Num.Ric.Gen 6889/16

Procura generale presso la Corte di cassazione

Memoria per la camera di consiglio delle Sezioni Unite del 28 aprile 2016 *

Sommario

**Al fine di non appesantirne eccessivamente il testo e di preservare la continuità dell'argomentazione la presente memoria è stata corredata da un apparato di note.*
Un allegato è stato riservato ai riferimenti relativi alla legislazione e alla giurisprudenza dei principali paesi europei il cui ordinamento presenta maggiori tratti di affinità con l'ordinamento italiano.

Via Serbelloni, 1 | 20122 MILANO (MI) | redazione@penalecontemporaneo.it
Direttore Responsabile Francesco Viganò | 2010-2016 Diritto Penale Contemporaneo

1, I temi in discussione.

L.S. ha proposto ricorso per cassazione avverso l'ordinanza del Tribunale del riesame di Palermo che aveva confermato la misura della custodia cautelare in carcere adottata nei suoi confronti , con provvedimento del 15 dicembre 2015, dal giudice per le indagini preliminari in relazione alla partecipazione all'associazione di tipo mafioso denominata " cosa nostra" (art. 416 bis, commi I, II, III, IV, e VI c.p.) ed ad un episodio di tentativo di estorsione aggravata .

Con il secondo motivo del suo ricorso il difensore del ricorrente ha dedotto l'illegittimità del decreto n. 315/14 con cui il GIP aveva autorizzato *" le operazioni di intercettazione di tipo ambientale tra presenti che avverranno nei luoghi in cui si trova il dispositivo elettronico in uso a a Lo Presti Tommaso"* nonché l'inutilizzabilità dei risultati relativi a tali captazioni - effettuate a mezzo di un virus autoinstallante attivato su di un apparecchio portatile in uso a Tommaso Lo Presti - per violazione degli artt. 15 Cost., 8 CEDU , 266, comma 2, e 271 c.p.p. .

In particolare il difensore ha sostenuto che , nella specie, è stato eluso il divieto posto dall'art. 266 , comma 2, c.p.p. di effettuare intercettazioni all'interno di private abitazioni a meno che all'interno di esse non si stia svolgendo una attività criminosa e , sotto diverso profilo, che l'intercettazione era stata autorizzata in violazione degli artt. 15 Cost. e 8 CEDU per non essere stati preventivamente indicati i luoghi in cui la captazione doveva essere effettuata , aggirando i limiti posti dall'art. 266, comma 2, c.p.p. e ponendo in essere intercettazioni non soggette ad alcuna restrizione spaziale i cui risultati devono essere ritenuti inutilizzabili.

Nella discussione svoltasi il 10 marzo 2016 in camera di consiglio dinanzi ad un collegio della VI Sezione penale , il procuratore generale ha concluso per il rigetto del ricorso sostenendo tra l'altro l'infondatezza del motivo di ricorso concernente le intercettazioni.

Il collegio, ravvisando un potenziale contrasto con la sentenza n. n. 27100/15 del 26.6.2015 della stessa Sezione, ha rimesso la questione alle Sezioni Unite della Corte di cassazione e, a conclusione di una approfondita motivazione della sua ordinanza (Cass., Sez. VI, ord. n. 59 del 10/3/2016 in proc. n. 13884/16) ha sintetizzato le questioni da sottoporre alle Sezioni Unite nei seguenti termini:

- *se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi dove debba avvenire la relativa captazione;*
- *se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, c.p.p.;*
- *se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.*

La presente memoria della Procura generale è circoscritta a tali questioni ed ai temi svolti nel secondo motivo del ricorso per cassazione.

Tutti gli altri profili del ricorso verranno trattati nella discussione orale nella camera di consiglio del 28 aprile.

2. Il parallelo sviluppo delle tecnologie di captazione e delle tecniche di elusione delle captazioni.

In esordio della presente memoria verrà offerta una sintetica rappresentazione degli aspetti tecnici delle intercettazioni tramite virus informatico come presupposto indispensabile per affrontare le questioni giuridiche poste nella pregevole e approfondita ordinanza di rimessione.

Prima però occorre sottolineare un più ampio dato di realtà.

Nell'ambito delle tecnologie informatiche e nel campo della telematica ogni rappresentazione dello stato dell'arte, ogni fotografia del grado di avanzamento della tecnica rischia di ingiallire e di divenire datata ed obsoleta nello spazio di pochi mesi.

Progrediscono infatti - con straordinaria velocità e quasi di pari passo - **tanto le tecnologie di captazione** , che si fanno via più sofisticate ed invasive , **quanto le tecniche di elusione** di ogni captazione possibile, che si affidano di volta in volta alla impenetrabilità degli apparecchi utilizzati, alla inaccessibilità di particolari reti di comunicazione o alla adozione di sistemi di criptazione dei messaggi scambiati.

Le valutazioni sul potenziale invasivo dei più moderni meccanismi di captazione devono perciò essere sempre compiute avendo presente che parallelamente e contemporaneamente si affinano e si moltiplicano anche i mezzi ed canali di comunicazione strutturati in modo da sottrarsi ai tradizionali strumenti di acquisizione. Mezzi e canali che spesso fondano la loro diffusione - oltre che sulla facilità dei contatti e sulla gratuità del servizio offerto, di regola compensato dagli introiti pubblicitari o dal valore delle informazioni sulla utenza raccolte attraverso di esse - proprio sulla loro vera o presunta inaccessibilità.

Se dunque è legittimo nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei virus informatici , suscettibili di ledere riservatezza, dignità e libertà delle persone, è del pari legittimo ricordare che solo siffatti strumenti sono oggi in grado di penetrare canali " criminali" di comunicazione o di scambio di informazioni utilizzati per la commissione di gravissimi reati contro le persone.

Così che, se si valuta l'impiego dei virus informatici in una delle loro molteplici funzionalità, quella relativa alle intercettazioni di conversazioni (l'unica peraltro che viene in rilievo nel presente giudizio di legittimità) si può ben sostenere che essi consentono **più che un potenziamento, un recupero dell'efficacia perduta o compromessa delle tecniche tradizionali.**

E' in questo contesto - caratterizzato dal dinamismo e dalla rapidissima evoluzione delle contrapposte tecnologie di "captazione" e di "elusione" - che emerge il ruolo prioritario del diritto e si percepisce l'estrema delicatezza e decisività del compito del giudice di legittimità.

E' il giudice di legittimità , infatti, che - interpretando le norme di diverso rango che regolano i nuovi fenomeni, leggendo tali fenomeni in tutta la loro complessità e bilanciando sapientemente interessi e valori in gioco – deve ricercare e indicare soluzioni che orientino e guidino correttamente le decisioni dei giudici di merito.

Chiarendo, in aderenza ai precetti della Costituzione e delle leggi, se e come le nuove tecniche di intercettazione possano essere usate nei termini strettamente necessari ed indispensabili per garantire le più elementari e vitali esigenze della sicurezza privata e collettiva, oggi spesso sottoposta a terribili minacce, e come restino fermi limiti invalicabili, a tutela di valori che stanno

egualmente a cuore ai cittadini , quali la inviolabilità e segretezza delle comunicazioni e la libertà delle persone e della loro sfera privata.

3. Sulle caratteristiche dei programmi di tipo " trojan horse" e sulle loro modalità di impiego per l'effettuazione di intercettazioni.

La dottrina che si è occupata dell'argomento ha fornito efficaci descrizioni dei programmi di tipo "*trojan horse*" e delle loro potenzialità per la captazione del contenuto di dati e programmi informatici nonché per la realizzazione delle stesse intercettazioni (1).

Si tratta di software che, prescindendo dalle autorizzazioni dell'utente, si installano su di un sistema scelto come "obiettivo" (sia esso un *personal computer* , un *tablet* od uno *smartphone*) e ne acquisiscono determinati poteri di gestione, funzionando come una sorta di microspia telematica.

Tali programmi sono concepiti e costruiti per installarsi in modo occulto sugli apparecchi da monitorare ed agiscono senza rivelare all'utente la propria presenza. In particolare essi comunicano attraverso Internet, in modalità nascosta e protetta, con un centro remoto di comando e controllo che li gestisce; catturano ciò che viene digitato sulla tastiera, visualizzato sullo schermo o detto al microfono; possono cercare tra i file presenti sul computer "ospite" o su altri connessi in rete locale; dispongono di contromisure che li rendono in grado di nascondersi ai più accreditati antivirus; sfruttano le vulnerabilità, spesso non ancora note, dei sistemi operativi o degli applicativi per aggirare controlli o contromisure che potrebbero ostacolarli od inibirli.

I *trojan horse* possono operare anche come le usuali cimici, o microspie per intercettazioni ambientali, fisicamente collocate nelle abitazioni, con la differenza che, in questo caso, si tratta di prodotti software installati surrettiziamente sul computer o altro apparecchio elettronico.

Nelle versioni più evolute questi software possono operare come veri e propri sistemi di controllo remoto (RCS: *remote control systems*), funzionare in modo autonomo, senza l'intervento diretto di persone responsabili, come strumenti (potenzialmente) onnipresenti ed "*always on*".

Come la dottrina (2) ha opportunamente sottolineato , per intercettare le comunicazioni realizzate attraverso l'impiego di apparati mobili collegati a WI-FI "aperte" o effettuate da utilizzatori di sistemi crittografati, è necessario avvalersi di un modello diverso dalle intercettazioni telematiche "classiche", fondate sulla assistenza tecnologica degli operatori che forniscono un accesso alla rete e dirette alla acquisizione dei soli dati che vi fluiscano "in chiaro".

Il *software trojan* si occupa della captazione della voce dell'utilizzatore e di quella dell'interlocutore dopo esser stata decifrata. Le informazioni così ottenute vengono mandate a *server* esterni, collocati presso la sala di ascolto. Ovviamente, questo avviene sfruttando la connettività del dispositivo elettronico scelto come *" obiettivo"*: laddove questo non abbia connettività, infatti, le informazioni verranno salvate in locale ed inviate al *server* non appena risulti disponibile un collegamento alla rete.

In sostanza tali *software* catturano quanto captato dal microfono e, conseguentemente, ogni qualvolta il computer risulti acceso con i microfoni attivati, potrà realizzarsi una vera e propria, intercettazione "ambientale".

La difficoltà maggiore riscontrabile in questo tipo di intercettazione è costituita dall'installazione del software RCS sul sistema *obiettivo* (la c.d "inoculazione") all'insaputa del suo possessore.

Installazione che può essere compiuta o mediante un accesso fisico al computer obiettivo o grazie ad installazione remota (attraverso l'invio di allegati con messaggi di posta elettronica o l'invio di comunicazioni provenienti da gestori dei servizi di messaggistica o *social network* o l'invio di aggiornamenti di software o di applicazioni).

Da ultimo , sempre in dottrina (3), si è segnalato che, tutte le volte in cui si parla di "captatore informatico" in ambito investigativo è necessario distinguere tra due diverse modalità operative : quella *on line search* e quella *on line surveillance*.

I programmi appartenenti alla categoria della *on line search* (modalità acquisitiva di dati) consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico individuato come obiettivo ; i dati e le informazioni sono quindi trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione tramite la rete Internet in modalità nascosta e protetta.

Attraverso i programmi che realizzano la c.d. *on line surveillance* (modalità captativa di flussi informativi) invece, è possibile captare il flusso informativo intercorrente tra le periferiche (video, tastiera, microfono, webcam, ecc.) e il microprocessore del dispositivo target, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo (*screenshot)*, digitato attraverso la tastiera (*keylogger*), detto attraverso il microfono, o visto tramite la webcam del sistema target controllato.

A conclusione di questa rapida disamina preliminare occorre mettere in luce un dato di estrema importanza.

La molteplicità di funzioni dei programmi informatici di cui si discute non deve indurre a credere di essere di fronte a strumenti onnipervasivi e onnipotenti, suscettibili di dar vita ad un potere invasivo esercitabile senza limiti o in forme incontrollabili sotto il profilo tecnico o giuridico.

Al contrario è seriamente ipotizzabile l'apposizione di limiti tecnici preventivi all'impiego dei virus informatici (ad es., inibendo *a priori* l'operatività di alcune delle loro molteplici funzioni acquisitive).

Inoltre, ciò che più conta in questa sede, è possibile dettare i limiti giuridici delle modalità di utilizzo dei captatori (ad es. escludendo che i programmi di *on line surveillance* possano essere utilizzati per effettuare videoriprese o che i programmi *on line search* siano impiegati per acquisire dati , al di fuori o in contrasto con le regole in tema di perquisizioni e sequestri).

Ancora una volta , dunque, come avviene del resto in altri delicatissimi campi dell'esperienza umana, sono la legge ed il diritto a fissare i confini delle possibilità offerte dalla tecnologia, commisurandole ai principi dello Stato democratico di diritto, ai diritti individuali ed alle esigenze e sensibilità della collettività.

4. Le ragioni della scelta di affrontare , con priorità, la terza delle questioni poste nell'ordinanza di rimessione , relativa alle intercettazioni tra presenti nei procedimenti per "delitti di criminalità organizzata".

