LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI GIURISPRUDENZA
CATTEDRA DIRITTO PROCESSUALE PENALE

IL CAPTATORE INFORMATICO: UTILIZZO DEL VIRUS *TROJAN HORSE* NELLE INTERCETTAZIONI DI COMUNICAZIONI TRA PRESENTI

RELATORE
Chiar.mo Prof. Giulio Illuminati

CANDIDATA
Francesca Severoni
107783

CORRELATORE
Chiar.mo Prof. Paolo Moscarini

ANNO ACCADEMICO 2018/2019

ai miei genitori. Sempre vicini in ogni traguardo della mia vita.

« *Timeo Danaos et dona ferentes*»

(Eneide, Libro II, 49.
Publio Virgilio Marone, parole di ammonimento di Lacoonte ai Troiani intenti a portare il cavallo dentro la città)

Indice

CAPITOLO II

IL TROJAN HORSE COME STRUMENTO D'INDAGINE

CAPITOLO III

INTERCETTAZIONI DI COMUNICAZIONI TRA PRESENTI CON IL CAPTATORE INFORMATICO

Introduzione

Con l'avvento dell'era digitale si è progressivamente assistito al mutamento della fisionomia delle forme di manifestazione dei reati che sempre più frequentemente vengono portati a compimento con l'ausilio dello strumento digitale[1].

Sebbene gli strumenti informatici possano inevitabilmente agevolare la commissione di determinati tipi di illeciti, anche gli organi investigativi possono, indubbiamente, disporre delle nuove tecnologie nella lotta alla repressione della criminalità.

In particolare negli ultimi anni si è affermato insistentemente nel panorama investigativo il captatore informatico, un *software* di tipo *trojan* che viene inoculato, occultamente, in un sistema informatico.

Così come il cavallo di Troia sconfisse i Troiani entrando nella città, fingendosi un dono pregiato da parte degli Achei, così anche il *virus trojan* riesce ad entrare nel dispositivo bersaglio, non per distruggerlo o danneggiarlo ma per apprendere qualsiasi dato che *ivi* possa trovarvi[2].

L'utilizzo del *trojan horse* in sede investigativa solleva problematiche di non poco conto perché se da un lato non si possono certamente negare i benefici e le potenzialità del captatore informatico per l'accertamento dei reati, dall'altro occorre sottolineare l'inevitabile frizione, determinata dall'uso di questo strumento, con i valori della libertà e segretezza delle comunicazioni, proclamati inviolabili dall'art. 15 Cost e con le 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),

Lo scopo di questa trattazione è quello di analizzare talune delle questioni inerenti all'impiego da parte degli organi inquirenti del virus *trojan* in un dispositivo elettronico portatile (*smartphone, tablet, personal computer*) per la realizzazione di intercettazioni di comunicazioni tra presenti.

---

[1] P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale, evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. e giust.*,2016, 5, p.2.

[2] M.GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, in *Dir. pen. cont.*,2018, 2, p.23.

Nell'ambito di tale ricerca verrà esaminata, in particolare, la disciplina delle intercettazioni di comunicazioni e saranno evidenziati, in un'esposizione ragionata, i numerosi profili di criticità concernenti l'uso del captatore informatico per la realizzazione di intercettazioni tra presenti, prendendo in considerazione le pronunce giurisprudenziali più rilevanti che si sono avvicendate sul tema e tutte le novità introdotte dal d.lgs. 216/2017, con il quale è stata attuata la delega contenuta nella legge n. 103/2017. Il decreto in questione oltre a regolamentare espressamente l'apprensione di colloqui tra presenti per mezzo del captatore informatico, introduce una nuova disciplina in materia d'intercettazioni preordinata a garantire la tutela della riservatezza delle persone coinvolte.

Il presente elaborato, inoltre, si propone di esaminare il dirompente impatto di questo poliedrico strumento investigativo nell'esecuzione delle indagini da parte dell'autorità giudiziaria e nel processo, evidenziando come il captatore informatico, oltre a consentire l'attivazione da remoto del microfono dispositivo bersaglio al fine di eseguire un'intercettazione, permette la realizzazione a distanza di perquisizioni *on line* e l'apprensione dei dati informatici contenuti nel sistema bersaglio mediante l'attivazione del virus in funzione *Keylogger, Screenshot* e *Screencast*.

