GIURISPRUDENZA PENALE

Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata

di ***Giuseppe La Corte***

Sommario: 1. Premessa: il panorama normativo attuale – **2.** La sentenza delle Sezioni Unite n. 26889/2016 – **3.** Proposte de iure condendo – **4.** Uno sguardo all'Europa.

1. Premessa: il panorama normativo attuale

Le temibili minacce che la criminalità organizzata di stampo mafioso, e adesso, anche la gravità crescente delle organizzazioni terroristiche, muovono alla vita, alla libertà, al patrimonio delle persone e alla sicurezza della collettività rendono evidente ogni sforzo che sia idoneo a prevenire *-a monte-* ed a contrastare *-a valle-* ogni attacco alla società democratica e civile.

L'evoluzione della tecnologia informatica ha fornito un valido ausilio per gli operatori che si occupano, ogni giorno, di arginare lo sviluppo delinquenziale delle criminalità organizzate *tout court*.[1]

I progressi in campo informatico, per converso, rischiano di diventare *locus amoenus* per criminali che tentano di eludere ogni captazione possibile dall'esterno attraverso l'utilizzo di impenetrabili apparecchi o attraverso sistemi di criptazione dei messaggi scambiati.

Considerata la velocità con cui gli strumenti tradizionali diventano obsoleti, si pensi, al riguardo, alla classica cimice che veniva posizionata *manualmente* nel luogo o nell' apparecchio in cui si volevano percepire, *rectius* captare, le conversazioni, che ivi si svolgevano, è giunto il momento di pensare a mezzi tecnologici migliori, all'avanguardia, che siano in grado di combattere e vincere la scaltrezza dei delinquenti più laboriosi.

La società si evolve e con essa anche le organizzazioni criminali. Lo scambio di informazioni non avviene più mediante *pizzini* ma attraverso un mezzo più veloce e

[1] Prima dell'avvento delle intercettazioni mediante *virus* informatico, le autorità procedenti avevano a disposizione le intercettazioni dei *telefax* e degli *s.m.s.* (quest'ultimi consentono la trasmissione di brevi messaggi scritti c.d. *short messages service*, sullo schermo del telefono).

Di grande utilità, potevano risultare, anteriormente all'uso costante delle *e-mails*, che ha limitato l'utilizzo dei *fax*, lo scambio di documenti tra due persone mediante il predetto strumento (un servizio telefonico consistente nella trasmissione -invio e ricezione- di immagini fisse).

Sul piano tecnico, i dispositivi consentivano di abbinare l'intercettazione dei *fax* a quella delle linee telefoniche e di conoscere, con precisione, la data e l'ora di trasmissione e l'utenza cui veniva inviato il documento.

pratico: *il computer*. Il *personal computer* diventa, pertanto, bagaglio di conoscenza per usi e costumi di un fenomeno criminale di *nuova generazione*, quella di *internet*.

I crimini informatici, c.d. *cybercrimes*, ad opera delle predette organizzazioni sono all'ordine del giorno: dalle grandi truffe, agli avvertimenti intimidatori, alle minacce estorsive mediante *messenger*, alle sostituzioni di persone, ai furti di identità come nuove interposizioni fittizie personali, fino agli attentati alla sicurezza della collettività e dei cittadini. Il mondo di *internet* è grande e sconosciuto e l'attrazione di facili guadagni, nella totale sicurezza (*forse*) di non essere scoperti, rende tutto ancora più fascinoso.

Dall'altra parte, anche chi, ogni giorno, si occupa di fermare i criminali non è, per fortuna, rimasto indietro all'evoluzione informatica.

Così, è questo costituisce l'argomento *principe* del presente progetto, si è parlato di "*virus informatici*", "*keylogger*", "*backdoor*", "*trojan*" e, più in generale, di "*agenti intrusori*".

Questi, al di là dei termini anglofoni con cui sono conosciuti, possono essere utilizzati come mezzi di prova inquadrabili, secondo l'impostazione codicistica, nelle intercettazioni.

Più in particolare, l'intercettazione di conversazioni o comunicazioni riservate è uno strumento di indagine particolarmente *insidioso* che mira ad introdurre nel processo mezzi di prova, acquisiti mediante captazione di colloqui tra ignari interlocutori.

Nel Codice, agli artt. 266-271 c.p.p., non si trova alcuna definizione di intercettazione. Il legislatore del 1988 ha preferito adottare una formula ampia ed aperta prevedendo, a tal proposito, all'art. 266 c.p.p., i limiti di ammissibilità delle "*intercettazioni di conversazioni di persone o comunicazioni di telefoniche e di altre forme di telecomunicazione*".

E' evidente che la norma, non individuando quali possano essere le altre forme di telecomunicazioni di cui si parla, si proietti nel futuro. Si parla, molto efficacemente, di una vera e propria clausola di adattamento automatico capace di adattarsi ai progressi inarrestabili della scienza elettronica.

Con apposita legge, nr. 547 del 1993, il legislatore della riforma ha inserito l'art. 266*bis* al predetto codice di procedura prevedendo "*le intercettazioni del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrenti tra più sistemi*".

Con ogni probabilità, l'esigenza di dettare un articolo specifico è stata avvertita a causa di una interpretazione restrittiva dell'art. 266 c.p.p. Il termine *telecomunicazione*, tuttavia, utilizzato dal comma 1 dell'art. 266 c.p.p. comprenderebbe qualunque sistema di trasmissione a distanza di informazione di diversa natura.

Il programma informatico, c.d. *malware* viene installato in un dispositivo *target*, in modo occulto, per mezzo del suo invio con una e-*mail*, un *sms* o una applicazione di aggiornamento.