Venendo ora all'esame del secondo motivo del ricorso sottoposto al giudizio delle Sezioni Unite e delle questioni poste nell'ordinanza di rimessione, si ritiene opportuno prendere le mosse dal terzo quesito formulato dal collegio rimettente nel quale si chiede *"se il decreto che dispone una intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico possa prescindere dalla indicazione dei luoghi dove deve avvenire la*

relativa captazione quando l'intercettazione sia disposta in un procedimento relativo a delitti di criminalità organizzata".

Vi sono più ragioni per scegliere di invertire l'ordine tracciato dall'ordinanza di rimessione.

In primo luogo le "intercettazioni tramite virus" , cui fa riferimento il ricorso all'esame delle Sezioni Unite , sono state disposte sulla base normativa offerta - oltre che dagli artt. 266 e ss. c.p.p. - dall'art. 13 del d.l. n. 152 del 1991, conv. nella l. n. 203 del 1991, e le loro risultanze sono state utilizzate nei confronti di un soggetto indagato per il reato di associazione di tipo mafioso (art. 416 bis, commi I, II, III, IV, e VI c.p.) , dunque in un procedimento per un delitto di criminalità organizzata.

Inoltre anche la sentenza della VI Sezione penale della Corte (la n. 27100 del 26.6.2015) , rispetto alla quale è stato sollevato il potenziale contrasto, aveva ad oggetto una intercettazione disposta nell'ambito di un procedimento di criminalità organizzata (anche se , come puntualmente rilevato nell'ordinanza di rimessione, la sentenza *" non sembra aver attribuito alcun rilievo a tale circostanza*" e non ha fatto menzione della legislazione speciale derogatrice di cui al citato art. 13 del d.l. n. 152/91).

Dunque tanto il ricorso in esame quanto il precedente giurisprudenziale rispetto al quale è stato formulato il potenziale contrasto riguardano misure cautelari ed intercettazioni nei confronti di soggetti indagati per il reato ex art. 416 bis c.p.p. nell'ambito di procedimenti per delitti di criminalità organizzata.

Ne consegue che la terza questione posta nell'ordinanza di rimessione - che investe la disciplina derogatrice dettata dal d.l. n. 152/91 – merita di essere esaminata con priorità essendo quella che ha più stretta , immediata e diretta aderenza al *thema decidendum* nel presente giudizio, mentre le prime due questioni investono la problematica delle intercettazioni per così dire ordinarie , disciplinate esclusivamente dagli artt. 266 e ss del codice di procedura.

Naturalmente sarà di straordinaria importanza anche l'insegnamento che le Sezioni Unite vorranno dare su questi ulteriori aspetti , egualmente cruciali , della problematica concernente le intercettazioni .

Ma è dalla risposta al terzo dei quesiti posti nell'ordinanza di rimessione che deriveranno le più dirette conseguenze giuridiche sul procedimento in esame e l'esito del giudizio di legittimità.

Infine, a giustificare l'inversione dell'ordine di trattazione delle questioni poste, sta la considerazione che i procedimenti per delitti di criminalità organizzata (nella rigorosa interpretazione che di questa locuzione legislativa verrà di seguito prospettata) presentano specificità tali, sul versante della disciplina legislativa e della realtà effettuale , da giustificare soluzioni peculiari ed all'occorrenza differenziate in tema di incisività dei mezzi di ricerca della prova impiegati e di contemperamento degli interessi e dei valori in campo.

Come si desume anche dai problemi affrontati nella ancora esigua ma significativa giurisprudenza di merito che si è formata sull'argomento, che viene ampiamente riportata in nota unitamente alle riflessioni critiche della dottrina sui primi provvedimenti adottati dai giudici di merito (4).

5. I dati normativi sui requisiti autorizzativi delle intercettazioni tra presenti : gli artt. 266 e ss. del codice di rito e la norma speciale derogatrice dettata dall'art. 13 del d.l. n. 152 del 1991 (conv. nella l. n. 203 del 1991).

Il tema da porre al centro della riflessione è quello delle "intercettazioni tra presenti" poste in essere , nell'ambito di un procedimento per delitti di criminalità organizzata, grazie all'installazione di un virus informatico in un apparecchio elettronico portatile in uso ad una persona , intercettazioni che sono necessariamente prive di una preventiva indicazione dei luoghi dove deve avvenire la relativa captazione .

Tema che può essere correttamente affrontato solo grazie ad una attenta lettura delle norme del codice di procedura e del testo della norma derogatrice dettata dal più volte citato art. 13 del d.l. n. 152/91.

E' significativo al riguardo che il codice di rito non parli di "intercettazioni ambientali" ma faccia invece riferimento ad *" intercettazioni di comunicazioni tra presenti"* (art. 266 , u.c. c.p.p.) nonché ad intercettazioni di comunicazioni tra presenti destinate ad avvenire *" nei luoghi indicati dall'art. 614 c.p."* (norma incriminatrice delle diverse fattispecie del reato di violazione del domicilio che a sua volta menziona le abitazioni, gli altri luoghi di privata dimora e le relative appartenenze).

Lo stesso vale per la norma speciale derogatrice che stabilisce : *" In deroga a quanto disposto dall'articolo 267 del codice di procedura penale, l'autorizzazione a disporre le operazioni previste dall'articolo 266 dello stesso codice è data, con decreto motivato, quando l'intercettazione è necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi…….Quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo a un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'articolo 614 del codice penale l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa."*

In sostanza le due categorie di intercettazioni deducibili dai testi normativi sono quella - ampia - delle *"intercettazioni di comunicazioni tra presenti"* e quella - più circoscritta - delle *"intercettazioni di comunicazioni tra presenti nei luoghi di privata dimora* ".

E queste ultime sono sottoposte a requisiti autorizzativi differenziati a seconda che siano disposte o meno in procedimenti per delitti di criminalità organizzata.

Non si vuol dire, con questo, che l'espressione " intercettazioni ambientali" , largamente impiegata dalla dottrina e dalla giurisprudenza , sia sbagliata o scorretta.

Ma è certo che la locuzione è entrata in uso e si è affermata in un periodo nel quale le possibilità di intercettazione in luoghi chiusi offerte dalle tecniche di captazione erano quasi sempre connesse alla installazione in uno o più "ambienti" predeterminati di microspie destinate alla captazione.

Se dunque la dizione di intercettazione ambientale non trova un diretto riscontro nel dato normativo (ma ha avuto la più ridotta funzione di descrivere efficacemente lo stato delle cose sino ad un certo stadio dello sviluppo tecnologico) essa non può essere "ipostatizzata" ed assunta come valido punto di partenza di un ragionamento che , enfatizzando il concetto di intercettazione ambientale giunga ad escludere la legittimità di ogni intercettazione tra presenti non strettamente collegata ad un predeterminato "ambiente".

A meno di non voler ripetere (*si parva licet componere magnis*) il percorso – a suo tempo magistralmente svelato e criticato da Riccardo Orestano - dei giuristi che , dopo aver elaborato, a

partire dalle norme, le categorie dogmatiche finivano poi con il ragionare solo o prevalentemente sulla base di queste ultime , svincolandosi progressivamente dai testi normativi.

6. Osservazioni critiche sull'orientamento espresso dalla sentenza n. 27100 del 2015.

Alla luce di queste lineari considerazioni l'orientamento espresso nella sentenza n. 2710072015, già oggetto dei rilievi di una parte della dottrina (5), stimola due considerazioni critiche.

La prima è di aver concentrato l'attenzione non sulla pregnante distinzione "normativa" tra intercettazioni tra presenti e intercettazioni tra presenti nei luoghi di privata dimora (e sui loro specifici requisiti autorizzativi) ma sulla distinzione , priva di agganci normativi, tra intercettazione tra presenti in ambienti predeterminati e intercettazioni prive di tale predeterminazione. .

Posizione, questa, evidente nei passaggi della sentenza nei quali si afferma che *"l'attivazione del microfono dà luogo ad una intercettazione ambientale "* ; che *"non sembra potersi dubitare che l'art. 266 , comma 2, c.p.p. nel contemplare l'intercettazione tra presenti , si riferisca alla captazione di conversazioni che avvengano in un determinato luogo e non ovunque"*; che *"l'intercettazione ambientale deve avvenire in luoghi ben circoscritti ed individuati ab origine"*.

La seconda, e per più versi decisiva, osservazione critica sta nel fatto che la sentenza sin qui discussa non ha preso in considerazione la norma speciale derogatrice ex art. 13 del d.l. n 152/91 che - per le intercettazioni domiciliari in procedimenti per delitti di criminalità organizzata – esclude espressamente il requisito autorizzativo previsto dall'art. 266, comma 2, c.p.p. e cioè la sussistenza di un *" fondato motivo di ritenere che nei luoghi"* di privata dimora *"si stia svolgendo l'attività criminosa."*

Per effetto di queste opzioni interpretative, la sentenza n. 27100/15 ha omesso di valutare l'incidenza del regime derogatorio sulla disciplina delle intercettazioni tramite captatori informatici, ponendosi in contrasto con altre recenti pronunce di codesta Corte .

Pronunce che avevano invece valorizzato la norma speciale per giungere alla conclusione della utilizzabilità delle intercettazioni tramite virus, proprio sul rilievo che *"le captazioni sono state disposte, trattandosi di reati in materia di criminalità organizzata, ai sensi dell'art 13 d.l. 13-5-1991 n. 152, conv. in l. 12-7-1991 n. 203, che testualmente prescinde dal predetto requisito, stabilendo che l'intercettazione di comunicazioni tra presenti è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 cod. pen. si stia svolgendo l'attività criminosa".* (così Cass., Sez. VI, 8/4/2015 n. 27536 e, in termini analoghi, Cass., Sez. VI, 12/3/2015 n. 24237).

Del resto la tesi sostenuta nella sentenza n. 27100/15 in ordine alla necessità di individuare con precisione, a pena di inutilizzabilità, i "luoghi" nei quali le intercettazioni tra presenti devono essere espletate non trova conferme in altre pronunce della Corte di cassazione.
La giurisprudenza precedente ha infatti sempre escluso la necessità di una siffatta indicazione, ad eccezione dei luoghi di privata dimora per i quali valga il disposto dell'art. 266 comma 2 c.p.p. (e non la norma derogatrice speciale).
Assolutamente esplicita è stata , in proposito, Cass., Sez. VI, n. 3541 del 5/11/1999, secondo cui «*l'intercettazione di comunicazioni tra presenti richiede l'indicazione dell'ambiente nel quale l'operazione deve avvenire solo quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 del codice penale. In tal senso i locali di uno stabilimento carcerario o, più ancora, la sala colloqui non sono luoghi di privata dimora*».
Laddove non si tratti di luoghi di privata dimora, la giurisprudenza ha ritenuto sufficiente, per le intercettazioni "ordinarie", l'indicazione della tipologia di ambienti dove eseguire le intercettazioni.

In tale prospettiva si è collocata Cass., Sez. I, n. 11506 del 25/2/2009, che ha considerato *"legittimo il decreto del pubblico ministero che disponga in via d'urgenza l'intercettazione dei colloqui con i familiari di alcuni detenuti senza indicare specificamente il luogo della intercettazione, che è sufficientemente individuabile nel riferimento alle sale colloqui della casa circondariale di detenzione"*.
La medesima *ratio* sta alla base anche dell'interpretazione accolta da Cass., Sez. II, n. 17894 dell'8/4/2014, secondo cui *"il trasferimento in altra struttura carceraria di un soggetto detenuto, nei cui confronti siano in corso operazioni di intercettazione ambientale regolarmente autorizzate, non comporta alcuna necessità di rinnovare il provvedimento autorizzativo delle attività di captazione ai fini della legittima prosecuzione delle stesse"*.
In altri termini , quando siano indicati i destinatari della captazione e la tipologia di ambienti (diversi dai luoghi di privata dimora) in cui eseguirla, l'intercettazione resta utilizzabile anche qualora venga effettuata in un altro luogo rientrante nella medesima categoria.
In particolare, il principio per cui sono utilizzabili i risultati delle intercettazioni di comunicazioni tra presenti anche quando nel corso dell'esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione, è stato affermato da Cass., Sez. VI, n. 15396/2008 dell'11/12/2007 , in una fattispecie nella quale l'autorizzazione dell'intercettazione tra presenti aveva ad oggetto la sala colloqui della casa circondariale dove si trovava l'imputato e le operazioni di captazione erano proseguite presso la sala colloqui della casa circondariale presso cui lo stesso era stato successivamente trasferito, e da Cass., Sez. V, n. 5956/2012 del 6/10/2011, in un caso in cui la captazione ambientale era stata trasferita dalla vettura oggetto di autorizzazione ad altra vettura successivamente acquistata dall'indagato sottoposto ad intercettazione.
Si tratta di un orientamento che trova il suo antecedente in Cass., Sez. I, n. 4561 del 30/6/1999, che ha ritenuto utilizzabili i risultati di una intercettazione ambientale autorizzata per una autovettura nella disponibilità dell'indagato ed eseguita su diversa autovettura, sempre nella sua disponibilità.
Ed è appunto riferendosi a tali pronunce, che una parte della dottrina ha parlato del riconoscimento della "dinamicità" delle intercettazioni, eseguibili in ambienti diversi frequentati dal soggetto sottoposto a controllo.