Capitolo I

LA DISCIPLINA CODICISTICA DELLE INTERCETTAZIONI DI COMUNICAZIONI E LE NOVITÀ INTRODOTTE DAL D.LGS. 216/2017

SOMMARIO: 1. Libertà e segretezza delle comunicazioni nell'art.15 della Costituzione. – 1.1 La libertà e segretezza delle comunicazioni nella CEDU. – 2. La disciplina legislativa delle intercettazioni: le innovazioni introdotte dal d.lgs. n.216/2017. – 2.1 Nozione d'intercettazione di comunicazioni. – 2.2 Limiti ammissibilità intercettazioni. – 2.3 Il procedimento di autorizzazione all'esecuzione delle intercettazioni. – 2.4 Esecuzione delle operazioni d'intercettazione. – 2.5 Le attività successive alla captazione. – 2.5.1 La decisione del giudice e la conservazione della documentazione. – 2.6 Utilizzabilità dei risultati delle intercettazioni. – 2.7. Il Decreto legge, 30 Dicembre 2019, n. 161: "la riforma della riforma". – 2.7.1. L'udienza di stralcio. – 3. Intercettazioni informatiche e telematiche. – 4. Intercettazioni ambientali o *inter praesentes*. – 4.1 Intercettazioni ambientali domiciliari. – 4.1.1 La nozione di privata dimora – 5. Le videoriprese investigative.

1. Libertà e segretezza delle comunicazioni nell'art.15 della Costituzione

Con l'art 15 Cost., rubricato libertà e segretezza delle comunicazioni[3], il Costituente, accanto alla mera corrispondenza in senso stretto, ha inteso assumere ad oggetto di tutela anche "ogni altra forma di comunicazione".

[3] Si veda art. 616, comma 3, c.p.: «*per corrispondenza s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*».

La libertà e segretezza delle comunicazioni è annoverato tra i principi "supremi" il cui contenuto essenziale «*non può essere oggetto di revisione costituzionale, in quanto incorpora un valore della personalità avente un carattere fondante rispetto al sistema democratico voluto dal Costituente*»[4].

Si ritiene che debbano essere ricomprese nella garanzia disposta dall'art 15 Cost. tutte le comunicazioni del pensiero e della corrispondenza che presentano le caratteristiche dell'intersoggettività e dell'attualità. Il primo requisito è soddisfatto dalla circostanza che le comunicazioni vengano indirizzate ad uno o più destinatari individuati[5], mentre, per quanto riguarda il presupposto dell'attualità, quest'ultimo si sostanzia nella delimitazione temporale della comunicazione che inizia nel momento della trasmissione da parte del mittente e si esaurisce con la ricezione da parte del destinatario[6].

I titolari del diritto alla libertà e segretezza delle comunicazioni sono tutte le persone fisiche sia considerate individualmente che nelle formazioni sociali delle quali siano membri[7].

La comunicazione, per rientrare nell'ambito di applicazione dell'art.15 della Cost., dovrà essere libera e segreta.

Il requisito della "libertà" potrà dirsi soddisfatto se il rapporto comunicativo non subisce coercizioni indebite o restrizioni né da parte dello Stato né da parte di soggetti privati; il profilo della "segretezza" dell'atto comunicativo si sostanzia nell'*intentio* del mittente di trasmettere un pensiero nei confronti di un soggetto determinato, adottando una forma espressiva e un mezzo di comunicazione che siano convenzionalmente riconosciuti come segreti, impedendo così a terzi di conoscere il contenuto della conversazione[8] .

Proprio il carattere segreto del messaggio permette di delineare il confine tra l'art. 15 e l'art. 21 della Costituzione che, invece, tutela specificatamente la libertà di manifestazione del pensiero. Il diritto alla libertà e segretezza delle comunicazioni, sebbene discenda logicamente dall'opportunità di manifestare il proprio pensiero

---

[4] Corte cost., sent., 23 luglio 1991, n. 366, in www.giustcost.org.

[5] P. BARILE- E. CHELI, voce *Corrispondenza (libertà di*), in *Enc. dir*., vol. X, Milano, 1962, p. 745.

[6] F. MODUGNO, *Lineamenti di diritto pubblico*, Torino, 2010, p.579.