Il *software* è costituito da due moduli principali: il primo, c.d. *server*, è un programma di piccole dimensioni che infetta il dispositivo bersaglio, il secondo, c.d. *client*, è l'applicazione che utilizza il *virus* per controllare detto dispositivo, ciò gli permette di scrutare tutto ciò questi apparecchi contengono: informazioni, dati, foto sia di pertinenza illecita che di matrice privata e personale.
Se è legittimo, a prima vista, nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei *virus* informatici, suscettibili di ledere la riservatezza, la dignità e la libertà delle persone, è del pari legittimo ricordare che solo siffatti strumenti sono, oggi, in grado di penetrare i canali criminali di comunicazione o di scambio di informazioni (di matrice mafiosa e terroristica) utilizzati per la commissione di perniciosissimi reati contro la persona e la libertà.
Così, molto efficacemente, si sostiene l'uso necessitato dei *predetti softwares* informatici perché, nelle loro *molteplici funzionalità*, consentono più che un potenziamento, un recupero dell'efficacia pressoché *perduta* e *sbiadita* delle normali tecniche tradizionali di intercettazione delle conversazioni.
Il problema principale, che, da subito, si sono posti i giudici, soprattutto nei procedimenti *de libertate*, è quello di arginare l'*onnipresenza* dei captatori informatici, così da evitare che gli stessi da strumenti nati contro l'abuso diventino, a loro volta, veicoli di incontrollabile invasione nel campo inviolabile della vita privata fuori dall'egida legislativa e giurisdizionale.
Il telefono cellulare è divenuto ormai oggetto che accompagna ogni nostro movimento ed è in grado, se sottoposto a finalità captatorie, di sottoporre l'individuo ad un indiscriminato controllo, non solo di tutta la sua vita privata ma anche dei soggetti che gli stanno vicino. La medesima intercettazione, pertanto, potrà divenire *ambientale* ed effettuarsi all'interno del domicilio, poiché il telefono cellulare diviene microfono e la sua telecamera una spia video.
La suesposta tematica, lungi dall'essere una questione pacificamente accettata dalla dottrina e dalla giurisprudenza, è, in realtà, foriera di un vivace e interessante dibattito politico e legislativo non accennato a placarsi nemmeno dopo la pronuncia emanata dalla Corte di Cassazione a Sezioni Unite n. 26889 del 2016.

2. La sentenza delle Sezioni Unite della Corte di Cassazione n. 26889 del 1 luglio 2016

Le argomentazioni principali, recepite o criticate dalle Sezioni Unite, relativamente alla materia *de qua*, scaturiscono da pronunce giurisdizionali elaborate da magistrati siciliani che svolgono la loro funzione nel distretto di Catania e Palermo.
In particolare si trattava di procedimenti di riesame[2] in relazione a misure cautelari applicate nei confronti di soggetti che facevano parte di storiche famiglie *mafiose* del circondario catanese o palermitano nei cui confronti era state utilizzate la tecnica

[2] Si tratta delle *ordinanze nr. 2001 del 2014 R.G. Libertà del Trib. di Catania* e *nr. 1823 del 2015 R.G. Libertà del Trib. di Palermo*

dell'agente intrusore per captarne il traffico di dati e di conversazioni mediante il loro *smartphone*.
I rispettivi difensori, in egual modo, si dolevano del fatto che in entrambe le fattispecie, in cui si era disposto l'intercettazione mediante *virus* informatico, il decreto di autorizzazione del giudice per le indagini preliminari non avesse indicato in maniera chiara e precisa i luoghi in cui si sarebbero dovute svolgere le intercettazioni, non essendo ammissibile un provvedimento generico che consenta la captazione in qualsiasi luogo si rechi il soggetto portando con sé il telefono infettato.
A dispetto di una dimensione tradizionalmente circoscritta, poiché coincidente con la sede in cui si trova localizzata la microspia, il perimetro delle intercettazioni ambientali attraverso il captatore informatico non conosce nessun limite spaziale.
E', pertanto, intuibile, la frizione ai valori inviolabili del domicilio e della libertà e segretezza delle comunicazioni garantite dagli artt. 2, 14 e 15 della Costituzione che ne ammettono la limitazione solo per atto motivato dell'autorità giudiziaria con le garanzie stabilite *ex lege*.
La Convenzione europea dei diritti dell'uomo e del cittadino, altresì, all'art. 8, enuncia il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza prevedendo, al secondo comma, una clausola di limitazione con la quale subordina l'ammissibilità di ogni ingerenza della pubblica autorità alla previsione legislativa al perseguimento di una delle finalità legittime indicate dalla norma ("*per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui*") e la necessità che la misura sia disposta nell'ambito di una società democratica.
I suddetti principi impongono una rigorosa interpretazione dell'art. 266, comma 2, c.p.p. nella parte in cui prevede che qualora le intercettazioni tra presenti "*si svolgano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa*".
Il legislatore ammette le intercettazioni ambientali *intra moenia* solo se vi sia "*fondato motivo di ritenere che in quei luoghi*, da qui il rinvio *all'art.614 c.p., si stia realizzando un'attività criminosa che debba essere perseguita*".
Il Tribunale di Palermo, nella veste di giudice del riesame, viene interpellato riguardo alla questione dell'inutilizzabilità delle risultanze delle intercettazioni ambientali effettuate presso il domicilio dell'indagato. A parere della difesa, infatti, non sussistevano né i requisiti previsti dal codice né l'indicazione specifica dei luoghi presso cui la medesima captazione avrebbe dovuto svolgersi.
Il giudice per le indagini preliminari, infatti, aveva autorizzato il pubblico ministero a disporre le operazioni di intercettazione di tipo ambientale delle conversazioni tra presenti "*nel luogo in cui si trova il dispositivo informatico in uso all'indagato".*[3]

[3] Cfr. *Decreto di autorizzazione nr. 315 del 2014 del Gip del Tribunale di Palermo*.

Da qui la doglianza difensiva per la quale l'ubicazione del dispositivo, per sua natura mobile, capace di seguire l'indagato in ogni suo spostamento, potesse captare ogni informazioni che sarebbe derivata nei luoghi domiciliari, *ex* art. 266 c.p.p., senza che il decreto autorizzativo si fosse preoccupato di motivare l'attualità dell'azione criminosa.
Il provvedimento del giudice era generico e lesivo di valori inviolabili che possono essere derogati secondo una *riserva di legge rinforzata* e per espresso provvedimento motivato da parte della *autorità giurisdizionale*.
In maniera agevole il Tribunale palermitano rigetta la prima eccezione sollevata. Nei procedimenti relativi alla criminalità organizzata, così come lo era quello in concreto, l'intercettazione domiciliare, in deroga al limite di cui al comma 2 dell'art. 266 c.p.p., è consentita "*anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa*", *ex* art. 13 del d.l. nr. 152 del 1991. Non vi è nessun obbligo, infatti, nelle ipotesi in cui la intercettazione avvenga in luogo di privata dimora, quando si procede per il delitto di cui all'art. 416 *bis* c.p., di motivare sul fatto che vi sia fondato motivo di ritenere che ivi si stia svolgendo un'attività criminosa. Il provvedimento autorizzatorio del giudice per le indagini preliminari, pertanto, era legittimo e non aggirava alcun divieto di legge.
Relativamente alla eccezione formulata sulla mancata precisione delle coordinate e dei confini spaziali, il collegio palermitano ha seguito un percorso argomentativo pregevole ed efficace.
Poiché l'indagato, attraverso la rete informatica, mantiene i contatti con i sodali, si sottolinea il rapporto di *pertinenzialità* tra il dispositivo elettronico -lo *smartphone* c.d. bersaglio- e le reti di relazioni mafiose *online* attivatasi attraverso l'utilizzo dei mezzi di comunicazioni informatici -*skype, internet*- tra cui quello in uso all'indagato.
Il Tribunale ritiene soddisfatta la specificazione dei luoghi che il decreto avrebbe individuato nella *stanza in cui è ubicato l'apparecchio informatico*, nella quale l'indagato si collega telematicamente con i suoi interlocutori del medesimo mandamento mafioso. Tale delimitazione garantisce che le conversazioni intercettate abbiano ad oggetto non vicende private della famiglia dell'indagato, come sarebbe stato se si fosse intercettato l'intero appartamento, ma solo l'attività criminosa circoscritta in quel contesto spaziale in cui il sodale si collega con gli altri affiliati per la gestione delle vicende di interesse mafioso.
La predetta considerazione era suffragata dal fatto che il captatore informatico, inserito nello *smartphone* intercettato, non copre una raggio superiore a 10 metri di distanza rispetto al luogo in cui l'apparecchio è posizionato.[4]