In conclusione sul punto, secondo l'interpretazione precedentemente consolidatasi nella giurisprudenza di legittimità:

-di regola il decreto autorizzativo delle intercettazioni tra presenti deve contenere la specifica indicazione dell'ambiente nel quale la captazione deve avvenire solo quando si tratti di luoghi di privata dimora (in cui tali intercettazioni ambientali possono essere effettuate, in base alla disciplina codicistica, soltanto se vi è fondato motivo di ritenere che in essi si stia svolgendo l'attività criminosa);

-per le intercettazioni tra presenti da espletare in luoghi diversi da quelli indicati dall'art. 614 c.p. (carceri, autovetture, capanni adibiti alla custodia di attrezzi agricoli, luoghi pubblici ecc.) è stato ritenuto sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti dove essa va eseguita; e l'intercettazione resta utilizzabile anche qualora venga effettuata in un altro luogo rientrante nella medesima categoria.

Sulla base di tali considerazioni relative alla pregressa giurisprudenza si può giungere ad un primo risultato interpretativo : l'indicazione del luogo o dell'ambiente della intercettazione tra presenti costituisce un imprescindibile requisito autorizzativo prescritto dal legislatore esclusivamente nei casi in cui occorre fare applicazione della disciplina codicistica sulle limitazioni delle captazioni effettuate nei luoghi di privata dimora.

Ed è , sotto questo profilo, che la soluzione adottata dalla sentenza n. 27100/15, in relazione ad un procedimento di criminalità organizzata, non può dirsi appagante.

7. I peculiari problemi posti da una modalità di intercettazione tra presenti attraverso un captatore informatico. La normativa ordinaria.

E' ora necessario confrontarsi , con riferimento al caso di specie, con le indubbie peculiarità delle intercettazioni tramite captatore informatico , che possono divenire intercettazioni "itineranti" suscettibili – ove il detentore porti con sé l'apparecchio nel quale è stato inoculato il virus – di penetrare in più luoghi di privata dimora.

Con la fondamentale avvertenza che nel procedimento nel quale è stata adottata l'ordinanza oggetto del presente ricorso per cassazione :

a) risulta che il captatore informatico utilizzato è stato impiegato esclusivamente per effettuare intercettazioni di comunicazioni tra presenti, i cui contenuti sono stati riversati nell'ordinanza del giudice per le indagini preliminari e sono state valutati e ripresi nella motivazione dell'ordinanza del Tribunale del riesame;
b) il giudice per le indagini preliminari ha espressamente negato l'autorizzazione all'utilizzo del captatore per l'effettuazione di videoriprese;
c) non risulta che il captatore informatico sia stato utilizzato per compiere operazioni di acquisizione dei contenuti dell'apparecchio infiltrato,

Esulano dunque dalla sfera del presente giudizio di legittimità aspetti diversi da quelli propri delle intercettazioni foniche ed in particolare :

a) l'effettuazione di videoriprese all'interno dell'abitazione dell'intercettato (o in altri luoghi sensibili sotto il profilo della tutela della riservatezza personale) in ordine alle quali va richiamato l'insegnamento delle Sezioni Unite nella sentenza n. 26795 del 28.3.2006 (6) ;

b) il compimento, a mezzo del virus, di attività di perquisizione e sequestro dei dati contenuti nell'apparecchio elettronico, con modalità sostanzialmente occulte e comunque tali da vanificare o ritardare ingiustificatamente il diritto del destinatario del sequestro a proporre richiesta di riesame e ricorso per cassazione.

Così circoscritto il *thema decidendum,* chi scrive ritiene che la più volte richiamata normativa derogatoria speciale non preclude che il giudice autorizzi , motivando adeguatamente e coerentemente le sue determinazioni, le particolari intercettazioni foniche oggi rese possibili dall'uso dei captatori informatici.

In particolare nessuna preclusione o controindicazione normativa è rinvenibile riguardo alle intercettazioni foniche realizzate in luoghi pubblici ed aperti e riguardo alle captazioni nel domicilio del soggetto intercettato , se si considera che, già sulla base della disciplina vigente, questi potrebbe essere destinatario di un decreto del giudice che estenda motivatamente le intercettazioni tradizionali ad una pluralità di stanze della sua abitazione o alle relative pertinenze.

Come si è accennato, il profilo fortemente problematico del tema in discussione è un altro ed attiene alla possibilità che il soggetto intercettato si rechi, portando con sé l'apparecchio elettronico nel quale è stato inoculato il virus, nei luoghi di privata dimora di altre persone , dando così vita ad altrettante intercettazioni domiciliari.

E' opinione di chi scrive che su questo particolare aspetto della questione il legislatore abbia già fornito , sia pure in un contesto tecnologico diverso da quello attuale, una chiara indicazione quando ha espressamente escluso - per le intercettazioni tra presenti in luoghi di privata dimora disposte in procedimenti di criminalità organizzata - il requisito autorizzativo previsto dall'art. 266, comma 2, c.p.p. per tutte le altre intercettazioni

Nella norma derogatoria è infatti prefigurato un peculiare e specifico bilanciamento di interessi nel cui ambito la segretezza delle comunicazioni e la tutela del domicilio subiscono più consistenti limitazioni in ragione della eccezionale gravità e pericolosità, per gli individui e per la intera collettività , dei reati dei quali si ricerca la prova.

Bilanciamento che si è tradotto nella possibilità di effettuare , previa motivata valutazione del giudice, intercettazioni tra presenti in luoghi di privata dimora "a prescindere" dalla dimostrazione che essi siano sedi di attività criminose in atto.

A ben guardare in tale opzione legislativa si colgono due dati.

Da un lato il segnale normativo della estrema incisività dei mezzi di ricerca della prova da mettere in campo nei confronti dei delitti propri della criminalità organizzata.

Dall'altro lato, il riflesso del carattere per così dire "totalizzante" dei delitti della grande criminalità organizzata, che , per essere ideati , programmati e portati a compimento, reclamano attività che possono, e spesso debbono, svolgersi in permanenza e in tutti i luoghi frequentati dai soggetti sospettati di esserne gli autori; così da rendere all'occorrenza necessaria una compressione di diritti assai più intensa di quella realizzabile nel corso di investigazioni per altri pur gravi reati o nei confronti di altri soggetti.

In altri termini , introducendo la norma derogatrice dell'art. 13 del d.l. n. 152, il legislatore ha accettato – limitatamente ai procedimenti per delitti di criminalità organizzata - il "rischio" di intercettazioni che si svolgano in luoghi di privata dimora anche nei casi in cui non sia fondatamente ipotizzabile che in essi siano in corso attività criminose.

Ed è alla luce di questa "accettazione" , frutto di un accurato e risalente contemperamento di valori ed interessi, che l'eventualità di intercettazioni domiciliari- conseguenti alle modalità impiego ed alla mobilità dell'apparecchio elettronico sede del captatore - non appare in contrasto con la normativa vigente in tema di intercettazioni e non risulta confliggente (come si dirà più ampiamente in seguito) con le norme di rango costituzionale poste a presidio della segretezza delle comunicazioni, del domicilio e della riservatezza.

D'altro canto è appena il caso di ricordare che il più ampio tema delle "intercettazioni casuali" non è nuovo ed è stato più volte affrontato e risolto della giurisprudenza della Corte costituzionale e del giudice di legittimità in sentenze che non hanno mai optato per soluzioni di pregiudiziale negazione e inutilizzabilità ma hanno attentamente esercitato l'arte della distinzione, sceverando le intercettazioni oggetto di preclusioni normative assolute o sottoposte a specifici regimi autorizzativi preventivi da quelle per le quali nella legge tali requisiti non sono rinvenibili (cfr. al riguardo Corte cost. n. 390 del 2007; Corte cost. n. 113 del 2010; Corte cost. n. 114 del 2010 ; Cass. , II, 16.11.2012 , sulle intercettazioni dirette o casuali dei parlamentari).

7.1. Segue…. gli artt. 15 e 14 della Costituzione.

Nella sentenza n. 27100/15 il collegio della Vi Sezione penale ha invocato , a sostegno della soluzione adottata, la garanzia costituzionale prevista dall'art. 15 della Costituzione, sostenendo, tra l'altro che *" una corretta ermeneutica della norma di cui all'art. 15 della Costituzione osta …all'attribuzione al disposto dell'art. 266, 2 comma, c.p.p. di una latitudine operativa così ampia da ricomprendere intercettazioni ambientali effettuate in qualunque luogo*" : il che sarebbe inibito *" prima ancora che dalla normativa codicistica , dal precetto costituzionale"* invocato.

A parte il rilievo critico , già ampiamente svolto, che il collegio - pur pronunciandosi in ordine alla legittimità di intercettazioni disposte in un procedimento di criminalità organizzata - ha ritenuto di espungere dal raggio della sua attenzione e delle sue argomentazioni il riferimento alla disciplina derogatrice, è agevole osservare che nella fattispecie l'intercettazione è stata disposta, come prescritto dalla carta fondamentale, con "atto motivato dell'autorità giudiziaria" (art. 15, comma 2, Cost.)

La discussione si sposta dunque sul rispetto dell'altro requisito necessario per l'imposizione di limitazioni alla libertà in questione e cioè il rispetto delle "garanzie stabilite dalla legge" (art. 15, comma 2, Cost.), ritornando al tema della disciplina dettata dalle leggi ordinarie sino ad ora esaminato.

Con il naturale corollario che il precetto costituzionale derivante dall'art. 15 della carta non può essere considerato – come ritiene Cass. 27100/2015 - "di per sé" ostativo alle intercettazioni ma va letto in stretta congiunzione con le norme del codice di rito e delle altre leggi regolanti le intercettazioni di cui si discute.

Se mai , a fronte della indubbia "novità" di intercettazioni itineranti e potenzialmente ubiquitarie, suscettibili di penetrare in una pluralità di luoghi di privata dimora , appare maggiormente rilevante la garanzia accordata dal legislatore costituente al domicilio (art. 14 Cost.).

Al riguardo meritano di essere attentamente meditati (anche per le preziose indicazioni di metodo che offrono) alcuni illuminanti passaggi della sentenza n. 135 del 2002 nei quali si sostiene che :
" *il riferimento, nell'art. 14, secondo comma, Cost., alle "ispezioni, perquisizioni e sequestri" non é necessariamente espressivo dell'intento di "tipizzare" le limitazioni permesse, escludendo a contrario quelle non espressamente contemplate; poichè esso ben può trovare spiegazione nella circostanza che gli atti elencati esaurivano le forme di limitazione dell'inviolabilità del domicilio storicamente radicate e positivamente disciplinate all'epoca di redazione della Carta, non potendo evidentemente il Costituente tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnici successivi.*
Per un altro verso, va osservato che la citata disposizione costituzionale, nell'ammettere "intrusioni" nel domicilio per finalità di giustizia, non prende, in realtà, affatto posizione sul carattere — palese od occulto — delle intrusioni stesse: la configurazione di queste ultime, e delle ispezioni in particolare, come atto palese emerge, difatti, esclusivamente a livello di legislazione ordinaria.
L'attribuzione all'elenco delle limitazioni alla libertà di domicilio, di cui all'art. 14, secondo comma, Cost., di un carattere "chiuso" e storicamente "cristallizzato" sulla fisionomia impressa dalla legge processuale del tempo ai singoli atti invasivi richiamati provocherebbe, d'altro canto, un evidente squilibrio nell'assetto costituzionale dei diritti di libertà.
Nel sistema delle libertà fondamentali, difatti, la libertà domiciliare si presenta strettamente collegata alla libertà personale, come emerge dalla stessa contiguità dei precetti costituzionali che sanciscono l'una e l'altra (artt. 13 e 14 Cost.), nonchè dalla circostanza che le garanzie previste nel secondo comma dell'art. 14, Cost., in rapporto alle limitazioni dell'inviolabilità del domicilio, riproducono espressamente quelle stabilite per la tutela della libertà personale.
Il domicilio viene cioé in rilievo, nel panorama dei diritti fondamentali di libertà, come proiezione spaziale della persona, nella prospettiva di preservare da interferenze esterne comportamenti tenuti in un determinato ambiente: prospettiva che vale, per altro verso, ad accomunare la libertà in parola a quella di comunicazione (art. 15 Cost.), quali espressioni salienti di un più ampio diritto alla riservatezza della persona.
Ciò posto, l'adesione alla tesi contrastata implicherebbe che il domicilio trovi tutela nella Carta

costituzionale — quanto alla tipologia delle interferenze da parte della pubblica autorità — in modo più energico, non solo rispetto alla libertà e alla segretezza delle comunicazioni (l'art. 15, secondo comma, Cost. fa generico riferimento, infatti, a possibili "limitazioni" di essa, senza alcuna restrizione quanto ai tipi); ma altresì rispetto alla stessa libertà personale, di cui l'inviolabilità del domicilio costituisce espressione in certo senso sotto-ordinata (l'art. 13, secondo comma, Cost., infatti, consente, a determinate condizioni, oltre alla "detenzione", "ispezione" e "perquisizione personale", "qualsiasi altra forma di restrizione della libertà personale"). Una simile ricostruzione appare tanto meno plausibile ove si consideri che nel terzo comma dell'art. 14 Cost. — per quanto attiene ai motivi ed ai modi della limitazione — la protezione costituzionale del domicilio risulta, viceversa, più debole di quella degli altri diritti di libertà dianzi menzionati; si ammette infatti in tale comma, in termini ampi, che "leggi speciali" consentano di eseguire "accertamenti e ispezioni" domiciliari anche per motivi "di sanità e di incolumità pubblica o a fini economici e fiscali".
Giova soggiungere che l'ipotizzata restrizione della tipologia delle interferenze della pubblica autorità nella libertà domiciliare non troverebbe riscontro nè nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (art. 8), nè nel Patto internazionale sui diritti civili e politici (art. 17); nè, infine, nella Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza nel dicembre 2000 (artt. 7 e 52), qui richiamata – ancorchè priva di efficacia giuridica – per il suo carattere espressivo di principi comuni agli ordinamenti europei."