[7] P. BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria,* Milano, 2002, p.43.

[8] C. CARUSO, *La libertà e segretezza delle comunicazioni nell'ordinamento costituzionale,* 21 ottobre 2013, in www.forumcostituzionale.it, p.5.

liberamente, si differenzia da quest'ultima poiché proprio il carattere riservato della comunicazione determina l'impossibilità per lo Stato di sindacarne il contenuto sulla base del limite del buon costume, previsto dal secondo comma dell'art. 21 della Costituzione[9]. Bisogna, inoltre, rimarcare le differenze tra la libertà di comunicare segretamente ed un'altra situazione giuridica che rientra nell'ambito di applicazione dell'art.2 della Costituzione ossia il diritto alla privacy, inteso come il diritto di tenere segrete tutte le informazioni e i dati attinenti alla sfera più intima dell'individuo. Il tratto distintivo di questi due diritti è l'aspetto dinamico che connota la libertà e la segretezza delle comunicazioni il quale richiede necessariamente un messaggio che il mittente vuole far pervenire nella sfera conoscitiva del destinatario senza l'interferenza di soggetti terzi. Mentre l'art. 15 della Cost. è preordinato a evitare l'illegittima conoscenza del contenuto della comunicazione, la tutela della privacy è volta ad evitare l'abuso di dati attinenti all'intimità di un altro individuo. Di conseguenza, il diritto alla segretezza della comunicazione è leso quando una conversazione segreta sia illegittimamente conosciuta da un terzo; il diritto alla privacy, invece, subisce una limitazione quando uno degli interlocutori riveli a un terzo il contenuto di una comunicazione riservata[10].

Dopo aver proclamato l'inviolabilità della libertà e segretezza delle comunicazioni, al secondo comma l'art. 15 Cost. dispone che «*la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*». Sul punto la Corte costituzionale, a partire dalla sentenza n. 34/1973 [11], ha evidenziato che nella disposizione in esame trovano protezione due distinti interessi, ossia la libertà e la

[9] Ad esempio: se Tizio scrive una lettera aperta ad un giornale, dà al suo pensiero la maggior divulgazione possibile: in tal caso si ricade nell'art. 21 Cost.; se invece scrive una lettera in busta chiusa ad un parente, il suo pensiero è noto solo al destinatario: in tal caso si ricade nell'art. 15 Cost. cfr. R.BIN-G.PITRUZZELLA, *Diritto pubblico*,Torino,2011, p. 423.

[10] C. CARUSO, *op.cit.*, p.7.

[11] Corte cost. 6 aprile 1973, n.34, www.giustcost.org: «*L'eccezione di incostituzionalità in riferimento all'articolo 15 della Costituzione non è fondata. Questa norma non si limita a proclamare l'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (comma primo), ma enuncia anche espressamente che "la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge" (comma secondo). Nel precetto costituzionale trovano perciò protezione due distinti interessi; quello inerente alla libertà ed alla segretezza delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost., e quello connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale*».

segretezza delle comunicazioni, da un lato, e l'esigenza di prevenire e reprimere i reati, dall' altro.

Inoltre, i giudici hanno rilevato come l'inviolabilità della libertà e segretezza delle comunicazioni si configuri come limite operante sia rispetto alle intrusioni dei privati sia dei pubblici poteri[12].

L'art. 15 della Cost. per preservare dei valori costituzionali così importanti, richiede sia l'intervento della legge (c.d. riserva di legge) allo scopo di escludere l'intromissione in questa materia dell'Esecutivo con atti secondari, sia il provvedimento motivato dell'autorità giudiziaria (c.d. riserva di giurisdizione). Si è rilevata, quindi, la necessità di fornire al provvedimento limitativo un'adeguata motivazione che dovrà indicare le ragioni di fatto e di diritto poste a fondamento del provvedimento giurisdizionale, al fine di verificare la legittimità dell'operato del giudice e di azionare i rimedi previsti dall'ordinamento, così come previsto in via generale dall' art.111, commi 6 e 7, Cost. per i provvedimenti giurisdizionali [13].