[4] Il predetto ragionamento non è scevro di *critiche*. In dottrina si afferma che la pretesa garanzia aumentata in punto di *privacy* presuppone che l'ascolto non attinga a colloqui relativi a vicende personali e strettamente private. Circostanza, di fatto, imprevedibile. Sarebbe, altresì, fuorviante il richiamo della stanza dove è ubicato il dispositivo informatico. Il riferimento ai luoghi *per relationem*, infatti, potrebbe permettere che l'apparecchio

Al riguardo, sulla base delle considerazioni svolte, meritano di essere approfondite due tematiche affrontate dalla sentenza succitata: le intercettazioni disposte per i delitti di criminalità organizzata e, più in particolare, l'ambito di applicazione (*rectius* raggio di azione) del *virus trojan*.

Per procedere alle intercettazioni nei procedimenti relativi alla criminalità organizzata, i requisiti sono in qualche modo attenuati rispetto al procedimento ordinario.

Le intercettazioni sono ammesse quando vi siano *sufficienti* indizi di reato, e non gravi indizi, come stabilito per i procedimenti contro i reati comuni, e quando le stesse siano *necessarie* e non indispensabili, *ex* art. 267 c.p.p., per lo svolgimento delle indagini. Le intercettazioni ambientali nel domicilio sono consente anche se *non* vi è motivo di ritenere che nei luoghi predetti si stia svolgendo attività criminosa.

Relativamente all'ambito di applicazione del *malware* denominato *trojan* è necessario, considerato la novità del suo utilizzo nelle fattispecie che stiamo considerando, un maggiore *approfondimento*.

Tutte le volte che si parla di captatore informatico, in ambito investigativo, è necessario distinguere tra due diverse modalità operative: quella *online search* e quella *online surveillance*.

I programmi appartenenti alla prima categoria consentono di fare copia, totale o parziale, delle unità di memoria del sistema informatico individuato come obiettivo. I dati sono trasmessi in tempo reale o ad intervalli prestabiliti, agli organi di investigazione tramite la rete internet in modalità nascosta e protetta.

Attraverso i programmi *online surveillance* è possibile, invece, captare il flusso informatico intercorrente tra le periferiche -video, microfono, tastiera, *webcame*- e il microprocessore del dispositivo bersaglio, consentendo al centro remoto di controllo di monitorare in tempo reale tutto ciò che viene visualizzato sullo schermo c.d. *screenshot*, digitato sulla tastiera c.d. *keylogger* o pronunciato al microfono.

Si tratta *softwares* che, prescindendo dalle autorizzazioni dell'utente, si installano in un sistemo scelto come obiettivo e ne acquisiscono qualsiasi informazione. Il virus *trojan* prende il suo nome, verosimilmente, dal leggendario cavallo di Troia che, per mezzo di Odisseo, l'uomo dal multiforme ingegno, riuscì ad entrare dentro le mura di Troia, con inganno, ed espugnarla.

Così come il cavallo di Troia sconfisse i Troiani entrando all'interno della loro cittadella muraria, fingendosi un dono pregiato da parte degli Achei, così anche il predetto *virus* riesce ad entrare, con inganno, nell'apparecchio (attraverso una richiesta di *download*, ad esempio) che si vuole intercettare, non per distruggerlo ne' tanto meno per danneggiarlo, ma per carpire qualsiasi dato che ivi possa trovarvi.

Tali programmi sono concepiti e costruiti per istallarsi in modo occulto sui congegni elettronici che si vuole monitorare ed agiscono senza rilevare all'utente la propria presenza.

---

infettato, proprio perché mobile, possa essere collocato anche in luoghi diversi dall'indagato, fino alle stanze private, e li rimanervi fino alla sua successiva utilizzazione.

Essi comunicano attraverso *internet* in modalità nascosta e protetta, con un centro remoto di comando e controllo che li gestisce, catturando ogni possibile informazione scambiata o messaggio digitato.
Possono cercare tra i *files* presenti nel *personal computer* infettato o su altri collegati in rete locale, captano tutto il traffico di dati in arrivo e in uscita, attivano, autonomamente, il microfono e la *webcamera* per carpirne voci ed immagini e sono in grado di perquisire l'*hard disk* e di fare copia delle unita i memoria del sistema informatico preso di mira[5].
I *software* dispongono, altresì, di contromisure che li rendano in grado di nascondersi agli *antivirus* e di sfruttare la vulnerabilità dei sistemi applicativi.
Addirittura nelle versioni più evolute, questi programmi possono operare come veri e propri sistemi di controllo remoto c.d. *remote control system* e funzionare in maniera autonoma senza intervento diretto delle persone.
Il *virus trojan* si occupa della captazione della voce dell'utilizzatore e di quella dell'interlocutore dopo essere stata decifrata. Le informazioni così ottenute vengono mandate ai *server* esterni, collocati presso la sala di ascolto.
Ciò avviene se il dispositivo elettronico sia collegato alla rete, nel caso in cui non lo fosse, le predette informazioni verranno salvate in locale ed inviate al *server* non appena risulti disponibile un collegamento alla rete.
Le intercettazioni che avvengono sfruttando le potenzialità degli agenti intrusori sono dette anche ***itineranti*** perché, trattandosi di intercettazioni ambientali, che prescindono dal riferimento ai luoghi, si spostano insieme allo *smartphone* in cui sono istallati e sono, altresì, dotati del dono della ***ubiquità*** perché possono captare qualunque informazioni ovunque esse si trovino e, quindi, sono suscettibili di "*entrare*" contemporaneamente in una pluralità di luoghi di privata dimora.[6]
La captazione di informazioni mediante *malware* si definisce, anche, ***dinamica***. Il dispositivo mobile segue gli spostamenti dell'intercettato e le informazioni captate variano a seconda del luogo in cui l'apparecchio "*infettato*" dal *virus* informatico sia posizionato. È totalmente differente l'ambito di applicazione della tradizionale cimice-microspia.
Grazie alle sue ridotte dimensioni, la classica cimice poteva facilmente essere occultata sia in ambiente domestico che lavorativo, perché poteva nascondersi e mascherarsi in qualsiasi oggetto, tuttavia, a differenza del *virus* informatico, una volta posizionato, *manualmente* (non è superfluo ricordare che i *virus* in esame si installano *autonomamente* presso il *computer bersaglio*), capterà solo ed esclusivamente le informazioni del luogo in cui la stessa è stata collocata.