Ed è su questa base che la Corte costituzionale ha escluso l'esistenza di un divieto costituzionale assoluto alla *"captazione di immagini in luoghi di privata dimora"* che si configuri *"come una forma di intercettazione di comunicazioni fra presenti, che si differenzia da quella operata tramite gli apparati di captazione sonora solo in rapporto allo strumento tecnico di intervento, come nell'ipotesi di riprese visive di messaggi gestuali: fattispecie nella quale già ora é applicabile, in via interpretativa, la disciplina legislativa della intercettazione ambientale in luoghi di privata dimora"* ed ha concluso il suo ragionamento con l'affermazione che *"stabilire quando la ripresa visiva possa ritenersi finalizzata alla captazione di comportamenti a carattere comunicativo e determinare i limiti entro i quali le immagini concretamente riprese abbiano ad oggetto tali comportamenti é…….questione che spetta al giudice a quo risolvere"*.

In forza di tali argomentazioni si può dunque escludere che anche l'art. 14 della Costituzione contenga divieti costituzionali assoluti in materia di intercettazioni foniche all'interno di luoghi di privata dimora e sia invocabile a prescindere dalle leggi ordinarie in materia di intercettazioni.

7.2. Segue…..l'art. 8 della Convenzione europea dei diritti dell'uomo.

Occorre infine verificare se l'art. 8 della Convenzione europea dei diritti dell'uomo si ponga come insormontabile ostacolo alla adozione delle intercettazioni in discussione.

Come è noto , in tale norma all'enunciazione del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, compiuta dal primo comma, si accompagna la c.d. clausola di limitazione contenuta nel secondo comma, che subordina l'ammissibilità di ogni ingerenza dell'autorità pubblica nel loro esercizio alla realizzazione di tre requisiti:

-la previsione legislativa; al riguardo la Corte di Strasburgo – che ha elaborato una concezione "materiale" (e non formale) del termine "legge", comprensiva sia del diritto scritto che del diritto non scritto - ha manifestato una forte attenzione per gli aspetti qualitativi della legalità, richiamando i profili della accessibilità e conoscibilità delle fonti normative e della relativa giurisprudenza, e quelli della sufficiente chiarezza e precisione circa l'ampiezza ed i limiti del potere discrezionale dell'autorità nazionale chiamata ad attuare l'ingerenza; in proposito, si è evidenziata la necessità che il cittadino possa disporre di informazioni sufficienti a consentirgli di regolare la sua condotta e

di prevederne ragionevolmente le conseguenze (sent. 26 aprile 1979, Sunday Times c. Regno Unito);

-il perseguimento di una delle finalità legittime, tassativamente indicate dalla norma, che ricomprendono sia una ampia serie di interessi dello Stato e della collettività (la sicurezza nazionale, la pubblica sicurezza, il benessere economico del paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale), sia la protezione dei diritti e delle libertà altrui;

-la necessità della misura, nell'ambito di una società democratica, per il conseguimento dei predetti obiettivi; si tratta di una valutazione imperniata su un giusto bilanciamento tra le esigenze di tutela di interessi generali e la protezione dei diritti individuali (sent. 7 luglio 1989, Soering c. Regno Unito); in tale prospettiva ogni ingerenza, per essere compatibile con la norma convenzionale, deve rispondere a un bisogno sociale imperativo e risultare proporzionata alla finalità legittima perseguita.

La giurisprudenza della Corte europea dei diritti dell'uomo ha ritenuto che l'art. 8 della Convenzione imponga allo Stato non soltanto l'obbligo negativo di astenersi da ingerenze arbitrarie nel godimento dei suddetti diritti (evitando, quindi, ogni misura limitativa che non soddisfi le tre condizioni sopra indicate), ma anche l'obbligo positivo di rendere effettivo l'esercizio dei diritti da parte dell'individuo e di proteggerlo contro le ingerenze poste in essere dai terzi (c.d. effetto orizzontale indiretto), adottando le opportune misure legislative, amministrative e giudiziarie.

Inoltre, la Corte di Strasburgo ha progressivamente elaborato una interpretazione evolutiva, fortemente dinamica, che ha condotto a un deciso ampliamento dell'ambito di applicazione della norma convenzionale.

Così dal diritto al rispetto della vita privata è stato enucleata, quale "applicazione settoriale" che gioca un ruolo fondamentale per l'esercizio del primo, anche la **protezione dei dati personali**, cui è stata estesa la tutela prevista dall'art. 8 della CEDU, interpretato alla luce della Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (il cui art. 2 adotta una nozione assai ampia di «dati a carattere personale», includendovi ogni informazione concernente una persona fisica identificabile).

La giurisprudenza della Corte di Strasburgo ha quindi definito i confini della raccolta e conservazione da parte delle autorità nazionali di dati personali, della loro divulgazione, e del diritto di accesso dell'interessato ai propri dati. In particolare, si è configurato a carico dello Stato sia un obbligo negativo, di non divulgare indebitamente i dati contro la volontà del soggetto cui si riferiscono (sent. 25 febbraio 1997, Z. c. Finlandia; sent. 29 giugno 2006, Panteleyenko c. Ucraina), sia un obbligo positivo, di consentire all'individuo l'accesso ai propri dati personali detenuti dalla pubblica autorità, nonché la facoltà di confutarli (sent. 26 marzo 1987, Leander c. Svezia).

Anche il concetto di corrispondenza è stato inteso secondo un'ampia accezione che comprende ogni forma di comunicazione privata, come le conversazioni telefoniche, le e-mail (sent. 3 aprile 2007, Copland c. Regno Unito) e vari tipi di messaggi.

Nell'ottica di evitare ogni interpretazione restrittiva del diritto alla vita privata, la nozione di "domicilio" è stata estesa dalla Corte europea dei diritti dell'uomo alla sede sociale, alle filiali e agli altri locali professionali di pertinenza di società (sent. 16 aprile 2002, Société Colas Est e altri c. Francia).

Nell'interpretazione dell'art. 8 della Convenzione, la giurisprudenza della Corte europea dei diritti dell'uomo ha elaborato, con riguardo alla materia delle intercettazioni, criteri più rigorosi di quelli ordinari, individuando uno specifico nucleo minimo di garanzie che giustifica l'ingerenza da esse arrecata nel diritto al rispetto della vita privata sotto i tre profili, tra di loro interconnessi, dell'esistenza di una base giuridica appropriata, della finalità legittima e della necessità in una società democratica (cfr. sent. 10 febbraio 2009, Iordachi c. Moldavia; sent. 29 maggio 2001, Taylor-Sabori c. Regno Unito).

Di particolare importanza appaiono i principi affermati con riguardo ai requisiti della previsione legislativa. La consapevolezza dell'evidente rischio di arbitrio insito in un potere esercitato in segreto ha indotto la Corte di Strasburgo ad affermare la necessità di regole chiare e dettagliate sulle intercettazioni, che indichino l'ambito della discrezionalità e le modalità di esercizio del potere conferito alle autorità competenti e diano ai cittadini una adeguata indicazione sulle circostanze e sulle condizioni in presenza delle quali è consentito il ricorso a tali misure.

In quest'ottica, le garanzie minime di contenuto che la normativa interna deve apprestare per evitare abusi di potere sono stati individuati nei seguenti elementi:

- la indicazione della natura dei reati che possono dare luogo a un ordine di intercettazione;
- la predeterminazione della tipologia delle comunicazioni intercettabili;
- la definizione delle categorie di persone le cui utenze telefoniche possono essere sottoposte ad intercettazione;
- il limite di durata delle intercettazioni;
- la procedura da seguire per esaminare, utilizzare e conservare i dati ottenuti (segnatamente, le precauzioni da prendere per comunicare le registrazioni, intatte e nella loro interezza, in modo da renderne possibile l'esame da parte del giudice e della difesa, e le cautele da adottare nel comunicare i dati ad altre parti);
- le circostanze in cui le registrazioni possono o devono essere distrutte, in particolare nel caso di proscioglimento dell'accusato;
- l'attribuzione ad un organo indipendente della competenza ad autorizzare le intercettazioni;
- la previsione del controllo del giudice (o comunque di un organo indipendente) sia sulle ragioni giustificatrici dell'interferenza, sia sulle concrete modalità della sua esecuzione.

Quest'ultimo aspetto risponde all'esigenza di predisporre controlli rigorosi al fine di garantire una tutela adeguata e concreta contro gli abusi da parte dell'autorità, pur non essendo stata prescritta dall'art. 8 della Convenzione una espressa riserva di giurisdizione.

Le suesposte indicazioni relative al contenuto della previsione legislativa si intrecciano con quelle concernenti il profilo teleologico, e segnatamente la verifica da compiere sulla necessità che il perseguimento dei fini corrisponda al mantenimento di una società democratica.

I parametri dai quali si misura la "necessità democratica" che giustifica l'ingerenza della pubblica autorità nella comunicazione privata sono quelli della proporzionalità e del controllo: l'ingerenza deve essere proporzionata rispetto alla giustificazione invocata, e deve sottostare ad un sistema di controllo adeguato ed effettivo, così da controbilanciare ed arginare «il pericolo insito nell'azione segreta di una parte dell'apparato dello Stato sul cittadino» (sent. 24 aprile 1990, Kruslin c. Francia).

Oltre a definire nei termini sopra indicati il contenuto dell'obbligo negativo di astenersi da interferenze arbitrarie, la Corte di Strasburgo (sent. 17 luglio 2003, Craxi c. Italia), partendo dall'idea che l'art. 8 pone a carico dello Stato un obbligo positivo di assicurare l'effettivo rispetto della *privacy*, ha affermato che le autorità nazionali sono tenute a impedire la pubblicazione sulla

stampa di conversazioni telefoniche intercettate aventi carattere strettamente privato e prive di rilevanza nel procedimento penale. Nell'ipotesi in cui in cui le misure finalizzate ad evitare la divulgazione di tali intercettazioni si siano rivelate insufficienti, le autorità nazionali hanno il dovere di iniziare un'inchiesta efficace per chiarire come gli organi di informazione abbiano avuto accesso a tale documentazione, e per punire, ove necessario, i responsabili di eventuali violazioni di legge.

La Corte europea dei diritti dell'uomo ha ritenuto imputabile allo Stato anche l'ingerenza nel diritto alla vita privata insita nell'intercettazione materialmente eseguita da un soggetto privato che registri le proprie conversazioni con altri su suggerimento della polizia, la quale, senza previa autorizzazione dell'autorità giudiziaria, provveda all'istallazione dei relativi dispositivi (sent. 8 aprile 2003, M.M. c. Paesi Bassi).

Importanti indicazioni sui requisiti qualitativi e contenutistici della normativa nazionale in materia di intercettazioni sono stati forniti dalla recente sentenza emessa il 4 dicembre 2015 dalla Grande Camera della Corte europea dei diritti dell'uomo nel caso Zakharov c. Russia.

La Corte ha anzitutto sottolineato la necessità di regole chiare e dettagliate sulle intercettazioni, specialmente perché la tecnologia disponibile diviene continuamente più sofisticata.