Il sistema della doppia riserva di legge e di giurisdizione predisposto nell'art. 15 Cost. si differenzia, tuttavia, dalle garanzie prescritte dall'art.13 Cost. per la libertà personale e dall'art. 14 Cost. per il domicilio in quanto non prevede la possibilità di un intervento straordinario limitativo della libertà e segretezza delle comunicazioni in casi di necessità ed urgenza da parte dell'autorità di pubblica sicurezza.

La *ratio* giustificatrice di questa vistosa divergenza tra le disposizioni costituzionali si riconduce al fatto che le misure limitative delle comunicazioni sono sempre idonee a ledere i diritti del soggetto nei cui confronti vengono disposte e necessariamente anche quelli di un altro soggetto sia esso il destinatario del messaggio o l'interlocutore telefonico[14] .

[12] Corte cost., sent., 4 maggio 1972, n. 77, in www.giustcost.org.

[13]A.VELE, *Le intercettazioni nel sistema processuale penale: tra garanzie e prospettive di riforma*, Asiago,2011, p.11.

[14] S. ROMANO-C. SORIO, *L'utilizzo dei c.d. trojan horse nelle indagini penali e la tutela progressiva della libertà e segretezza delle comunicazioni*, in *Law and Media Working Paper Series*,2016, 14, p.4.

1.1 La libertà e segretezza delle comunicazioni nella CEDU

Il diritto alla libertà e segretezza delle comunicazioni assume una rilevanza fondamentale anche per il diritto internazionale pattizio.

L'art.8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali riconosce, infatti, ad ogni persona il diritto al rispetto della sua vita privata, familiare, del domicilio e della corrispondenza, escludendo che questo diritto possa subire delle indebite interferenze da parte della pubblica autorità non espressamente previste dalla legge e non necessarie per salvaguardare la sicurezza nazionale, la sicurezza pubblica, il benessere economico del paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute e dei diritti e delle libertà degli altri[15].

La Corte Edu nella sentenza relativa al caso *Zakharov* [16], ha affrontato la questione della compatibilità della normativa russa in materia di intercettazioni con l'art.8 della CEDU in quanto non rispettosa del canone della "*quality of law"*[17], che impone al legislatore nazionale di introdurre disposizioni in grado di consentire alla persona intercettata di prevedere le conseguenze dell'attività captativa sulla propria posizione giuridica.

La normativa censurata non conteneva, infatti, disposizioni concernenti le modalità autorizzative, la durata delle intercettazioni e le modalità di conservazione o distruzione del materiale intercettato, contravvenendo al dettato dell'art.8 della Cedu.

Riguardo sempre la compatibilità della normativa degli Stati aderenti alla CEDU in materia d'intercettazioni ed il principio della "*quality of law*" è importante segnalare un'altra pronuncia della Corte Edu relativa al caso c.d. "*Datagate*"[18].

Nel 2013 Edward Snowden, analista dell'Agenzia per la Sicurezza Nazionale statunitense (NSA) ha rilevato che il governo USA stava usando programmi di sorveglianza di massa che consentono di accedere a conversazioni personali su *Facebook, Google, Skype* e altre piattaforme. Dalle sue dichiarazioni è emerso che anche l'agenzia GCHQ (*Government Communication Headquarters*) di Londra stava impiegando programmi simili che consentivano di accedere alle comunicazioni quotidiane di milioni di utenti.

---

[15] Corte Edu, sent.,2 settembre 2010, Uzun c. Germania.

[16] Corte Edu, sent., 4 dicembre del 2015, Zakharov c. Russia.

[17] Corte Edu, sent., 2 agosto 1984, Malone c. Regno Unito.

[18] Corte Edu, sent., 13 settembre 2018, Big Brother e altri c. Regno Unito.

La Corte Edu censura la normativa inglese in tema di "*mass surveillance"* per incompatibilità con quanto disposto dall'art. 8 CEDU, in quanto, in contrasto il canone della "*quality of law*", non prevedeva alcuna supervisione da parte di un'autorità indipendente in merito all'utilizzo dei filtri e dei criteri di selezione delle comunicazioni da intercettare. I metodi di raccolta dati e l'individuazione delle persone sottoposte a questa forma di monitoraggio, infatti, non venivano specificati in maniera sufficiente e mancava, inoltre, una normativa adeguata che disciplinasse compiutamente il filtraggio, la selezione e la ricerca delle comunicazioni captate.