---

[5] In riferimento alle intercettazioni telematiche occorre dare atto del diffuso utilizzo di *skype*. Trattasi di un *software* che consente di parlare in tutto il mondo, per effettuare gratuitamente videochiamate e chiamate con un solo interlocutore e chiamate di gruppo, inviare messaggi istantanei e condividere *files* con altri utenti di *Skype*. Si può utilizzarlo sul telefono cellulare, sul *computer* oppure su una TV abilitata.

[6] Cfr. *Memoria per la Camera di Consiglio delle Sezioni Unite della Procura generale presso la Corte di Cassazione* del 28.04.2016 in *www.dirittopenalecontemporaneo.it*

Da quanto si evince, pertanto, i mezzi tecnologici in esame, utilizzati per le intercettazioni, costituirebbero una vera e propria *rivoluzione* nell'ambito delle captazioni informatiche.
Basterebbe, infatti, un solo *click* degli agenti addetti all'ascolto, previa, naturalmente, autorizzazione del giudice nelle forme di legge, per impossessarsi, seppur *virtualmente*, dell'apparecchio elettronico infettato.
Ciò, ragionevolmente, ha destato molte perplessità, soprattutto in ordine ai limiti della ammissibilità di questo meccanismo investigativo, dalle potenzialità non ancora pienamente conosciute, rispetto alla tutela di diritti primari della persona. La domanda, allora, che bisogna porsi è se i diritti fondamentali potrebbero soffrire di un mancato adeguamento, in termini di tutela, rispetto all'evoluzione tecnologica e all'esigenza di un'efficace perseguimento di reati.
E' lo stesso legislatore, infatti, che orienta l'interprete e stabilisce i casi in cui la tutela dei diritti medesimi sia recessiva ad altri fini di pari importanza per la sopravvivenza dell'ordinamento.
I difensori dell'indagato, la cui richiesta di riesame da parte del collegio palermitano era stata rigettata, ritenevano che il ragionamento posto in essere dal giudice fosse erroneo e, di conseguenza, impugnavano la sentenza presso la Corte di Cassazione.
L'impostazione difensiva ribadiva, con forza, l'inutilizzabilità delle intercettazioni effettuate mediante *virus* informatico e, a sostegno della predetta tesi, citavano una importantissima sentenza della Corte di Cassazione che affermava il seguente principio di diritto "*l'intercettazione da remoto delle conversazioni tra presenti, con l'attivazione tramite il c.d. agente intrusore informatico del microfono di un apparecchio telefonico smartphone, può ritenersi legittima solo se il relativo decreto autorizzativo individui* ***con precisione*** *i luoghi in cui eseguire tale attività captativa"* (Cass. nr. 27100 del 2015).
Il predetto orientamento sulla base del fondamentale principio secondo il quale la libertà e la segretezza delle comunicazioni sono inviolabili, sosteneva che le norme che prevedevano la possibilità di intercettare comunicazioni tra presenti fossero di *stretta interpretazione*, ragion per cui non poteva considerarsi giuridicamente corretto attribuire alla norma codicistica una portata applicativa così ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si trovi.
Pertanto, l'unica opzione interpretativa, compatibile con il dettato costituzionale, era quella secondo cui l'intercettazione ambientale dovesse, *obbligatoriamente*, avvenire in luoghi ben circoscritti e individuati *ab origine* dal giudice. Nel caso in cui le intercettazioni si siano realizzate, fuori i casi di legge, *ex* art. 271 c.p.p., infatti, la conseguenza è quella della inutilizzabilità.
Le intercettazioni mediante *virus* informatico, a tal proposito, sono illegittime perché violano un espresso divieto probatorio che trova il proprio riconoscimento nel codice, nel comma 2 dell'art. 266 c.p.p. e, prima ancora, nella Costituzione, *ex* artt. 2, 14 e 15. Al giudice, pertanto, sulla base di una *prova di resistenza*, è imposto di verificare se le rimanenti risultanze, siano in grado di fondare la gravità indiziaria che è alla base della misura cautelare disposta nei confronti dell'indagato.