Inoltre, la Corte europea ha fornito significative precisazioni sui seguenti aspetti:

a) area di operatività delle intercettazioni; in proposito la Corte ha ribadito che la legislazione nazionale deve definire l'ambito di applicazione delle predette misure dando ai cittadini un'adeguata indicazione delle circostanze in cui le autorità pubbliche hanno il potere di ricorrervi, in particolare mediante una chiara definizione della natura dei reati che possono dare luogo a un ordine di intercettazione e delle categorie di persone le cui utenze telefoniche possono essere sottoposte ad intercettazione; per quanto attiene alla natura dei reati, la Corte ha sottolineato che la condizione della prevedibilità non richiede che gli Stati indichino esaustivamente e nominativamente le specifiche ipotesi criminose che possono dar luogo ad intercettazioni; comunque devono essere forniti sufficienti dettagli sulla natura di tali reati, ad esempio mediante la indicazione del massimo di pena edittale per essi prevista; con riferimento alla definizione dei potenziali destinatari delle intercettazioni, la Corte ha evidenziato che le intercettazioni possono essere ordinate non solo nei confronti di un indiziato o di un accusato, ma anche di una persona che possa essere in possesso di informazioni relative a un reato o comunque rilevanti per il procedimento penale;
b) durata delle misure di sorveglianza segreta; sul punto la Corte ha ritenuto che non sia irragionevole lasciare la complessiva durata delle intercettazioni alla discrezione delle autorità nazionali competenti per ordinare e rinnovare gli ordini di intercettazione, purché esistano adeguate garanzie, come una chiara indicazione nella legislazione interna del periodo dopo il quale un ordine di intercettazione perde la sua efficacia, delle condizioni di cui è subordinata la sua rinnovazione, e delle circostanze nelle quali l'attività di intercettazione deve cessare;
c) procedure da seguire per la conservazione, l'accesso, l'esame, l'uso, la comunicazione e la distruzione dei dati ottenuti mediante le intercettazioni; in proposito la Corte ha espresso un apprezzamento positivo per la normativa che regola la conservazione, l'uso e la comunicazione dei dati in modo da minimizzare il rischio di un accesso o di una rivelazione in mancanza di autorizzazione, mentre ha richiesto che la legislazione contenga la previsione della immediata distruzione di tutti i dati chiaramente irrilevanti per lo scopo in funzione del quale sono stati ottenuti (come nel caso in cui non venga formulata una accusa penale a carico del destinatario della captazione) e fornisca

indicazioni sulle circostanze nelle quali il contenuto dalle intercettazioni può essere conservato dopo la fine del processo (suscitando preoccupazione la previsione legislativa che lascia al giudice del dibattimento una illimitata discrezionalità sulla conservazione o distruzione dei dati usati come prove dopo la fine del processo);

d) procedure di autorizzazione: in proposito, la Corte europea ha attribuito rilievo a un insieme di fattori, che attengono in particolare;
- all'autorità competente per l'autorizzazione; sotto tale profilo, si è ritenuta compatibile con la convenzione anche l'attribuzione della competenza ad autorizzare le intercettazioni telefoniche ad una autorità non giudiziaria, purché essa sia sufficientemente indipendente dal potere esecutivo;
- alla ampiezza della valutazione affidata alla autorità competente per l'autorizzazione, che deve avere il potere di verificare l'esistenza di un ragionevole sospetto a carico della persona interessata, nonché la presenza, nell'intercettazione richiesta, dei requisiti della necessità in una società democratica e della proporzione rispetto al fine legittimo perseguito (ad esempio, sotto il profilo della possibilità di raggiungere lo scopo con mezzi meno invasivi);
- al **contenuto della autorizzazione all'intercettazione, che deve identificare chiaramente la specifica persona da porre sotto sorveglianza oppure l'unico insieme dei luoghi rispetto ai quali viene ordinata l'intercettazione**; una simile identificazione può essere fatta per mezzo di nomi, indirizzi, numeri di telefono o altre informazioni pertinenti (sul punto, la Corte ha richiamato le sentenze già emesse rispettivamente il 6 Settembre 1978 nel caso Klass e altri c. Germania, § 51, il 1° luglio 2008 nel caso Liberty e altri c. Regno Unito, §§ 64-65, il 26 aprile 2007 nel caso Dumitru Popescu c. Romania, § 78, il 28 giugno 2007 nel caso Association for European Integration and Human Rights e Ekimdzhiev c. Bulgaria, § 80, e il 18 maggio 2010 nel caso Kennedy c. Regno Unito, § 160).

e) accesso delle autorità alle comunicazioni: la Corte ha considerato il requisito della presentazione dell'autorizzazione alle intercettazioni al fornitore di servizi di comunicazione prima di ottenere l'accesso alle comunicazioni di un soggetto come una importante garanzie contro gli abusi da parte delle autorità di polizia;

f) supervisione sull'implementazione delle misure di sorveglianza segreta fondate su una appropriata autorizzazione giudiziaria: sul tema la Corte europea in precedenza ha ritenuto che, pur essendo in linea di principio desiderabile che una simile attività di controllo sia affidata ad un giudice, anche la supervisione da parte di un organo non giudiziario può essere considerata compatibile con la Convenzione, purché si tratti di un organo indipendente dalle autorità che attuano la sorveglianza e investito di sufficienti poteri e competenza per esercitare un controllo continuo ed effettivo;

g) successiva comunicazione delle intercettazioni e rimedi disponibili: in proposito la Corte europea ha osservato che nella pratica può risultare impossibile di richiedere la successiva comunicazione in tutti i casi, sia perché l'attività o il pericolo contro cui una particolare serie di misure di sorveglianza è rivolta può continuare anche per decenni dopo la sospensione delle stesse misure, con la conseguenza che una simile comunicazione pregiudicherebbe le finalità di lungo termine che hanno suggerito il ricorso alla sorveglianza, sia perché tale comunicazione potrebbe rivelare i metodi di lavoro e i campi di operazione dei servizi segreti e persino identificarne gli autori; pertanto dalla mancata comunicazione delle intercettazioni ai loro destinatari una volta che le stesse siano cessate non può di per sé trarsi la conclusione che si tratti di una interferenza non necessaria in una società democratica, giacché è proprio l'ignoranza della sorveglianza che assicura l'efficacia dell'interferenza; tuttavia, nella misura in cui la successiva comunicazione può essere effettuata senza pregiudicare lo scopo della misura dopo la cessazione di essa, si dovrebbero fornire le relative informazioni al destinatario; la Corte europea ha inoltre

> sottolineato che la questione della successiva comunicazione delle intercettazioni condiziona l'effettività dei rimedi disponibili per le persone che si rivolgono all'autorità giudiziaria lamentando una violazione dei propri diritti conseguente all'intercettazione delle loro comunicazioni; infatti la effettività di tali rimedi viene minata quando la legittimazione a presentarli è ristretta esclusivamente alle persone che hanno avuto notizia delle intercettazioni nel quadro dei procedimenti penali instaurati nei loro confronti, e non anche a coloro che non sono stati sottoposti a un procedimento penale, non vengono informati delle intercettazioni eseguite a loro carico, e non hanno diritto di richiedere e ottenere informazioni sulle intercettazioni.

Dalla sentenza Zakharov si desume quindi con chiarezza che non è necessario che nel provvedimento autorizzativo delle intercettazioni siano indicati i luoghi in cui le stesse devono svolgersi, purché ne venga identificato chiaramente il destinatario.

I due requisiti contenutistici di tale provvedimento – e cioè la specifica persona da porre sotto sorveglianza oppure l'unico insieme dei luoghi rispetto ai quali viene ordinata l'intercettazione – sono, infatti, alternativi tra di loro.

Anche sotto questo profilo, dunque, non si rinvengono, nell'art. 8 della CEDU , così come interpretato nella giurisprudenza della Corte di Strasburgo, assolute preclusioni riguardanti le intercettazioni effettuate mediante captatore informatico in procedimenti come quelli per delitti di criminalità organizzata in ordine ai quali appare indiscutibilmente rispettato il principio di proporzione tra l'incisività del mezzi usati e la "regolata" compressione dei diritti fondamentali delle persone che ne deriva, a fini di tutela di esigenze vitali di uno Stato democratico di diritto.

7.3. Il bilanciamento possibile.

Le minacce terribili che la grande criminalità organizzata ed oggi con gravità crescente le organizzazioni terroristiche muovono alla vita ed alle libertà delle persone ed alla sicurezza collettiva rendono evidente che è ravvisabile la "*necessità della misura nell'ambito di una società democratica"* , su cui opportunamente insiste la Corte di Strasburgo.

Né, come ci si è sforzati di sostenere, si profilano ostacoli insormontabili alla legittimazione, nel nostro ordinamento, dello sfruttamento , nel campo delle intercettazioni tra presenti, delle potenzialità captative dei virus informatici.

A patto, naturalmente, che tale impiego, una volta ritenuto indispensabile per la ricerca della prova , sia rigorosamente circoscritto attraverso prescrizioni tecniche d'impiego e limitazioni di ordine giuridico fissate dal giudice ed altrettanto rigorosamente controllato sotto il profilo della gestione dei programmi e della esecuzione delle attività captative (7).

Sull'altro versante, a chi sia legittimamente preoccupato che il nuovo strumento captativo possa produrre , in casi limite, esiti lesivi della dignità umana si può rispondere che l'ordinamento, anche attingendo alla fonte dei principi costituzionali e facendone diretta applicazione, ha gli strumenti per neutralizzare tali pericoli.

Ad esempio , facendo discendere dal principio personalistico enunciato dall'art. 2 della Costituzione, e dalla tutela della dignità della persona che ne deriva, la sanzione di inutilizzabilità delle risultanze di "specifiche" intercettazioni che nelle loro modalità di attuazione e/o nei loro esiti abbiano acquisito "in concreto" connotati direttamente lesivi della persona e della sua dignità .(8)

8. La nozione di “delitti di criminalità organizzata” nell’art. 13 del d.l. n. 152 del 1991.

A completamento delle argomentazioni sin qui svolte appare utile sollecitare un’ulteriore riflessione (ed all’occorrenza un ripensamento o una precisazione) delle Sezioni Unite sulla nozione di *“delitti criminalità organizzata*” di cui all’art. 13 del d.l. n. 152 del 1991.

Come è noto la giurisprudenza di codesta Corte è già più volte intervenuta sul tema al fine di definire il significato e la portata della espressione usata dal legislatore.

Così, da ultimo, Cass. VI, n. 28602 del 19.3.2013 ha affermato che *“ in tema di intercettazioni, la nozione di "delitti di criminalità organizzata” di cui all'art. 13, D.L. n. 152 del 1991 (conv. in l. 203 del 1991), ricomprende nel suo ambito applicativo attività criminose diverse, purché realizzate da una pluralità di soggetti i quali, per la commissione del reato, abbiano costituito un apposito apparato organizzativo, talchè sono ad essa riconducibili non solo i reati di criminalità mafiosa e assimilati, ma tutte le fattispecie criminose di tipo associativo”.*

In termini sostanzialmente analoghi si erano precedentemente espresse , su identica questione, Cass. I, n. 2612 del 20.12.2004 e Cass., I, n. 3972 del 2.7.1998.

Gli scriventi ritengono che un siffatto orientamento sia maturato , in via sostanzialmente tralaticia, sulla scia della sentenza delle Sezioni Unite n. 17706 del 22.3.2005 , che però non si era pronunciata sulla nozione di delitti di criminalità organizzata nell’art. 13 del dl n. 152 /1991 ma su di un tema notevolmente diverso: la latitudine della nozione di criminalità organizzata nell’art. 240 bis disp. coord. , c.p.p. , norma recante disposizioni sulla sospensione dei termini processuali in periodo feriale.

Ed è riferendosi alla sospensione dei termini nel periodo feriale che le Sezioni Unite hanno affermato che : “ *ai fini dell'applicazione dell'art. 240 bis, comma secondo, disp. coord. cod. proc. pen., che prevede l'esclusione, operante anche per i termini di impugnazione dei provvedimenti in materia di cautela personale, della sospensione feriale dei termini delle indagini preliminari nei procedimenti per reati di criminalità organizzata, quest'ultima nozione identifica non solo i reati di criminalità mafiosa e assimilata, oltre i delitti associativi previsti da norme incriminatrici speciali, ma anche qualsiasi tipo di associazione per delinquere, ex art. 416 cod. pen., correlata alle attività criminose più diverse, con l'esclusione del mero concorso di persone nel reato, nel quale manca il requisito dell'organizzazione”.*

Con ogni probabilità , dunque, si è verificata - anche per effetto della autorevolezza propria delle pronunce delle Sezioni Unite - una meccanica “traslazione” della definizione di delitti e procedimenti di criminalità organizzata elaborata in relazione alla sospensione dei termini feriali nel diverso e più sensibile ambito della disciplina delle intercettazioni.

E ciò senza che sia stata effettuata , nelle sentenze prima citate, una compiuta valutazione degli effetti diretti e delle complessive ripercussioni di tale trasposizione in contesti normativi profondamente diversi.

Non è perciò inappropriato sollecitare le Sezioni Unite a dire una parola decisiva in materia, chiarendo quale sia la più corretta lettura della nozione di “delitti di criminalità organizzata” nell’ambito della normativa speciale derogatrice sulle intercettazioni tra presenti dettata dall’art. 13 del d.l. n. 152/1991 (ed estesa ai delitti di sfruttamento della prostituzione e contro la personalità individuale con l’art. 9 della legge n. 228 dell’11.8. 2003 sulla tratta delle persone).

Ad avviso di chi scrive tale nozione potrebbe essere ancorata ad un preciso dato normativo, quale l'elenco dei delitti elencati nell'art. 407 comma 2, lett. a) del codice di procedura penale commessi dai componenti delle diverse associazioni criminali (di volta in volta terroristiche, di tipo mafioso, dedite al traffico di stupefacenti o di altra natura) che tali delitti contemplano nel loro programma criminoso.

Oppure, alternativamente, essere ricavata da una rigorosa ricognizione di carattere sistematico del concetto di "criminalità organizzata" desumibile dall'ampio complesso di dati normativi esistenti nel nostro ordinamento, e dunque certamente comprensiva delle associazioni con finalità di terrorismo e di eversione dell'ordine democratico (art. 270 bis c.p.) , delle associazioni di tipo mafioso (art. 416 bis c.p.) e delle associazioni finalizzate al traffico illecito di stupefacenti di cui all'art. 74 del DPR n. 309 del 1990.

