. (citando le sentenze n. 366 del 1991 e n. 81 del 1993), al pari di ogni altro diritto costituzionalmente protetto, possono essere soggetti a limitazioni, purché disposte «per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge», poiché, se così non fosse, «si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette» (sentenza n. 85 del 2013).

Per questo, la «Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi», nel rispetto dei canoni di proporzionalità e di ragionevolezza (sentenza n. 85 del 2013).

Pertanto, anche alcuni diritti inviolabili possono subire limitazioni o restrizioni «in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario

costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia» della riserva assoluta di legge e della riserva di giurisdizione (sentenza n. 366 del 1991).

La Corte costituzionale ritiene che non vi sia dubbio sul fatto che l'amministrazione della giustizia e la persecuzione dei reati costituiscano interessi primari, costituzionalmente rilevanti, idonei a giustificare una normativa limitativa del diritto alla libertà e alla segretezza della corrispondenza e della comunicazione. Ciò avviene, appunto, attraverso la previsione legislativa di mezzi di ricerca della prova, disciplinati dal Libro III, Titolo III, Capo III, del codice di procedura penale, che consentono all'autorità giudiziaria di prendere conoscenza dei contenuti delle comunicazioni interpersonali rilevanti ai fini dell'accertamento dei reati e di utilizzarli come evidenze processuali.

Sono, dunque, i mezzi di ricerca della prova a dover essere coperti da riserva di legge, ma non le specifiche modalità attuative, influenzate da materiali questioni pratiche o di sviluppo tecnologico, a godere della medesima riserva, rimanendo evidente, peraltro, che l'unico profilo oggetto di verifica di costituzionalità sia quello relativo al fatto che "*il legislatore abbia operato in concreto un bilanciamento tra il principio costituzionale della tutela della riservatezza nelle comunicazioni e l'interesse della collettività, anch'esso costituzionalmente protetto, alla repressione degli illeciti penali, senza imporre limitazioni irragionevoli o sproporzionate dell'uno o dell'altro (sentenza n. 372 del 2006)*".

E' pertanto manifestamente infondata la questione di illegittimità costituzionale proposta dal ricorrente in relazione all'art. 42 Cost. della disciplina delle intercettazioni tra presenti tramite virus captatore informatico (*trojan*) posto che le conseguenze di "perdita" e "sottrazione" patrimoniale di una quota del proprio diritto di proprietà da parte del soggetto intercettato (costituita dalla sottrazione di energia dalle batterie e dall'utilizzo indebito dello stesso dispositivo elettronico-*target*) rimangono soccombenti, anche per la loro minima compressione, rispetto all'obiettivo, egualmente legittimo dal punto di vista costituzionale, del soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio dell'obbligatorietà dell'azione penale di cui all'art. 112 Cost.

2.4. Anche rispetto all'obiezione relativa all'impossibilità di procedere legittimamente ad autorizzare intercettazioni tramite captatore informatico prima che un'espressa previsione di legge fosse emanata – cosa poi accaduta grazie alla novella di cui al d.lgs. n. 216 del 2017 - l'eccezione difensiva appare priva di fondamento.

La pronuncia Sez. U, n. 26886 del 28/4/2016, Scurato, Rv. 266905-06 ha affrontato direttamente il problema rilevando come, in tema di intercettazioni ambientali, vi fosse

la possibilità di utilizzare il captatore informatico già col sistema vigente e come tale possibilità derivasse direttamente dalle disposizioni normative vigenti ed in particolare dall'art. 13 del d.l. n. 152 del 1991, convertito in l. n. 203 del 1991, in tal modo, contestualmente, limitandone l'utilizzo ai reati di "criminalità organizzata" ed offrendo anche la nozione di tale categoria criminologica.

Ciò perché, quando si autorizza l'utilizzazione di questo strumento esecutivo dell'intercettazione, ovviamente secondo i parametri normativi usuali dettati dalla disciplina codicistica, si deve prescindere dall'indicazione dei luoghi in cui la captazione deve avvenire, posto che è impossibile, utilizzando tale mezzo di captazione, una preventiva individuazione ed indicazione dei luoghi di interesse, data la natura itinerante dello strumento di indagine da utilizzare, che, detto altrimenti, implica l'impossibilità di circoscrivere a priori l'intercettazione ambientale rispetto a determinati luoghi.