La Suprema Corte, tuttavia, ometteva di considerare che la fattispecie, sulla quale era chiamata a pronunciarsi, riguardava il delitto di associazione mafiosa, *ex* art. 416 *bis* c.p., e, pertanto, le intercettazioni presso il domicilio dell'indagato possono essere realizzate *senza* che via sia il fondato motivo che ivi si stia svolgendo attività criminosa.
Il legislatore, ha previsto, con una legge speciale, *ex* art.13 d.l. nr.152 del 1991, rispetto allo stesso codice di procedura, che nei procedimenti relativi ai delitti di criminalità organizzata, la clausola di salvaguardia, *ex* art. 266, comma 2 c.p.p., non dovesse operare.
In un bilanciamento fra diritti, infatti, secondo un'interpretazione ragionevole delle norme costituzionali, la prevenzione di reati gravi che potrebbero essere commessi in danno alla sicurezza della collettività, al benessere sociale, alla vita, alla libera autodeterminazione delle persone e al loro patrimonio imporrebbe che il diritto della riservatezza e del domicilio possano essere considerati cedevoli.
Altresì, un orientamento consolidato ha sempre escluso una precisa indicazione dei luoghi, ad eccezione nei casi di luoghi di dimora, seconda una interpretazione più corretta del testo di legge.[7]
La Corte di Cassazione, nr. 13884 del 2016, rilevato il contrasto tra la succitata pronuncia e un orientamento pressoché consolidato della Suprema Corte contrario decide rimettere la decisione alle Sezioni Unite, considerato che la sezione *de qua* non ritiene di poter accogliere le "*radicali conclusioni*" cui era giunta le sentenza nr. 27100 del 2015.
Considerata la delicatezza della materia, in cui il ricorso a strumenti di sofisticata tecnica informatica di forte invadenza nella *privacy* dei soggetti e dei di lui conviventi intercettati compromette valori tutelati dalla nostra Costituzione e dalle Convenzione internazionali il cui rispetto l'Italia è vincolata, *ex* art.117 Cost., e dall'altra, l'esigenza assicurare una maggiore capacità investigativa da parte degli organi inquirenti per la repressioni di crimini gravi, così come sono quelli di criminalità organizzata, la sesta sezione, ritenendo la questione sottoposta alla sua attenzione di massima importanza, al fine di evitare contraddizioni e aporie in seno all'ordinamento, rimette gli atti al Primo Presidente.
L'interrogativo che si pongono i giudici è se la disciplina delle intercettazioni consenta di poter prescindere dalla indicazione del luogo ovvero, se l'omessa indicazione determini l'inutilizzabilità del mezzo di ricerca della prova.
In via preliminare, infatti, come si è avuto modo di notare, con riferimento alla tecnica dell'agente intrusore, la pretesa di indicare con precisione e anticipatamente i luoghi interessati dall'attività captativa è *incompatibile* con questo tipo di intercettazione, che, per ragioni tecniche (e puramente pratiche aggiungerei) prescinde dal riferimento preciso e specifico del luogo.

[7] Cfr. *ex plurimis* Cass. nr. 3541 del 1999 e Cass. 3677 del 2003.

L'attività di captazione segue tutti gli spostamenti nello spazio del suo utilizzatore. Questo, naturalmente, comporta che al giudice sia impedito conoscere *ex ante* i luoghi in cui lo *smartphone* verrà attivato dall'indagato.
Il problema, così come è stato esposto dal Collegio, potrebbe essere risolto considerando la *natura giuridica* della intercettazione informatica.

Rilevato che la stessa abbia delle peculiarità nella sua utilizzazione rispetto al modello classico di intercettazione, si imporrebbe al giudice di cogliere le suddette specificità e renderle ben evidenti nel procedimento di autorizzazione.
La soluzione migliore, infatti, sarebbe quella di ritenere utilizzabile l'intercettazione itinerante, *a patto che* il decreto di autorizzazione delle intercettazioni *de quibus* sia adeguatamente motivato per giustificare le ragioni per le quali si ritiene debba utilizzarsi la metodica dell'istallazione da remoto, consentendo una captazione di informazioni dinamica.
Così facendo, non solo le intercettazioni informatiche avrebbero una copertura legislativa, al riguardo si rinvia agli artt. 266 e 266 bis c.p.p., ma vi sarebbe anche un'adeguata motivazione sul punto. Il giudice, infatti, sarà chiamato ad autorizzare la predetta captazione fornendo una più precisa esposizione dei presupposti di fatto e giuridici che stanno alla base della sua decisione.
Sebbene debba riconoscersi l'invadenza imponente delle intercettazioni in esame, si può rilevare che il principio, secondo cui il decreto di autorizzazione debba individuare con precisione i luoghi all'interno dei quali dovrà essere eseguita l'intercettazione delle comunicazioni tra presenti, non è desumibile *da alcuna disposizione di legge* (è stata la *sola* giurisprudenza a ritenere l'indicazione della *sedes intercettandi* un presupposto funzionale alla tutela dei diritti costituzionalmente garantiti che vengono in gioco).
La necessità dell'indicazione del luogo specifico, quale assoluta condizione per l'ammissibilità delle intercettazioni, non risulta, infatti, *nemmeno*, inserita come presupposto di validità nelle copiose *sentenze della Corte di Strasburgo*, secondo cui le garanzie minime, che la legge nazionale deve apprestare nella materia delle intercettazioni, riguardano: la predeterminazione della tipologia delle comunicazioni oggetto di intercettazione riguardano la predeterminazione della tipologia delle comunicazioni oggetto di intercettazione, la ricognizione dei reati che giustificano tale mezzo di intrusione nella *privacy*, l'attribuzione di un organo indipendente della competenza ad autorizzare le intercettazioni con il controllo del giudice e la definizione della categorie di norme prefissate, i limiti della durata delle intercettazioni e i casi in cui le risultanze delle registrazioni captate vadano distrutte.[8]
La questione che la Suprema Corte sottopone all'attenzione delle Sezioni Unite può sintetizzarsi come segue: "*se, anche nei luoghi di privata dimora, ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa, sia consentita l'intercettazione di conversazioni o comunicazioni tra*

[8] Si rinvia, sul punto, alle sentenze della Corte EDU, 31 maggio 2005, *Vetter contro Francia*; Corte EDU, 18 maggio 2010, *Kennedy contro Regno Unito*.

presenti, mediante l'istallazione di un captatore informatico in dispositivi elettronici"

La Suprema Corte, con decisione del 28 aprile del 2016, fornisce risposta *parzialmente* affermativa al superiore quesito.

L'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico in un dispositivo elettronico, infatti, è consentita nei ***soli procedimenti per delitti di criminalità organizzata*** per i quali trova applicazione la disciplina di cui all'art. 13 del d.l. n. 151 del 1991, convertito dalla legge nr. 203 del 1991, che consente la captazione anche nei luoghi di privata dimora, senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto.

La medesima Corte ha cura di sottolineare che, in considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso.

Il riferimento al *luogo*, a tal proposito, non rappresenta un *presupposto* per l'autorizzazione delle intercettazioni ma soltanto un *elemento* ravvisabile nella motivazione del relativo decreto nella quale il giudice "*deve indicare le situazioni ambientali oggetto della captazione, e ciò solo ai fini della determinazione delle modalità esecutive del mezzo della ricerca della prova che avviene mediante la collocazione fisica di microspie*".

La locuzione intercettazioni ambientali è entrata a far parte del linguaggio giuridico in un momento storico nel quale le intercettazioni tra presenti erano possibili soltanto attraverso l'installazione di microspie in determinati ambienti preventivamente individuabili. Da qui, dunque, l'esigenza di individuare i luoghi in cui materialmente collocarle. Tale condizione, tuttavia, non è prevista ai fini della legittimità del provvedimento autorizzativo.