9. La risposta – affermativa - sulla terza questione all'esame delle Sezioni Unite.

Sulla scorta delle considerazioni sviluppate nella presente memoria si può conclusivamente affermare, in ordine alla terza questione prospettata nell'ordinanza di rimessione, che la sentenza della VI Sezione n. 27100 del 26/5/2015, introducendo, in una decisione relativa ad un procedimento di criminalità organizzata, la specifica indicazione del luogo di esecuzione della intercettazione tra presenti come requisito autorizzativo , ha qualificato come contenuto necessario ed imprescindibile del decreto autorizzativo delle intercettazioni un elemento non richiesto dalla legge.

Si condivide invece la tesi prospettata nell'ordinanza di rimessione nella parte in cui sostiene che "*il principio secondo cui il decreto deve individuare con precisione i luoghi in cui dovrà essere eseguita l'intercettazione delle comunicazioni tra presenti .....non.... è desumibile dalla legge,…….e non sembra costituire un requisito significativo funzionale alla tutela dei diritti in gioco"*.

Nella specie il decreto autorizzativo emesso dal giudice per le indagini preliminari contiene la chiara individuazione del destinatario del provvedimento ed una adeguata e coerente motivazione delle ragioni fondanti la disposizione di intercettazioni tra presenti , mentre le conversazioni intercettate , sui cui si basano l'ordinanza del giudice delle indagini preliminari di Palermo e l'ordinanza del Tribunale del riesame, riguardano solo soggetti (tra cui l'odierno ricorrente) indagati e sottoposti a misure cautelari come concorrenti nel reato di cui all'art. 416 bis c.p..

Ne consegue che il secondo motivo del ricorso in esame concernente le intercettazioni è da ritenere infondato.

10. Le risposte - negative - sulle prime due questioni all'esame delle Sezioni Unite.

Relativamente più agevole è fornire risposta agli altri due interrogativi posti dal collegio rimettente.

Nelle intercettazioni non ricomprese nella disciplina derogatoria e regolate esclusivamente dagli artt. 266 e ss. c.p.p., il requisito autorizzativo delle intercettazioni tra presenti , imperniato sul *"fondato motivo di ritenere che*" nei luoghi di privata dimora investiti dalle captazioni *" si stia svolgendo l'attività criminosa"* , si pone infatti in tutta la sua pienezza e non tollera eccezioni di sorta.

Ed è un fatto che , all'atto di autorizzare una intercettazione da effettuarsi a mezzo di captatore informatico installato su di un apparecchio portatile , il giudice non sarà in grado di prevedere e

predeterminare *a priori* i luoghi di privata dimora nei quali il congegno verrà introdotto e quindi non potrà controllare , né sotto il profilo oggettivo né sotto il profilo soggettivo , l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari ordinarie.

In un siffatto contesto, il "rischio" di dar vita ad una pluralità di intercettazioni tra presenti in luoghi di privata dimora del tutto al di fuori dei cogenti limiti previsti dalla normativa codicistica è altissimo e si profila come incompatibile con la norma della legge ordinaria oltre che socialmente intollerabile in uno Stato di diritto, risolvendosi in una lesione delle norme della Costituzione e della Convenzione europea (che possono dirsi realmente rispettate solo quando legislatore e giudici concorrano , ciascuno nel proprio ruolo, a porre alle intercettazioni limiti osservabili e rispettosi del principio di proporzione).

Infine chi scrive non ritiene che la sanzione di inutilizzabilità di captazioni eventualmente avvenute in luoghi di privata dimora al di fuori dei presupposti di cui all'art. 266, comma 2, c.p.p. possa essere utilmente invocata nella fattispecie in esame.

Tale sanzione è infatti riservata a gravi patologie degli atti del procedimento e del processo mentre nell'ipotesi qui in discussione essa dovrebbe essere contemplata , con una evidente torsione, come mezzo per riequilibrare gli effetti di una fisiologia distorta e *contra legem* , rappresentata dall'adozione di provvedimenti giudiziari dagli effetti imprevedibili e incontrollabili a priori nella loro conformità alla legge.

Considerazione, questa , che esime dall'affrontare qui il tema spinoso , ma in un'ottica realistica non irrilevante, della possibile divulgazione, ben prima di ogni declaratoria di inutilizzabilità, dei contenuti di intercettazioni destinate ad essere successivamente dichiarate inutilizzabili. Rischio che non può ancora dirsi scongiurato nonostante i significativi ed impegnativi atti di autoregolamentazione adottati da importanti uffici giudiziari , le iniziative in atto, nel circuito del governo autonomo della magistratura, per generalizzarne l'applicazione e le prospettive di interventi legislativi in materia.

Queste considerazioni sui dati normativi e fattuali appaiono di per sé sufficienti a negare legittimità al ricorso a virus informatici nell'ambito delle intercettazioni per reati diversi da quelli di criminalità organizzata ed a fornire altrettante risposte negative alle prime due questioni poste dall'ordinanza di rimessione.

Almeno sino a quando non sarà tecnicamente provato che il captatore informatico può essere predisposto ed utilizzato con modalità tali da svolgere captazioni sonore "esclusivamente" quando il soggetto intercettato si muova in luoghi pubblici o aperti o nel proprio domicilio , individuato come luogo di attuale svolgimento delle attività criminose (ad es. attraverso l'impiego combinato di un preciso servizio di localizzazione satellitare e di un correlato meccanismo di attivazione del captatore solo nei luoghi pubblici o nel suo domicilio).

Un tale uso della tecnologia captativa consentirebbe infatti di ricondurre l'impiego del nuovo strumento di intercettazione nell'alveo delle norme in vigore , permettendo di rispettare le rigorose coordinate tracciate dal codice di rito in materia di intercettazioni nei luoghi di privata dimora.

Roma, 18 aprile 2016

L'Avvocato generale
A.Nello Rossi

Il Sostituto Procuratore generale
Antonio Balsamo

NOTE

1. Testaguzza, *I sistemi di controllo remoto: fra normativa e prassi*, in Dir. Pen. e Processo, 2014, p. 759 e ss.
2. Testaguzza, *Digital forensic. Informatica giuridica e processo penale* , Cedam, 2014, p.81 e ss.
3. Torre, *Il virus di Stato nel diritto vivente tra esigenza investigative e tutela dei diritti fondamentali*, in Dir. Pen. e Processo, 2015, p. 1163 e ss.
4. Di recente, la questione è stata affrontata dal **Tribunale del riesame di Palermo** con **l'ordinanza dell'11 gennaio 2016**, che ha confermato una ordinanza di custodia cautelare emessa dal Gip per i reati di partecipazione ad associazione mafiosa e ad associazione finalizzata al traffico di stupefacenti. Nel corso delle indagini, il P.M. nell'istanza di autorizzazione all'intercettazione ambientale aveva chiesto sia la captazione di conversazioni tra presenti nei luoghi in cui era ubicato il dispositivo elettronico, sia le videoriprese negli stessi luoghi. Il Gip aveva autorizzato la prima istanza, ma aveva rigettato la seconda, facendo riferimento al divieto di legge per le videoriprese svolte in domicilio privato, ed emettendo declaratoria di inammissibilità della richiesta di autorizzazione alle videoriprese all'esterno di domicilio privato poiché di "competenza dello stesso pubblico ministero".
   Il Tribunale del riesame ha precisato che, quando si proceda – come nel caso di specie – per il delitto di cui all'art. 416 bis c.p., il limite motivazionale contenuto nel comma 2 dell'art. 266 c.p.p. non trova applicazione, ex art. 13 d.l. 13 maggio 1991, n. 152, non essendovi obbligo, nell'ipotesi in cui l'intercettazione avvenga in luogo di privata dimora, di motivare sul fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.
   Ha, poi, sottolineato che, mentre le videoriprese a domicilio sono vietate (salva l'autorizzazione del titolare del domicilio e salve le condotte non comunicative), le intercettazioni ambientali al domicilio privato, non sono, invece, affatto vietate dalla legge, ma sottostanno a precisi requisiti. Inoltre, le videoriprese all'esterno dell'abitazione, in quanto prove documentali atipiche che, non subendo i limiti dell'inviolabilità domiciliare, possono essere disposte direttamente dal p.m. , non sottostanno all'autorizzazione del Gip.
   Con riguardo alle intercettazioni ambientali presso il domicilio, il Tribunale del riesame ha osservato: «il provvedimento autorizzativo del Gip, contiene, comunque nel caso concreto, sufficienti e specifiche garanzie contro un'indiscriminata intrusione dell'attività investigativa nella libertà e segretezza delle comunicazioni, delineandone con precisione le coordinate ed i confini. Intanto il Gip precisa nel corpo motivazionale del provvedimento, che, dopo la scarcerazione, OMISSIS, capo del mandamento di OMISSIS, aveva riattivato tutti i canali di comunicazione interni al sodalizio (…), sì da assumere un ruolo di primaria importanza a seguito della cattura del reggente, OMISSIS e che OMISSIS, tramite dispositivo informatico nella sua disponibilità, manteneva la rete di contatti con i sodali. Il Gip, ha, cioè, palesato, da un lato la permanenza del delitto di associazione di tipo mafioso, cioè l'attuale svolgimento di tale delitto associativo (ciò che non è richiesto dalla legge per il delitto in argomento, ma che a maggior ragione giustificherebbe un'intercettazione domiciliare tout court) e, dall'altro, il rapporto di pertinenzialità tra il dispositivo elettronico del bersaglio (OMISSIS) e la rete di relazioni mafiose, vitali per l'operatività del sodalizio, riattivatasi proprio intorno all'uso di quel mezzo di comunicazione. Il Gip infatti spiega che poiché il OMISSIS si collegava tramite la rete internet e via Skype con i suoi sodali, allora era indispensabile procedere alle intercettazioni ambientali "che avverranno tra il OMISSIS ed i suoi interlocutori all'interno dei luoghi ove si trova il personal computer…in uso allo stesso…ed attraverso il quale il predetto si collega telematicamente coi suoi interlocutori,

atteso che nel corso di detti collegamenti telematici, già sottoposti ad attività d'intercettazione, potrebbero avvenire conversazioni tra OMISSIS, ossia il soggetto che utilizza il dispositivo, ed altri soggetti presenti con lui nella stanza in cui è ubicato in quel momento l'apparecchio portatile in cui si faccia riferimento alle vicende legate al mandamento mafioso". Dal contenuto della motivazione del decreto di autorizzazione all'intercettazione non solo si evince la specificazione del rapporto di pertinenzialità tra il dispositivo intercettato ed il reato per cui si procede (consumato proprio attraverso le comunicazioni telematiche e quelle tra tutti i soggetti presenti al momento dell'uso del suddetto tablet), ma anche dei luoghi, che si indicano "nella stanza" in cui il dispositivo "è ubicato in quel momento": con esclusione, cioè, di tutte le altre stanze della privata dimora del OMISSIS e, quindi, contrariamente all'assunto difensivo, con un aumento delle garanzie della privacy che avrebbe, di contro, offerto un'intercettazione ambientale al domicilio dell'indagato tout court. Del resto tale delimitazione garantisce che le conversazioni intercettate abbiano ad oggetto non vicende private della famiglia OMISSIS o dei loro ospiti - come all'evidenza sarebbe stato intercettando l'intero appartamento del OMISSIS (si ricordi che il *trojan i*nserito in un pc non arriva ad intercettare a dieci metri di distanza) - ma solo e soltanto l'attività criminosa svoltasi per mezzo e, per così dire, intorno al tablet usato per l'attività criminale, delimitando, quindi, ulteriormente l'ambito spaziale di intrusione nell'altrui sfera riservata. Per tali ragioni, ritiene il collegio che il decreto in contestazione, in ragione della specificità delle argomentazioni surriportate e addotte in motivazione (…) debba ritenersi legittimo e non cozzi contro gli artt. 15 Cost, 266, co. 2 c.p.p. e 8 CEDU».