Per tali ragioni le Sezioni Unite hanno sì affermato la possibilità di accedere all'intercettazione tramite captatore informatico da parte degli organi investigativi, ma ne hanno limitato l'ammissibilità rispetto ai soli procedimenti per i delitti di criminalità organizzata di cui all'art. 13 d.l. n. 152 del 1991, convertito in legge n. 203 del 1991, perché tale norma consente la captazione anche nei luoghi di privata dimora senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto, evitando in radice il problema della pervasività indiscriminata dello strumento di captazione.

Peraltro, il Supremo Collegio ha sottolineato come, proprio in considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso.

Si tratta di un richiamo rigoroso al rispetto degli obblighi di motivazione da parte del giudice che autorizza l'intercettazione, pur dovendo la motivazione del decreto essere "contenuta" e sobria, secondo i canoni propri della categoria di provvedimento cui si riferisce, il decreto (cfr. Sez. 6, n. 4057 del 22/12/1998, dep. 1999, Colombani, Rv. 214777; Sez. 4, n. 27235 del 20/6/2002, Piccolo, Rv. 221807).

Accanto all'indicazione di una motivazione puntuale, sia pur sintetica, del decreto di intercettazione quanto agli indizi di sussistenza della compagine associativa, le Sezioni Unite hanno esse stesse offerto all'interprete la nozione di *procedimenti relativi a delitti di criminalità organizzata* intesi per essere quelli elencati nell'art. 51, commi 3-*bis* e 3-*quater*, cod. proc. pen. nonché quelli comunque facenti capo ad una associazione per delinquere, con esclusione del mero concorso di persone nel reato.

L'utilizzo del nuovo mezzo tecnologico, quindi, è stato escluso dalle Sezioni Unite per i reati comuni perché, non essendo possibile nel momento dell'autorizzazione prevedere

i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto, non sarebbe consentito verificare il rispetto della condizione di legittimità richiesta dall'art. 266, comma 2, cod. proc. pen. che presuppone, per le captazioni in luoghi di privata dimora, che ivi sia in atto l'attività criminosa.

Tale approdo ermeneutico non è stato risparmiato dalle critiche di una parte della dottrina che ritiene la pronuncia non abbia tenuto conto di tutte le potenzialità del nuovo strumento, con le quali si sarebbe potuto garantire un adeguato contemperamento tra le esigenze investigative alle quali è funzionale l'utilizzo del *trojan* e quelle del rispetto delle condizioni di autorizzabilità previste dall'art. 266, comma secondo, cod. proc. pen., evitando il rischio di autorizzazioni "al buio".

E tuttavia, dal punto di vista più specificamente tecnico della nozione e dei caratteri distintivi di tale mezzo di captazione informatica delle conversazioni afferenti ad un determinato obiettivo/dispositivo elettronico, le Sezioni Unite Scurato offrono sin dal 2016 un punto d'arrivo sicuro al quale il Collegio intende riportarsi per rigettare, come rilevato in apertura del paragrafo, l'eccezione difensiva in proposito formulata.

Si è infatti chiarito nella pronuncia che utilizzando tale strumento: "*le intercettazioni vengono effettuate mediante un software, del tipo definito simbolicamente trojan horse, che è chiamato, nelle prime sentenze che si sono confrontate con esso, "captatore informatico" (Sez. 5, n. 16556 del 14/10/2009, 7 dep. 2010, Virruso, Rv. 246954) o "agente intrusore" (Sez. 6, n. 27100 del 26/05/2015, Musumeci, Rv. 265654). Tale programma informatico, viene installato in un dispositivo del tipo target (un computer, un tablet o uno smartphone), di norma a distanza e in modo occulto, per mezzo del suo invio con una mali, 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 che il virus usa per controllare detto dispositivo.*

Uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente: - di captare tutto il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia web mail, che outlook); - di attivare il microfono e, dunque, di apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi; - di mettere in funzione la web camera, permettendo di carpire le immagini; - di perquisire l'hard disk e di fare copia, totale o parziale, delle unità di memoria del sistema informatica preso di mira; - di decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (keylogger) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (screenshot); - di sfuggire agli antivirus in commercio.

I dati raccolti sono trasmessi, per mezzo della rete internet, in tempo reale o ad intervalli prestabiliti ad altro sistema informatico in uso agli investigatori."