Relativamente alle *sole* intercettazioni tra presenti nei luoghi di cui all'art. 614 c.p., e, dunque, nei luoghi di privata dimora, è necessario il "*fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa*".

Solo ed esclusivamente per questi luoghi e nelle condizioni indicate dal comma 2 dell'art. 266 c.p.p., la previa determinazione dei luoghi opera come requisito di legittimità ai fini dell'autorizzazione delle intercettazioni tra presenti.

Ne deriva, dunque, che, nonostante l'individuazione dei luoghi non sia requisito di legittimità dell'atto autorizzativo, l'utilizzazione del sistema del captatore informatico non è consentito per le intercettazioni tra presenti in quanto all'atto di autorizzare un'intercettazione da effettuarsi con tale tecnica, il giudice non può prevedere i luoghi di privata dimora nei quali il dispositivo verrà introdotto "*con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale*".

Ciò potrebbe dar luogo ad una pluralità di intercettazioni nei luoghi di privata dimora che comporterebbero la violazione di limiti non soggetti ad eccezione alcuna e per i quali la determinazione dei luoghi è condizione di legittimità dell'autorizzazione.
La Corte, infine, ha anche chiarito che per l'ipotesi in cui lo strumento captativo informatico dovesse produrre eventi lesivi della dignità umana, tale pericolo potrebbe essere neutralizzato, facendo discendere dal principio personalistico di cui all'art. 2 Cost., la sanzione della *inutilizzabilità* delle risultanze di specifiche intercettazioni
Gli Ermellini inquadrano immediatamente la fattispecie problematica della questione sottoposta alla loro attenzione. "*Il tema,* si legge, *deve essere esaminato muovendo necessariamente da una approfondita lettura delle disposizioni del codice di rito e della norma speciale, di cui all'art. 13 del d.l. nr. 152 del 1991*".
Uno dei nodi interpretativi che aveva suscitato ampio dibattito in giurisprudenza consisteva nella individuazione del rapporto normativo tra le disposizioni codicistiche, di cui all'art.266, comma 2 c.p.p. e quella speciale, di cui all'art. 13.
La pronuncia nr. 27100 del 2015, infatti, aveva ritenuto di applicare ad una vicenda di associazione mafiosa, sottoposta alla sua cognizione, quegli stessi limiti non previsti dall'art. 13 per i delitti di criminalità organizzata ma, che, invece, sono specificati dall'art. 266, comma 2 c.p.p., per tutti gli altri reati meno gravi.
L'art. 13 d.l. 152 del 1991, come norma speciale, rispetto all'art. 266, comma 2, c.p.p., dispone, testualmente, che "*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*".
La disposizione in commento specifica l'ambito della sua applicazione ai *soli delitti di criminalità organizzata*, circoscrivendo la sua portata rispetto alla formulazione generale, di cui all'art. 266, comma 2, c.p.p. Sicché, nel contrasto tra norma generale e norma speciale successiva, entrambe aventi pari grado gerarchico, prevale la norma speciale. La norma contenuta nel codice di procedura, pertanto, non andava applicata al caso concreto, in quanto risultava essere stata *derogata*.
La stessa Corte ha il merito di individuare con chiarezza la categoria dei *delitti di criminalità organizzata* per i quali possa trovare applicazione la deroga sopra enunciata.
Non vi è unanimità di vedute nella definizione dei predetti delitti.
Da una parte, si vorrebbero comprendere tutti i reati collegabili, a qualsiasi titolo, alle associazioni criminali ovvero quelli che presuppongono l'esistenza di un alto livello di capacità criminale in capo a chi ne è responsabile o, finanche, a tutte le ipotesi di concorso di persone nel reato, quando vi sia una suddivisione dei compiti al fine di collaborare per la realizzazione dl medesimo risultato antigiuridico. Dall'altra, si riferisce il concetto di criminalità organizzata a delitti tassativamente previsti da elenchi normativi.

Una prima tesi ha fatto riferimento al catalogo di reati di cui all'art. 407, comma 2, lett. a) c.p.p.[9]
Un altro orientamento ha fatto riferimento ai reati previsti dall'art. 51, comma 3*bis* c.p.p. rilevando che l'art. 54 *ter* c.p.p., in tema di contrasti tra pubblici ministeri e l'art. 371 bis c.p.p. che regola l'attività di coordinamento del Procuratore nazionale antimafia.[10]
Ben presto, considerata il mancato accordo interpretativo sulla nozione *de qua*, si è affermata una diversa opzione interpretativa di tipo *finalistico*, secondo la quale il significato dell'espressione "*criminalità organizzata*" deve essere individuato avendo riguardo alle finalità specifiche della singola disciplina che deroga alla regola processuali generali. Sono ricomprese in detta categoria, pertanto, attività criminose eterogenee, purché realizzate da una pluralità di soggetti, i quali, per la commissione del reato, abbiano costituito un apposito apparato organizzativo, con esclusione del mero concorso di persone.
È sufficiente la costituzione di un apparato organizzativo, la cui struttura assume un ruolo preminente rispetto ai singoli partecipanti.
La conclusione, cui perviene la Suprema è la seguente "*per i reati di criminalità organizzata devono intendersi non solo quelli elencati dall'art. 51, commi 3bis e 3 quater, c.p.p. ma anche quelli comunque facenti capo ad una associazione per delinquere, ex art. 416 bis c.p. correlata ad attività criminose più diverse, con esclusione del mero concorso di persone*".

3. Prospettive de *jure condendo*

Pochi mesi successivi alla emanazione della sentenza della Sezioni Unite, precisamente il 29 luglio 2016, con un comunicato stampa, alcuni docenti di ruolo nelle Università italiane emanano un documento in cui esprimono "*preoccupazione*" per l'impiego dei mezzi di intrusione informatica non *formalmente* regolati dalla legge ma, *sostanzialmente*, legittimati dalla giurisprudenza.

---

[9] Cfr. Tra i quali (…) "*3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo;*
4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma, e 306, secondo comma, del codice penale (…)*".*

[10] *"Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 416, sesto e settimo comma, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 600, 601, 602 , 416bis e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'articolo 74 del testo unico approvato con decreto del Presidente della Repubblica 9 ottobre 1990 n. 309 e dall'articolo 291quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43 le funzioni indicate nel comma 1 lettera a) sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente".*

Le interpretazioni estensive utilizzate dai giudici, in una materia in cui vige un principio di riserva di legge e di tassatività (l'inviolabilità del domicilio e della segretezza) non sono idonee ad introdurre nel nostro *Stato di diritto* meccanismi di captazione la cui applicazione è rimessa alla discrezionalità dell'organo procedente, senza che via siano limiti legislativi sull'utilizzo di questi strumenti.