Il problema dell'ammissibilità delle intercettazioni ambientali mediante virus informatico è stato risolto positivamente anche nel **c.d. "caso Bisignani"** (su cui v. Testaguzza , *I sistemi di controllo remoto* cit. e, dello stesso autore, *Digital forensic*, cit.)
Si tratta dell'indagine avviata dalla Procura della Repubblica presso il Tribunale di Napoli sulla c.d. P4; secondo gli inquirenti, gli imputati avrebbero instaurato, grazie ad un'intricata rete di influenti amicizie, un sistema informativo parallelo che avrebbe avuto tra i suoi obiettivi «l'illecita acquisizione di notizie e di informazioni, anche coperte da segreto, alcune delle quali inerenti a procedimenti penali in corso nonché di altri dati sensibili o personali al fine di consentire a soggetti inquisiti di eludere le indagini giudiziarie ovvero per ottenere favori o altre utilità» (Torre, *op. cit*.)
Nel procedimento penale n. 39306/2007 R.G.N.R., il G.I.P. del Tribunale di Napoli autorizzava la disposizione delle intercettazioni ambientali attraverso l'utilizzo di un software apposito installato nei rispettivi personal computer degli indagati ed in grado di captare le conversazioni verbali dagli stessi intrattenute.
In questo caso il captatore informatico era in grado, non soltanto di acquisire ed estrapolare dati ed informazioni di natura digitale memorizzati sulla memoria di massa del sistema informatico "bersaglio", ma anche di realizzare una vera e propria intercettazione ambientale, prendendo il controllo occulto del microfono e della webcam dell'elaboratore.
Il P.M., rendendosi conto della necessità di contemperare, nell'utilizzo di siffatto strumento investigativo, le esigenze investigative finalizzate all'accertamento del fatto con i diritti di difesa delle persone sottoposte ad indagine, aveva chiesto al G.I.P. di autorizzare, con decreto, tanto la *on line search*, quanto la *on line surveillance*, ai sensi degli art. 266 ss. c.p.p.
Il giudice per le indagini preliminari ritenne inquadrabili le intercettazioni ambientali, seppur effettuate attraverso lo strumento atipico della "cimice informatica", nel novero delle attività previste dal comma 2 dell'art. 266 c.p.p., e dunque le autorizzò, con decreto emesso a norma dell'art. 267 c.p.p..
Invece per l'acquisizione dei dati il GIP, non qualificando le relative attività come intercettazioni, ritenne sufficiente un semplice provvedimento del PM, alla luce delle

indicazioni espresse da Cass., sez. V, 14 ottobre 2009, n. 16556/10, Virruso e altri. Sul punto, nel decreto di autorizzazione alle intercettazioni si esplicitava: «quanto invece all'estrapolazione […] di dati non aventi ad oggetto un flusso bidirezionale (o pluridirezionale) di comunicazioni inteso in senso stretto, ma piuttosto documenti e dati informatici già formati (o che verranno formati in futuro) contenuti nella memoria del personal computer, anche alla luce dell'arresto giurisprudenziale citato dal P.M. e che si richiama, ritiene il giudicante che si tratti di un'attività che esula dalla nozione di intercettazione di comunicazioni o conversazioni. Come tale non deve essere autorizzata dal G.I.P.» (Torre, *op. cit.*).

Nei primi **commenti dottrinali** sulle recenti pronunce di merito, sul tema – di indubbia centralità – della inclusione tra i requisiti essenziali del decreto autorizzativo della precisa indicazione del luogo dell'intercettazione ambientale si è manifestata una diversità di vedute.

L'opzione interpretativa accolta da Trib. Palermo, Sez. riesame, 11/1/2016 è stata sottoposta a critiche da una parte della dottrina (Lorenzetto, *Il perimetro delle intercettazioni ambientali eseguite mediante " captatore informatico"* , in *Diritto Penale Contemporaneo*, 24 marzo 2016) che muove dalla premessa che «a dispetto di una dimensione tradizionalmente circoscritta, poiché coincidente con la sede in cui si trova localizzato l'apparato-microspia, il perimetro dell'intercettazione ambientale conosce oggi una dirompente *vis* espansiva grazie all'impiego del c.d. captatore informatico. Trattasi di *software*, innestato in modo occulto all'interno di un dispositivo *target* (di qui, l'allegorico epiteto di "*trojan horse*"), che consente - *inter alia* - di azionare da remoto il microfono del sistema "bersaglio" (*personal computer*, *smartphone*, *tablet*) e di apprendere per tale via i colloqui che si svolgono nello spazio circostante, ovunque si trovi il soggetto che ne ha la disponibilità. Intuibile la frizione con i valori di libertà e segretezza delle comunicazioni: proclamandone l'inviolabilità e ammettendone la limitazione "soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge" (art. 15 Cost.), i principi costituzionali - ribaditi, quanto al dovere di previsione legale, dalle norme convenzionali che tutelano il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, a fronte di ingerenze di una pubblica autorità (art. 8 Cedu) - impongono la rigorosa interpretazione dell'art. 266 comma 2 c.p.p., mettendo a rischio i risultati dell'intercettazione ambientale ove manchi la predeterminazione dei luoghi in cui si svolgono le operazioni» (peraltro, sul fronte dell'intercettazione tra presenti "tradizionale", la giurisprudenza - argomentando dal tenore dell'art. 266 comma 2 c.p.p. - richiede l'indicazione dell'ambiente in cui deve svolgersi l'operazione "*solo quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 c.p.*": Cass., sez. VI, 5 novembre 1999, n. 3541).
In questa prospettiva, si è osservato che l'eccezione difensiva secondo cui l'ubicazione del dispositivo elettronico anche nei luoghi di privata dimora aveva reso possibile l'intercettazione domiciliare senza che il decreto autorizzativo si fosse preoccupato di motivare circa l'attualità dell'azione criminosa in quel luogo (art. 266 comma 2 secondo periodo c.p.p.) è stata agevolmente respinta dal Tribunale del riesame atteso che nei procedimenti relativi ai delitti di criminalità organizzata - come appunto nel caso concreto - l'intercettazione domiciliare, in deroga al limite di cui all'art. 266 comma 2 c.p.p., è consentita «anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa» (art. 13 comma 1 d.l. n. 152 del 1991).
E' stato invece considerato invece meno lineare il percorso argomentativo che - sul presupposto che il decreto autorizzativo descriva "con precisione le coordinate e i confini" dell'attività investigativa sottesa all'intercettazione - ha condotto a disattendere anche

l'eccezione difensiva secondo cui l'autorizzazione avrebbe dovuto specificare il luogo delle conversazioni, non essendo ammissibile un provvedimento generico che consenta la captazione in qualsiasi luogo si rechi il soggetto.
In particolare, il Tribunale del riesame ha ritenuto soddisfatta la specificazione dei luoghi, che il decreto avrebbe individuato "*nella stanza in cui è ubicato in quel momento l'apparecchio portatile*". Delimitare "*intorno al tablet*" lo spazio di intrusione, considerato che il captatore informatico copre un raggio non superiore ai dieci metri di distanza, avrebbe quindi il pregio di circoscrivere l'intercettazione ad alcune stanze soltanto della privata dimora, preservando in termini ancor più solidi quella *privacy* che un'ordinaria captazione ambientale, invece, avrebbe potuto estendere all'intero domicilio dell'indagato.
In dottrina si è però osservato che «non sembra (…) che la ridotta gittata captatrice tributata al *software-trojan* possa fornire argomenti tranquillizzanti a tal punto, da compensare l'indeterminatezza implicita nel decreto che autorizza l'intercettazione ambientale individuandone i luoghi soltanto *per relationem*. Certamente, non si dubita che la riservatezza dei soggetti coinvolti risulti maggiormente tutelata ove si riesca a contenere la captazione domiciliare ai soli colloqui riferibili all'attività criminosa: per questa via, si accorda nei fatti protezione all'intimità domestica, anche quando il titolo di reato - come nel caso concreto - consentirebbe di svincolare l'intercettazione dal requisito di cui all'art. 266 comma 2 secondo periodo c.p.p. Ciò posto, la pretesa garanzia "aumentata" in punto di *privacy* presuppone che l'ascolto, ammesso che sia davvero esperibile soltanto nelle immediate vicinanze del dispositivo-bersaglio, non attinga accidentalmente colloqui relativi a vicende strettamente private; circostanza a conti fatti imprevedibile, che risente di variabili connesse alle modalità esecutive delle operazioni. Ferma dunque l'alea che si registra a valle del ragionamento, l'equivoco si colloca - a monte - nell'avere riconosciuto come specifico un luogo per definizione generico, poiché identificato sulla base della collocazione contingente di un dispositivo portatile. Fuorviante è infatti il rimando alla "*stanza*", per identificare il luogo in cui l'apparecchio "*è ubicato in quel momento*": il riferimento, in certa misura evocativo di un ambiente domestico, non esclude che il dispositivo, proprio perché mobile, possa essere utilizzato anche in luoghi del tutto diversi dall'appartamento del soggetto indagato, finanche all'interno di "stanze" di altre private abitazioni. Se così è, il decreto autorizzativo avrebbe dovuto impegnarsi per rendere stabile un ambiente altrimenti mutevole, attraverso la rigorosa predeterminazione dei luoghi in cui eseguire le operazioni, pena l'illegittimità - e, quindi, l'inutilizzabilità - delle captazioni autorizzate senza la necessaria specificazione. Nella stretta interpretazione delle norme che consentono di intercettare le comunicazioni tra presenti, insomma, non vi è spazio per ossimori giuridici, come quello sotteso all'intercettazione ambientale provvista del dono dell'ubiquità».

Per analoghe ragioni una parte della dottrina (Torre, *op.cit.)* **ha espresso valutazioni critiche anche sul decreto autorizzativo delle intercettazioni ambientali emesso dal G.I.P. del Tribunale di Napoli nel procedimento penale n. 39306/2007 R.G.N.R.**
Si è ritenuto infatti necessario operare una distinzione quanto all'incasellamento giuridico della *on line surveillance* - ovvero captazione di informazioni a contenuto comunicativo - nell'ambito della disciplina propria delle intercettazioni telematiche. Precisamente, quando il flusso comunicativo bidirezionale o pluridirezionale intercettato attraverso il virus consiste in email, messaggi di chat, sms, ecc., non sorgerebbe alcun dubbio circa la copertura giuridica offerta dall'art. 266 bis del codice di rito: si tratta, a tutti gli effetti, di una tipologia di intercettazione telematica che trova la sua disciplina tipica negli artt. 267 ss. c.p.p..
Quando, invece, come nel caso *de quo*, il virus consente di effettuare una vera e propria intercettazione ambientale, la questione si complicherebbe in ragione del combinato disposto degli artt. 266, comma 2, e 614 c.p. Infatti, sulla base dei principi fissati da Cass., Sez. VI, 2 dicembre 1999, n. 3541, «l'intercettazione di comunicazioni tra presenti richiede

l'indicazione dell'ambiente nel quale l'operazione deve avvenire […] quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 c.p.». Sennonché, l'utilizzo della "cimice informatica" esclude a priori la possibilità di predeterminare con esattezza i luoghi in cui avverrà l'operazione di intercettazione ambientale. È noto, infatti, che il personal computer portatile (ma anche e soprattutto lo smartphone o il tablet) segue la persona ovunque, in maniera del tutto imprevedibile e non pronosticabile. Si è quindi affermato che l'impossibilità di stabilire con esattezza gli spostamenti dello strumento digitale e, quindi, l'inattuabilità della previsione dei luoghi in cui autorizzare, da parte del G.I.P., le operazioni di intercettazione, svilisce i limiti imposti dalla giurisprudenza di legittimità all'utilizzo delle intercettazioni ambientali e stride con le prerogative di riservatezza sancite a livello costituzionale.

In una prospettiva analoga, un'altra parte della dottrina (Testaguzza, *I sistemi di controllo remoto*, cit.) ha considerato quantomeno opinabili le scelte del G.i.p. di autorizzare le intercettazioni ambientali, pur nella consapevolezza della indeterminatezza del luogo di posizionamento del personal computer. Sul punto, si sono espresse le seguenti osservazioni:
«Indubbiamente l'installazione di un captatore informatico sullo stesso può trasformare l'oggetto *de qua* in una vera e propria microspia (come ribadito dalla Procura), forse dai caratteri più evoluti rispetto alle comuni "cimici" utilizzate negli anni pregressi. Del resto, lo sviluppo di un software da inserire all'interno di un elaboratore elettronico che sia in grado di captare il contenuto della conversazione intercorsa fra più soggetti, ritrasmettendola contestualmente agli organi inquirenti, altro non è che l'espressione più evidente dei cambiamenti in atto di una società avanzata ed in constante evoluzione. E tale consapevolezza, se già era sentita dal Legislatore del '93, preoccupato di introdurre l'art. 266-*bis* c.p.p. per far fronte anche ai reati «compiuti mediante l'impiego di tecnologie informatiche o telematiche», non può venir meno né essere disconosciuta di certo ora, nel "secolo della tecnologia".
L'autorizzazione del G.i.p. a disporre le intercettazioni *de quibus*, pertanto, si pone in perfetta sintonia con i principi cardine del nostro sistema e, quindi, con quell'affievolimento del fondamentale diritto alla riservatezza e della inviolabilità del domicilio realizzabile attraverso un provvedimento motivato dell'Autorità giurisdizionale. Restano, tuttavia, dei dubbi relativamente alle modalità di svolgimento delle operazioni in esame: se è vero, infatti, che deve ritenersi esclusa una predeterminazione *a priori* dei luoghi ove realizzare l'intercettazione sulla base di precedenti orientamenti giurisprudenziali secondo i quali «l'intercettazione di comunicazioni tra presenti richiede l'indicazione dell'ambiente nel quale l'operazione deve avvenire solo quando si tratti di abitazioni o luoghi privati, secondo l'indicazione di cui all'art. 614 c.p.» (Cass. VI, 2.12.1999, 3541) è anche vero, di converso, che l'impossibilità di determinarli con esattezza non esclude il rischio di aggiramento degli stessi limiti imposti dalla pronuncia in esame. Si pensi al caso in cui il personal computer (ma anche tutti gli altri strumenti che oramai sono entrati a far parte della quotidianità di ognuno, quali *smartphone, tablet, ecc..)*, ormai infetto dell'indagato, proprio perché "mobile" e dunque collocabile astrattamente in ogni dove (ipotesi contemplata dallo stesso decreto di autorizzazione del G.i.p), venga portato in un luogo di privata dimora ed utilizzato come strumento di ricezione di comunicazioni e di conversazioni fra presenti.
Né tanto meno può considerarsi attendibile il riferimento ai casi di intercettazione "casuale, a cornetta sollevata" posto come termine di paragone, rispetto al caso in esame, da parte della Procura: appare evidente la diversità dell'ambito cognitivo originato dalle due fattispecie. Se nel primo caso, infatti, la "casualità" è l'elemento di spicco ovvero l'esistenza di un accadimento del tutto imprevisto ed involontario, che potrà verificarsi come non verificarsi e tale da escludere una sua preventiva configurazione nelle stesse richieste di autorizzazione alle intercettazioni, nel secondo non c'è margine per l'eventualità. In