Successivamente all'intervento delle Sezioni Unite, a conclusione di un'elaborazione parlamentare già in atto da anni, il legislatore ha definitivamente avvertito il bisogno di disciplinare normativamente e direttamente lo strumento intercettativo del *trojan*, emanando il d. lgs. 29 dicembre 2017, n. 216 (cd. decreto Orlando), il cui art. 4 ha modificato il comma 2 dell'art. 266 cod. proc. pen., inserendo espressamente la possibilità di dar luogo alle intercettazioni tra presenti tramite captatore informatico (attraverso l'inclusione nel testo delle seguenti parole: "*che può essere eseguita anche mediante l'inserimento di un captatore informatico su dispositivo elettronico portatile.*") Aggiungendo poi anche un comma 2-*bis* alla medesima disposizione codicistica, in forza del quale: "*L'intercettazione di comunicazioni o conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti di cui all'art. 51, comma 3-bis e 3-quater*".

In tal modo, l'attuale testo dell'art. 266 cod. proc. pen. costituisce la codificazione del quadro normativo preesistente così come già ricostruito dalle Sezioni Unite con la sentenza Scurato.

Orbene, il fatto che il legislatore successivamente all'intervento delle Sezioni Unite abbia provveduto a regolamentare espressamente la materia non priva di validità le affermazioni alle quali è pervenuto il massimo Collegio nomofilattico in relazione ai procedimenti per i quali le operazioni di intercettazione sono state autorizzate prima dell'entrata in vigore della novella.

In proposito, si rammenta che conferma di tale ricostruzione si ritrova anche nella pronuncia delle Sezioni Unite Civili n. 741 del 3/12/2019, dep. 2020, Rv. 656792.

Affermano le Sezioni Unite Civili che tale possibilità preesisteva e prescindeva dalla modifica del testo delle disposizioni del codice di rito operata dall'art. 4 del decreto legislativo del 2017 e deriva direttamente, come sostenuto dalle Sezioni Unite Scurato, dall'art. 13 d.l. n. 152 del 1991.

Di conseguenza, è legittimo argomentare che anche al momento dell'emanazione dei decreti di intercettazione del presente procedimento, antecedenti alla novella normativa del d.lgs. n. 216 del 2017, vi era possibilità di autorizzare le intercettazioni di conversazioni tra presenti tramite l'utilizzo dello strumento del virus *trojan*; a prescindere, dunque, dall'entrata in vigore della riforma sul cd. captatore informatico, tali decreti potevano essere autorizzati, avendo ad oggetto indagini per reati di associazione mafiosa e di associazione finalizzata al traffico di stupefacenti, palesemente rientranti nella nozione di criminalità organizzata prevista dall'art. 13 d.l. n. 152 del 1993 così come interpretata dalle Sezioni Unite Scurato.

Il tentativo del ricorrente di chiamare il Collegio ad una surrettizia critica e revisione degli argomenti e delle conclusioni di tale pronuncia quanto alla piena legittimità dell'utilizzo del captatore informatico per le intercettazioni disposte in ambito di criminalità organizzata prima dell'entrata in vigore del d.lgs. n. 216 del 2017 -

argomenti e conclusioni che invece si condividono pienamente, per come sin qui riassunti - deve essere, pertanto, decisamente respinto.

3.5. Infine, anche rispetto alla formulazione dell'art. 271 cod. proc. pen., la questione sulla presunta illegittimità delle operazioni esecutive dell'intercettazione, per la parte contestata dal ricorrente, che darebbe luogo alla sanzione di inutilizzabilità del loro contenuto, non trova spazio.

A prescindere, infatti, dalla considerazione generale, supportata dalle affermazioni già svolte al paragrafo precedente, che il sistema normativo complessivo predisposto in relazione all'istituto delle intercettazioni quale mezzo di ricerca della prova punta a ritenere la non deducibilità come questione di inutilizzabilità o nullità delle eventuali distonie applicative riscontrate nella fase esecutiva delle operazioni di intercettazioni diverse da quelle contenute nell'art. 268, commi primo e terzo, cod. proc. pen., espressamente richiamate dall'art. 271 del codice di rito (cfr. anche la giurisprudenza in tema di mancata indicazione, nel verbale delle operazioni compiute, delle generalità dell'interprete delle conversazioni intercettate; per tutte: Sez. 5, n. 7030 del 16/1/2020, Polak, Rv. 278659), è la stessa formulazione dell'art. 271 cod. proc. pen. che rende "chiuso" e tassativo il richiamo volto alla sanzione di inutilizzabilità dei contenuti dell'intercettazione, riferendolo alla sola inosservanza delle disposizioni previste dall'art. 267, sui presupposti e forme del provvedimento autorizzativo, e, per quel che riguarda la fase esecutiva, dall'art. 268, commi primo e terzo, cod. proc. pen.