"*Si auspica*, si legge, *che i suddetti strumenti siano ritenuti indispensabili per l'accertamento dei gravi reati e che il legislatore intervenga con specifiche disposizioni a regolare la materia nell'adeguato bilanciamento dei principi costituzionali*".[11]

Il nostro legislatore, negli ultimi tempi, anche sulla spinta di eventi che hanno avuto caratteri dal sapore politico, ha espresso la propria intenzione di riformare la materie delle intercettazioni, soprattutto per evitare le indebite divulgazioni delle stesse.

Le intercettazioni, infatti, al di là del piano processuale in cui generano i loro effetti, hanno delle refluenze immediate sul versante sociale e politico.

Il 2 agosto scorso, la Commissione giustizia del Senato ha adottato un testo unificato di legge nr. **2067**, contenente "*le modifiche al codice penale e di procedura per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi nonché all'ordinamento giudiziario*".

In particolare, il testo conferisce al Governo una delega per la riforma del processo penale sulla materia *de qua*.

Fatte salve le intercettazioni nel caso di reati gravi come mafia e terrorismo, l'emendamento in questione riduce il campo d'azione del *virus* informatico. Prevede, infatti, che le intercettazioni, così ottenute, possano essere utilizzate ai fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e possano essere utilizzati in procedimenti diversi a condizione che siano indispensabili per l'accertamento dei delitti di cui all'art. 380 c.p.p.[12].

L'attivazione del microfono deve avvenire solo in conseguenza di un apposito comando inviato da remoto e non con il solo inserimento del *virus*, nel rispetto dei limiti stabiliti dal decreto di autorizzazione del giudice.

In ogni caso, il decreto di autorizzazione deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini.

La procedura investigativa *de qua*, sulla scorta di quanto previsto dalle Sezioni Unite, è sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51,

---

[11] Cfr. *Comunicato del Dipartimento di Giurisprudenza* presso l'Università degli Studi di Torino del 29 luglio 2016 in *www.dg.unito.it*

[12] Cfr. (…) *i) delitti commessi per finalità di terrorismo o di eversione dell'ordine costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni;*
(…) *l-bis) delitti di partecipazione, promozione, direzione e organizzazione della associazione di tipo mafioso prevista dall'articolo 416 bis del codice penale;*
m) delitti di promozione, direzione, costituzione e organizzazione della associazione per delinquere prevista dall'articolo 416 commi 1 e 3 del codice penale, se l'associazione è diretta alla commissione di più delitti fra quelli previsti dal comma 1 o dalle lettere a), b), c), d), f), g), i) del presente comma.

comma 3*bis* e *quater*, e fuori da tali casi, nei luoghi di cui all'art. 614 c.p. qualora si stia svolgendo attività criminosa.
Il trasferimento delle informazioni deve essere effettuato soltanto verso il *server* della Procura così da garantire l'originalità ed integrità delle registrazioni e al termine della registrazione il captatore informatico viene disattivato e reso inutilizzabile.
E' necessario che i programmi informatici utilizzati siano conformi ai requisiti tecnici stabiliti con apposito decreto al fine di garantire uno *standard* di certezza e affidabilità.
Il pubblico ministero, in caso di *urgenza*, limitatamente ai delitti di cui all'art. 51, comma 3*bis* e *quater,* c.p.p., può di disporle con successiva convalida del giudice entro il termine massimo di quarantotto ore, sempre che il decreto d'urgenza dia conto delle specifiche situazioni di fatto che rendano impossibile la richiesta al giudice e delle ragioni per le quali tale specifica modalità di intercettazione sia necessaria allo svolgimento delle indagini.
I risultati acquisiti non possono essere conoscibili, divulgabili ne' pubblicabili se abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede.
Si può notare come il nostro legislatore si preoccupi di precisare in che modo il *software trojan* debba essere utilizzato, a tal proposito, si indicano i reati per il perseguimento dei quali il *malware* potrà essere installato, la motivazione specifica del giudice, quasi a denotare una *extrema ratio* della procedura *de qua* rispetto a quella ordinaria.
La proposta di legge, fin qui esaminata, non è che l'unica di una serie di progetti incardinati presso le Camere e che ivi giacciono insabbiati.
Si tratta, perlopiù, di progetti di legge che trovano fondamento in contributi dottrinali che si sono confrontati con le prime applicazioni del particolare strumento tecnologico in argomento e che auspicano l'intervento di una precisa regolamentazione per definire i modi ed i casi dell'azione investigativa, considerando i canoni della proporzionalità e della necessità dell'ingerenza pubblica nella vita privata.
Nel corso dei lavori parlamentari per la conversione del **d.l. nr. 7 del 2015** "*misure urgenti per il contrasto al terrorismo, anche di matrice internazionale*" era stata proposta una modificazione dell'art. 266*bis* c.p.p. inserendo le parole "anche attraverso l'impiego di strumenti o programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico" ma, in sede di conversione, la norma era stata stralciata.
La proposta di legge nr. C. **3470** "*Modifiche all'art. 266bis c.p.p. in materie di intercettazioni e di comunicazioni informatiche o telematiche*". Intendendo garantire l'adeguamento tecnologico del sistema delle intercettazioni, mediante l'utilizzo dei programmi informatici che consentano l'accesso al computer da remoto, per acquisire dati presenti in un sistema informatico ritenute utili per le organizzazioni criminali, anche di stampo terroristico,

E, successivamente, segue quella nr. C. **3762**, dell'aprile di quest'anno, illustra, sul piano metodologico prevede l'utilizzo captatori legali per i reati di cui all'art. 51 comma 3*bis* e *quater* e disciplina il loro uso per compiere intercettazioni dei flussi di dati e per la localizzazione geografica del dispositivo. Ne sancisce, tuttavia, il carattere residuale.

Altro problema di cui il legislatore si è occupato, sempre collegabile al tema che stiamo trattando, riguarda l'utilizzazione degli atti giudiziari e la successiva pubblicazione da parte degli organi di informazione delle intercettazioni relative a conversazioni di contenuto non incriminate intercorse con persone non indagate.

Costituisce un tema molto importante, soprattutto alla luce del fatto che l'apparecchio infettato mediante *virus* informatico è capace di captare qualsiasi informazione e comunicazione effettuata dall'indagato e da soggetti terzi, ad esempio i suoi familiari.