quest'ultimo caso resta sconosciuto il posto di ubicazione dello strumento su cui è installato il captatore informatico ma si è perfettamente consapevoli del ruolo da esso svolto.
L'impossibilità di stabilire con esattezza gli spostamenti dello strumento elettronico e la garanzia offerta agli inquirenti di poter comunque svolgere un'attività di intercettazione ambientale, debitamente autorizzata, non può che stridere con le prerogative di riservatezza sancite a livello costituzionale. Anche a voler ammettere una successiva inutilizzabilità, in sede processuale, di quando acquisito, la violazione dei predetti principi costituzionali, in questo caso, si configurerebbe *ex ante*, già nelle fasi di autorizzazione alle operazioni da parte del G.i.p. con un contestuale svilimento della portata "avanguardista" dell'art. 15 Cost.
A differenza di quanto previsto dall'art. 271 c.p.p., il quale al primo comma stabilisce un divieto di utilizzazione dei risultati delle intercettazioni eseguite fuori dai casi consentiti dalla legge o senza osservare le prescrizioni di cui agli artt. 267 e 268, comma 1 e comma 3, c.p.p. e che richiede un inevitabile controllo *ex post* sul materiale acquisito (con potenziale illegittimità o irritualità della prova assunta in spregio dei divieti probatori imposti da norme processuali), la non indicazione dei luoghi ove svolgere l'intercettazione ambientale, avvalendosi di uno strumento comunque suscettibile di travalicare i limiti imposti dal comma 2 dell'art. 266 c.p.p., potrebbe (o dovrebbe?) configurare una ipotesi di vera e propria "prova incostituzionale".
Nonostante, infatti, il dissenso autorevolmente espresso in ordine alla sua esistenza (Galantini, voce *Inutilizzabilità (dir.proc.pen.)* in *Enc. Dir.Agg*. I Milano, 1997, p.699) la quale - si è osservato - non sarebbe sorretta da alcun argomento giuridico, dal momento che i precetti costituzionali rappresentano altrettanti paradigmi della formazione attuata in sede legislativa, è noto come la giurisprudenza della Consulta, negli anni passati, abbia spesso operato un suo implicito riconoscimento. Basti pensare alla sentenza n. 34 del 6 aprile 1973 nella quale il Giudice delle leggi ha più volte rimarcato il principio secondo cui «attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione e a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito» e ribadendo che «non possono validamente ammettersi in giudizio mezzi di prova che siano stati acquisiti attraverso attività compiute in violazione delle garanzie costituzionali poste a tutela dei fondamentali diritti dell'uomo e del cittadino».
Consentire, dunque, all'interno di un decreto di autorizzazione alle intercettazioni la possibilità di svolgerle in ogni luogo (ad eccezione di quelli di privata dimora) pur nella consapevolezza della potenziale mobilità dello strumento utilizzato per la captazione, renderebbe del tutto vano lo sforzo, promosso in sede costituente, di disciplinare un'autorizzazione preventiva da parte dell'Autorità giurisdizionale per la limitazione del diritto inviolabile di libertà e segretezza della comunicazione. In caso contrario (si giustifichi la provocazione) basterebbe autorizzare sempre e comunque tali attività, contando sulla sola esistenza dei gravi indizi di reato e dell'indispensabilità del mezzo ai fini della prosecuzione delle indagini, riservando la verifica dei presupposti previsti dal comma 2 dell'art. 266 c.p.p. in un momento successivo. Ma non sembra questa una lettura conforme al dettato costituzionale».
In tale ottica si è aggiunto (Testaguzza , *Digital forensic*, cit.) che la possibilità di utilizzare un software, surrettiziamente installato nel personal computer dell'indagato, come una vera e propria "cimice informatica", all'atto pratico rischia di vanificare la portata del 2° comma dell'art. 266 c.p.p. non potendo, gli organi inquirenti, essere messi nelle condizioni di conoscere previamente l'ubicazione dell'elaboratore elettronico soggetto alla installazione del captatore.

(5) La soluzione accolta da Cass., Sez. VI, 26/5/2015 n. 271 ha suscitato rilievi critici di una parte della dottrina (Amato, *Intercettazioni mediante agenti intrusori : la Cassazione non è*

al passo con i tempi, in *Guida al diritto*, 2015, n. 41), che ha osservato che «la conclusione non convince perché non coglie la specificità tecnica e giuridica delle intercettazioni ambientali e le differenze tra queste e le intercettazioni telefoniche. Queste ultime, in effetti, presuppongono l'esistenza di una specifica apparecchiatura o di un particolare sistema da sottoporre a intercettazione, in modo tale che per ciascuna operazione di intercettazione i dati di identificazione dell'apparecchio da sottoporre a verifica e controllo devono essere precisati nel decreto autorizzativo. Diverso discorso vale per le intercettazioni ambientali, di cui al comma 2 dell'articolo 266 del Cpp, che per la loro intrinseca natura non necessitano della individuazione degli apparecchi, ma si riferiscono ad ambienti in cui deve intervenire la captazione, con la conseguenza che devono considerarsi legittime, con possibilità di piena utilizzazione dei risultati, anche quando in corso di esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione. Ciò che è necessario e sufficiente è che nel decreto di autorizzazione siano specificamente indicate le situazioni ambientali oggetto di intercettazione. Il tema è quindi quello dell'adeguata motivazione su tale specificità ambientale, che ben può essere dettagliata, nel caso di interesse, facendo riferendo ai luoghi (comunque) frequentati dal possessore dell'apparecchio su cui è stato installato l'agente intrusore. Il richiamo operato dalla Corte ai principi costituzionali appare generico e aspecifico, non riuscendosi a cogliere quel plus di intrusione, rispetto a una intercettazione ambientale classica (ergo, disposta in un ambiente ben determinato e immutabile), allorquando si preveda la dinamicità del controllo con l'interessamento di ambienti diversi frequentati dal soggetto sottoposto a controllo. Dinamicità che, del resto, è stata in passato già consentita dalla giurisprudenza di legittimità, allorquando ha qualificato come legittima nel corso delle operazioni la variazione dei luoghi dove doveva svolgersi la captazione (Sezione VI, 11 dicembre 2007, Sitzia e altri, in una vicenda in cui l' autorizzazione dell'intercettazione ambientale aveva a oggetto la sala colloqui del carcere in cui era ristretto il soggetto e le operazioni erano proseguite presso la sala colloqui di altro istituto penitenziario in cui il medesimo era stato trasferito; Sezione V, 6 ottobre 2011, Ciancitto, in cui la captazione ambientale era stata trasferita dalla vettura oggetto di autorizzazione ad altra vettura successivamente acquistata dall'indagato sottoposto a intercettazione; nonché Sezione II, 15 dicembre 2010, Fontana e altri, in una fattispecie in cui l'intercettazione ambientale autorizzata in un determinato luogo è stata ritenuta legittimamente disposta anche nelle relative pertinenze). Ciò che rileva, piuttosto, a supporto di intercettazioni del tipo di che trattasi è l'adeguatezza della motivazione del provvedimento autorizzativo, che spieghi cioè la metodica tecnica utilizzata e quindi giustifichi la mobilità/dinamicità delle operazioni captative».

(6) La sentenza Sez. U. 28-3-2006, n. 26795 ha stabilito che le videoregistrazioni in luoghi pubblici o aperti o esposti al pubblico, non effettuate nell'ambito del procedimento penale, vanno incluse nella categoria dei documenti, ex art. 234 cod. proc. pen.. Le predette registrazioni, se vengono invece effettuate dalla polizia giudiziaria, anche d'iniziativa, vanno incluse nella categoria delle prove atipiche, soggette alla disciplina dettata dall'art. 189 cod. proc. pen.. Ma esse non possono essere espletate ovunque, perché le videoregistrazioni effettuate in ambito domiciliare, ai fini del procedimento penale, sono acquisite illecitamente e sono perciò inutilizzabili, anche se la tutela costituzionale del domicilio va limitata ai luoghi con i quali la persona abbia un rapporto stabile, sicché, quando si tratta di tutelare solo la riservatezza, la prova atipica può essere ammessa con provvedimento motivato dell'autorità giudiziaria. Vanno dunque tutelate dall'autorità giudiziaria (p.m. o giudice) le riprese visive che, pur non comportando intrusione domiciliare, violino la riservatezza personale (come, ad esempio, le riprese effettuate dalla polizia giudiziaria in un bagno pubblico.

(7) Su tali profili problematici riguardanti le fasi della "gestione e della "applicazione " dei nuovi strumenti destinati a trovare soluzioni adeguate nella prassi si rinvia alle considerazioni svolte da Torre (op.cit.) che ha segnalato che l'utilizzo dei virus trojan per fini investigativi desta perplessità anche in ragione della eterogenea moltitudine di informazioni - di carattere "comunicativo", ma anche "non comunicativo" - potenzialmente estrapolabili attraverso questo nuovo strumento tecnologico.
Sul punto, si sono espresse le seguenti considerazioni:
«Quanto alle informazioni qualificabili come "comunicazioni" e ottenibili attraverso il virus, la copertura giuridica offerta dagli artt. 266 ss. del codice di rito tiene entro i limiti già esposti *supra*, ma ciò non ci esenta da qualche ulteriore considerazione critica.
Il "captatore informatico" (tecnica di remote forensics) è gestito, su delega del P.M., da tecnici nominati ausiliari di polizia giudiziaria. Il problema è che, spesso, l'attività dei tecnici sfugge, per sua natura, al controllo dell'autorità giudiziaria e della stessa p.g. Quanto al pubblico ministero, questi si limita ad emettere un "decreto di intercettazione" (art. 267, comma 3, c.p.p.) valido formalmente, ma carente, nella sostanza, di quelle modalità esecutive necessarie, ex art. 271, comma 1, c.p.p., ai fini della utilizzabilità delle intercettazioni stesse. Per quanto riguarda la p.g., invece, non sempre è possibile affermare, senza il rischio di essere smentiti, che l'ufficiale di polizia giudiziaria assiste in prima persona alle operazioni di captazione svolte dal tecnico. D'altro canto, l'ignoranza delle effettive modalità esecutive fa sì che gli organi inquirenti possano mantenersi estranei all'attività effettuata, talora al limite del consentito.
Inoltre, mentre nel caso delle intercettazioni tradizionali è necessario, oltre all'ausilio dei tecnici, anche il contributo "terzo" del gestore telefonico (con conseguente tracciamento esterno delle operazioni), in ipotesi di captazione da remoto del contenuto di un dispositivo di memorizzazione digitale delle informazioni non è necessaria alcuna "collaborazione tecnica" ulteriore, con la conseguenza che l'attività di remote forensics è totalmente nelle mani del tecnico ausiliario di p.g.».
Sul tema vedi anche le importanti osservazioni di Aterno, *Digital forensic (investigazioni informatiche)* in *Dig. Disc.Pen*. Agg. , UTET, 2014.

(8) La questione delle prove lesive della dignità umana è venuta all'attenzione della Corte europea dei diritti dell'uomo in due sentenze, entrambe riguardanti la Germania.
Il primo caso attiene al prelievo coattivo di campioni biologici. Si è affermato che occorre comunque che gli organi inquirenti si servano di metodiche rispettose della dignità della persona e del suo diritto alla salute (come avviene qualora vengano utilizzate procedure non invasive o minimamente invasive: ad esempio, nei prelievi di saliva o capelli o sangue); in caso contrario, la condotta dell'autorità pubblica potrà integrare un trattamento inumano e degradante vietato dall'art. 3 della Convenzione. Si è pertanto riscontrata una violazione del divieto di trattamenti inumani o degradanti nel caso della somministrazione, da parte della polizia, di un emetico nei confronti di un soggetto sospettato di avere ingerito sostanze stupefacenti, allo scopo di provocarne il rigurgito, pur sussistendo mezzi alternativi ugualmente adeguati (sent. 11 giugno 2006, Jalloh c. Germania).
Il secondo caso riguarda la minaccia – rivolta dal personale di polizia all'indagato nel corso di un interrogatorio al fine di ottenere informazioni sul luogo di segregazione di un bambino sequestrato - di applicare un regime carcerario costituente occasione per violenze da parte di altri detenuti. Si è affermato che la minaccia di sottoporre un individuo a tortura, quando appaia sufficientemente concreta e immediata, costituisce di per sé un trattamento inumano, e che il divieto posto dall'art. 3 della Convenzione, avendo carattere assoluto ed inderogabile, non è soggetto a bilanciamento con altri valori, come quelli riguardanti l'intento di salvare la vita di altri individui (sent. 1 giugno 2010, Gäfgen c. Germania).