Pertanto, la sanzione d'inutilizzabilità degli esiti di intercettazioni telefoniche o ambientali, anche tramite *trojan*, stante il principio di tassatività, non può essere dilatata sino a comprendervi l'inosservanza delle disposizioni di cui all'art. 89 disp. att. cod. proc. pen., non espressamente richiamato dall'art. 271 cod. proc. pen. (cfr. Sez. 4, n. 49036 del 17/9/2004, Cao, Rv. 229922; nonché vedi Sez. 1, n. 8836 del 2/12/2009, dep. 2010, Bragaglio, Rv. 246377).

Tale affermazione non muta pur constatata la modifica della disposizione attuativa prevista dall'art. 89 citato (cui fa riferimento il ricorso per sostenere, ancora una volta, la non praticabilità prima della riforma del 2017 e della sua completa entrata in vigore delle intercettazioni con captatore informatico), proprio in relazione all'introduzione esplicita della possibilità di disporre intercettazioni tramite *trojan*, modifica avvenuta, come più volte ricordato, appunto con la novella di cui al d.lgs. n.216 del 29 dicembre 2017, attraverso la quale si è fatto obbligo, proprio per tutelare la genuinità e correttezza delle operazioni di intercettazione tramite uno strumento così invasivo quale il captatore informatico, di indicare nel verbale di esecuzione delle operazioni di intercettazione, il tipo di programma software impiegato (potendo essere impiegati solo quei programmi conformi ai requisiti tecnici indicati con decreto del Ministero della Giustizia) ed i luoghi in cui si svolgono le comunicazioni o conversazioni, indicando

anche esplicitamente regole per il trasferimento dei dati e per la disattivazione del captatore.

E difatti, fermo il testo del primo comma dell'art. 271 cod. proc. pen. ed il richiamo ai soli articoli 267 e 268, commi primo e terzo, dello stesso codice, avente ad oggetto l'inosservanza di disposizioni che determina inutilizzabilità dei contenuti, il legislatore ha aggiunto un nuovo comma 1-*bis* all'art. 271 cit. in cui espressamente prevede l'inutilizzabilità dei dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico nel dispositivo-*target* e di quelli acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo.

Ma non vi è questione alcuna su tali aspetti proposta dal ricorrente.

4. Il secondo motivo di ricorso è manifestamente infondato ed anche in parte generico, poiché non si confronta con le ragioni esposte sul punto dal provvedimento impugnato.

In realtà, il Riesame ha centrato il punto cruciale da tenere presente per risolvere la questione posta dal ricorrente, sostanzialmente legata alla necessità o meno di individuare preventivamente i luoghi entro i quali si svolgeranno le intercettazioni tramite *trojan* pur in relazione alle operazioni autorizzate per reati per i quali non è necessario che, se di privata dimora, vedano ivi in corso l'attività criminosa.

Il dettato normativo, infatti, come indicato più volte dalle Sezioni Unite nella citata sentenza Scurato, non si riferisce alle intercettazioni cd. ambientali facendo riferimento ai *luoghi ove esse avvengono*, bensì le individua facendo ricorso alla locuzione *intercettazione tra presenti*, svincolando l'autorizzazione dall'indicazione dei luoghi, salvo che non si tratti di luoghi di privata dimora nei quali deve indicarsi, tuttavia, ed è questo il punto da motivare e segnalare, che ivi si stia svolgendo l'attività criminosa.

In tale ultimo caso, peraltro, come noto, neppure occorrerà tale indicazione se si ricade nella disciplina speciale prevista per le intercettazioni tra presenti in materia di criminalità organizzata dall'art. 13 del d.l. n. 152 del 1991, conv. in l. n. 203 del 1991, oggi veicolata, per le intercettazioni tramite *trojan*, nell'art. 266, comma 2-*bis,* cod. proc. pen. che l'ha estesa ai reati dei pubblici ufficiali o degli incaricati di pubblico servizio per i delitti commessi contro la p.a. puniti con la pena della reclusione non inferiore nel massimo a cinque anni, oltre che ai procedimenti, appunto, per i delitti di cui agli artt. 51, commi 3-*bis* e 3-*quater*; anche l'art. 266, comma 2-*bis*, del codice di rito, peraltro, conferma la dizione normativa di "intercettazioni tra presenti" e non "ambientali".