Si pensi al caso di un *computer*, in cui è installato il *malware*, che sia utilizzato da tutti i componenti della famiglia che, come una sorta di diario personale, conservano e inviano foto, dati ed informazioni personali, c.d. *uploading*, che nulla hanno a che vedere con l'indagine.

In primo luogo, la spesso difficile identificabilità tra i ruoli, soprattutto nei reati a criminalità organizzata, nel corso delle indagini preliminari non consente di creare una distinzione tra soggetti coinvolti e soggetti terzi, se non in una fase prossima all'esercizio dell'azione penale, con l'effetto di ritardare di molto l'operatività di un eventuale filtro che opererebbe *ex post*.

Dall'altro, le conversazioni intrattenute con soggetti estranei alle indagini possono assumere un significativo valore probatorio solo se contengano dichiarazioni accusatorie rese al terzo dall'autore di reato o in quanto utile a ricostruire il contesto in cui si svolge l'azione criminale.

Questo patrimonio di informazioni non può definirsi *a priori* non rilevante. Spetta all'autorità giudiziaria in modo esclusivo stabilire in relazione alla singola indagine in che misura dare riscontro nel contesto degli elementi acquisiti.

In questo campo, pertanto, spetta al magistrato procedente individuare il punto di equilibrio tra l'esigenza di suffragare il quadro probatorio in vista di un migliore accertamento giudiziario e l'esigenza di tutelare la *privacy* dei terzi estranei all'indagine che, comunque, in nessun caso, può essere arbitrariamente pregiudicata.

Il 29 luglio 2016, molto efficacemente, il Consiglio Superiore della Magistratura ha emanato una delibera[13] in materie di intercettazioni per richiamare gli organi giudiziari a "*manipolare con cura*" i dati personali cui vengono in contatto nell'esercizio dell'attività investigativa le intercettazioni, infatti, costituiscono uno fra i possibili strumenti attraverso i quali gli attori del processo vengono in possesso di dati personali con il conseguente obbligo di garantirne la correttezza.[14]

---

[13] Pratica nr. 285/VV7206. *Ricognizione di buone prassi in materia di intercettazione di conversazione* del 29 luglio 2016, in *www.csm.it*.

[14] Sui criteri direttivi in materie di trascrizione delle intercettazioni e la loro utilizzazione da parte del pubblico ministero si rinvia alle *Circolari* emanate dalla Procura di Napoli, direttiva

Sia le Procure distrettuali che il Consiglio Superiore della Magistratura non affrontano il tema delle intercettazioni informatiche mediante agente intrusore.
Per la novità della tematica e, forse, ancora per il suo limitato (quanto originale e multiforme) utilizzo non hanno provveduto ad emanare, ad oggi, le linee guida per la loro applicazione.

4. Uno sguardo all'Europa

Il problema delle intercettazioni mediante *virus* informatico è stato affrontato in sede legislativa e giurisprudenziale in diversi paesi europei.
In questa, sembra opportuno accennare alla legislazione tedesca, spagnola e francese.
Un primo caso importante di utilizzo di tali sistemi si ebbe in ***Germania***, quando nel 2006, nel *Land* del nord Reno-*Westfalia*, si introdusse la possibilità di condurre attività di *intelligence* per il tramite di programmi -*backdoors*-[15] eseguiti sul *computer* con l'intento di creare collegamenti tra lo stesso ed un suo remoto, in modo da consentire al fruitore di quest'ultimo il pieno controllo del primo sistema informatico.
Addirittura, si autorizzava un organismo tecnico investigativo, afferente al Ministero dell'interno, ad effettuare l'accesso segreto nei sistemi informatici "*a tutela della Costituzione*".
La Corte Costituzionale ha dichiarato incostituzionale la predetta disposizione, chiarendo che l'illegittimità della norma di legge impugnata non ha ad oggetto l'ammissibilità del nuovo mezzo investigativo di ricerca della prova, di carattere tecnologico, ma la sua previsione in termini assoluti e poco nitidi da parte del legislatore. Quest'ultimo, a parere dei giudici, avrebbe dovuto determinare i casi, finalità, ed i confini di compressione dei diritti fondamentali e limitare la zona di intervento ai gravi reati a tutela di importanti beni giuridici, quali la sicurezza nazionale e la sopravvivenza ordinata dell'ordinamento.
La ***Spagna***, con apposita legge nr. 13 del 2015, ha disciplinato la captazione e la registrazione mediante l'impiego di dispositivi elettronici. Le intercettazioni mediante *virus* informatico, a tal proposito, devono risultare necessarie e sussidiarie agli altri mezzi di ricerca della prova.
Questa misura, si legge, è ritenuta fondamentale per lo svolgimento delle indagini nel processo penale ma "*non caben autorizaciones de captaciòn y grabaciòn de conversaciones orales de caràcter general o indiscriminatas, debiendose identificar con precision en lugar o dependencias sometidos a vigilancia*".

1/2016 del 16 febbraio 2016, della Procura di Torino del 15 febbraio 2016 e della Procura di Roma , circ. nr. 27del 26 novembre 2015

[15] Sono programmi malevoli che si insediano nel computer utilizzando "*una porta sul retro*" (ecco la traduzione italiana del *malware*) già aperta da altri programmi e difficilmente individuabili dagli *antivirus*. Hanno lo scopo di creare un collegamento nascosto tra il computer attaccato e quello attaccante.
Dal *computer* attaccante può arrivare un gran numero di comandi che il *computer* attaccato esegue, senza che il proprietario se ne renda conto.

La norma, prevede, pertanto, che il decreto di autorizzazione del giudice specifichi le generalità delle persone nei cui confronti andranno svolte le intercettazioni, i mezzi mediante si quali si procederà alla captazione delle telecomunicazioni ed i luoghi ad essa afferenti.

La ***Francia***, da ultimo, prevede l'utilizzo del *virus* informatico per una serie di gravi delitti, tra i quali sono compresi quelli di criminalità organizzata e terrorismo, sotto il controllo del giudice e senza alcuna indicazione dei luoghi in cui deve essere seguita la captazione informatica "*d'accèder en tous liex a dès donnès informatiques, de lès enregistrer telles qu'elles s'affichent sur un ècran pour l'utilisateur d'un systeme de traitement automatisè de donnès, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont recues et emises par des pèriphèriques audiovisuel*"[16]

[16] Sul punto si rinvia ad *Allegato alla memoria della Procura generale per la Camera di consiglio della Corte di Cassazione* del 28.04.2016 in *www.dirittopenalecontemporaneo.it*