Orbene, nel caso del ricorrente, in relazione a reati di criminalità organizzata, è logico ritenere che, se non è necessario fornire motivazione nel decreto autorizzativo circa il fatto che in un determinato luogo, perché di privata dimora, si stia svolgendo il reato,

diventa priva di rilievo anche l'indicazione di tale luogo, che intanto era importante in quanto finalizzata ad individuarlo nella sua funzione di possibile futuro *locus delicti.*

Non vi è motivo, dunque, per non ribadire le affermazioni delle Sezioni Unite Scurato, che il ricorrente mira a confutare, secondo cui, limitatamente (all'epoca della pronuncia, n.d.r.) ai procedimenti per delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un 'captatore informatico' in dispositivi elettronici portatili (ad es. personal computer, tablet, smartphone, ecc.) – anche nei luoghi di privata dimora ex art. 614 codice penale, *pure non singolarmente individuati* e anche se ivi non si stia svolgendo l'attività criminosa (cfr. Rv. 266905).

Già il Riesame aveva ben chiarito, infatti, e di qui l'inammissibilità dell'argomento difensivo anche per la sua aspecificità, come le Sezioni Unite Scurato abbiano affermato che "*Va.. evidenziato innanzi tutto il dato testuale della norma, posto che 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 secondo cui le garanzie minime che la legge nazionale deve apprestare nella materia delle intercettazioni riguardano la predeterminazione della tipologia delle comunicazioni oggetto di intercettazione, la ricognizione dei reati che giustificano tale mezzo di intrusione nella privacy, l'attribuzione ad un organo indipendente della competenza ad autorizzare le intercettazioni con la previsione del controllo del giudice, la definizione delle categorie di persone che possono essere interessate, i limiti di durata delle intercettazioni, la procedura da osservare per l'esame, l'utilizzazione e la conservazione dei risultati ottenuti, la individuazione dei casi in cui le registrazioni devono essere distrutte (cfr., Corte EDU, 31/05/2005, Vetter c. Francia; Corte EDU, 18/05/2010, Kennedy c. Regno Unito): non è dato rilevare, dunque, alcun riferimento alla indicazione del luogo della captazione."

Concludendo, quindi, le Sezioni Unite, nel senso di ritenere che: "*Anche la giurisprudenza sovranazionale conforta, pertanto, l'interpretazione secondo cui nell'intercettazione tra presenti, compiuta con mezzi definibili "tradizionali", il riferimento al luogo non integra un presupposto dell'autorizzazione, ma rileva solo limitatamente alla motivazione del decreto nella quale il giudice deve indicare le situazioni ambientali oggetto della captazione, e ciò solo ai fini della determinazione*

delle modalità esecutive del mezzo di ricerca della prova, che avviene mediante la collocazione fisica di microspie. Un'esigenza di questo tipo è invece del tutto estranea all'intercettazione per mezzo del c.d. virus informatico: la caratteristica tecnica di tale modalità di captazione prescinde dal riferimento al luogo, trattandosi di un'intercettazione ambientale per sua natura "itinerante"."

Tale affermazione deve essere ulteriormente precisata ed aggiornata alla luce dell'ulteriore elaborazione della giurisprudenza europea che, in un'importante pronuncia della Corte di Strasburgo successiva a quelle citate dalle Sezioni Unite – la sentenza Grande Camera *Roman Zakharov c. Russia* del 4.12.2015 -, ha confermato come non sia necessario che nel provvedimento autorizzativo delle intercettazioni siano indicati i luoghi in cui le stesse devono svolgersi, purchè ne venga identificato il destinatario.

Questi due elementi, infatti, sono citati dalla Corte EDU *in termini alternativi e non cumulativi* e l'affermazione assume particolare valore perché si inscrive in una pronuncia che a ragione viene indicata come quella da cui si può ricavare una sorta di "statuto europeo" della legittimità delle operazioni di intercettazione per valutarne la conformità ai principi insiti nell'art. 8 CEDU, che sancisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza (cfr. sul tema anche la sentenza Corte EDU, *Capriotti c. Italia* del 23.2.2016).

Posto che, dunque, il riferimento al luogo di svolgimento dell'intercettazione tra presenti non ne costituisce un presupposto di autorizzabilità necessario – ma rileva solo in chiave motivazionale -, essendo alternativamente sempre consentito far ricorso all'indicazione sul destinatario di essa, secondo le indicazioni della giurisprudenza europea, in particolare riprese dalla sentenza suddetta *Roman Zakharov*, e considerato, altresì, che l'intercettazione mediante captatore informatico per sua natura prescinde dal riferimento ai luoghi, in ragione della sua dinamicità e del suo essere strumento di per sé "itinerante", l'eccezione del ricorrente si rivela manifestamente infondata.

5. Il quarto motivo di censura è anch'esso manifestamente infondato.

L'obbligo di un'adeguata motivazione, idonea a supportare uno strumento di indagine così invasivo, è stato previsto sia dalla novella del 2017 (cfr. il secondo periodo dell'art. 267 cod. proc. pen.) in termini di "necessità" del suo utilizzo, sia dalle stesse Sezioni Unite nella sentenza Scurato del 2016, sotto il profilo, cui si è già fatto riferimento, dell'esigenza che, in considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso.

L'indagato lamenta l'assenza di tali caratteri motivazionali, in particolare, ritiene applicabile la nuova formulazione normativa anche a decreti autorizzati prima della sua entrata in vigore (i decreti autorizzati relativi ai RIT 109/2018, 454/2018, 780/2018),

che sarebbero privi della motivazione specifica sulla necessità di far ricorso all'intercettazione tramite *trojan* e sull'impossibilità che agli stessi risultati investigativi potesse giungersi con le tradizionali e meno invasive intercettazioni telefoniche o ambientali.

Orbene, a prescindere dalla questione relativa al fatto che, secondo il criterio pacifico del *tempus regit actum* operante in ambito di successione di leggi nel tempo in materia processuale (cfr. da ultimo Sez. U, n. 44895 del 17/7/2014, Pinna, Rv. 260927), la nuova disciplina sulla rafforzata motivazione per installare un virus *trojan* non si applica al caso di specie, avente ad oggetto decreti autorizzativi precedenti alla sua entrata in vigore, è bene evidenziare come nel caso di specie il giudice ha dato pienamente atto delle ragioni che rendevano indispensabile far ricorso allo strumento del captatore informatico.

Non corrisponde al vero, infatti, che vi sia stato un utilizzo di formule stereotipate, come sostenuto nel ricorso, essendovi anzi nel testo omogeneo dei decreti autorizzativi un preciso riferimento al fatto che lo strumento di intercettazione maggiormente invasivo veniva preferito poichè non vi erano dichiaranti o testimoni che potessero all'epoca rendere contributi utili all'accertamento di reati e responsabilità individuali, nonché in considerazione dello stato di detenzione di molti dei soggetti ritenuti obiettivi interessanti, della tipologia dei reati e sulle modalità della condotta associativa sino ad allora già registrata nelle indagini.

Alle pagine 6, 7 e ss. del provvedimento impugnato si spiegano bene tutte le richiamate ragioni alla base della scelta del GIP di disporre una captazione intrusiva tramite *trojan* per ciascuno dei tre RIT contestati, in particolare sottolineando il ruolo associativo dei soggetti-obiettivo ed il fatto che in tal modo fosse possibile individuare le direttive in partenza dal carcere per lo svolgimento delle attività criminali del sodalizio ovvero scoprire la gestione delle dinamiche interne al gruppo e monitorarne i livelli di operatività.

A pagina 11 del provvedimento del Riesame si ritrova, poi, eguale motivazione analitica anche in riferimento ai decreti di proroga delle intercettazioni relative ai decreti contestati, non senza evidenziare ciò che effettivamente costituisce un approdo condiviso della giurisprudenza di legittimità, e cioè la minore specificità alla quale possono essere ispirate le motivazioni dei decreti di proroga rispetto alle motivazioni dei decreti autorizzativi originari, potendosi risolvere tali ragioni motivazionali anche nel dare atto della constatata plausibilità delle argomentazioni esposte nella richiesta di proroga del pubblico ministeri (cfr., tra le tante, Sez. 4, n. 16430 del 19/3/2015, Caratozzolo, Rv. 263401: Sez. 6, n. 22524 del 1/7/2020, Bertoldi, Rv. 279564).

P. Q. M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese processuali.

Manda alla cancelleria per gli adempimenti di cui all'art. 94, comma 1-ter, disp. att. cod. proc. pen.

Così deciso il 30 settembre 2020

Il Consigliere estensore
Matilde Brancaccio

Il Presidente
Maria Vessichelli