Alla luce di queste pronunce è evidente come il principio di legalità, secondo la Corte Edu, abbia un contenuto rafforzato perché impone al legislatore nazionale di determinare in maniera prevedibile la durata delle operazioni di intercettazione, le autorità deputate all'autorizzazione, l'esecuzione, il controllo dell'attività captativa, le vie di ricorso che possono essere esperite dai singoli e le modalità di conservazione e utilizzazione dei dati così raccolti[19] .

[19] S. ROMANO-C. SORIO, *op.cit.* p.13-15.

2. La disciplina legislativa delle intercettazioni: le innovazioni introdotte dal d.lgs. n.216/2017

Le intercettazioni sono, tra tutti gli strumenti di ricerca della prova, quelle che determinano maggiormente un'inevitabile compressione del diritto alla libertà e segretezza delle comunicazioni.

La disciplina di cui gli artt. 266 e ss. del c.p.p., conformemente al dettato costituzionale, è preordinata ad evitare che i valori protetti dall'art.15 della Cost. vengano ingiustamente sacrificati per soddisfare l'esigenza di repressione dei reati.

Le intercettazioni hanno assunto un ruolo preminente nelle investigazioni degli organi inquirenti: dalle statistiche ufficiali del Ministero della Giustizia, infatti, risulta che solo nell'anno 2016 sono stati ben 265.173 i soggetti intercettati dalle Procure ordinarie, 113.333 dalle Direzioni Distrettuali Antimafia, 8.102 dalle sezioni addette al contrasto al terrorismo, 2.872 dalle Procure generali presso le Corti di Appello e 528 dalle Procure presso i Tribunali per i minorenni [20]. Da questi dati emerge in maniera evidente l'utilità delle intercettazioni ai fini dell'accertamento del reato. Tuttavia non si può prescindere dalla considerazione che la disciplina contenuta nel testo originario del codice non tiene conto del progresso tecnologico e dello sviluppo di tecniche sempre più all'avanguardia per l'esecuzione delle operazioni captative che non erano nemmeno immaginabili nel 1988-1989 all'epoca dell'entrata in vigore dello stesso.

Oltre alle "sfide nuove" che deve affrontare il legislatore, derivanti dallo sviluppo tecnologico, bisogna considerare che le intercettazioni, determinando la compressione di beni di primissimo rango costituzionale, coinvolgono molteplici interessi e spesso contrastanti tra loro. Si pensi, ad esempio, all'interesse ad un efficace svolgimento delle indagini e allo stesso tempo al diritto di difesa, laddove il difensore, per svolgere in maniera consapevole il proprio mandato deve aver accesso alle comunicazioni intercettate al fine di vagliarne la rilevanza o, anche, al diritto dei cittadini alla conoscenza delle indagini[21].

---

[20] Questi dati sono ricavati dal sito www.webstat.giustizia.it, cfr. V. GIGLIO, *Manuale delle intercettazioni: il nuovo regime normativo, i principi e la giurisprudenza*, Bologna, 2018, p. 9.

[21] Sul tema si veda Convegno "*Le Intercettazioni: problemi antichi e sfide nuove"*, Roma 6 Luglio2017, I sessione Le direttive del d.l. n. 4368, Introduzione G. ILLUMINATI, in *Jusonline*, 2017, 3, p.330.

Il legislatore con la riforma del regime delle intercettazioni introdotta con la legge 103/2017 e affidata al Governo per l'attuazione della disciplina di dettaglio con il d.lgs. n. 216/2017, ha focalizzato l'attenzione sui profili critici della previgente disciplina delle intercettazioni.

Questa riforma mira a garantire, sempre nel rispetto delle esigenze investigative, la riservatezza delle conversazioni intercettate con riguardo delle persone occasionalmente coinvolte nell'attività captativa, sanzionando penalmente la diffusione di riprese audiovisive o registrazioni audio effettuate con frode. Ulteriore obiettivo è quello di rendere più agevoli le intercettazioni nei procedimenti per gravi reati dei pubblici ufficiali contro la pubblica amministrazione[22].

Il d.lgs. n.216/2017 provvede, inoltre, a regolamentare l'uso del captatore informatico, disciplinando, però, soltanto uno dei possibili risvolti applicativi del *trojan horse* per l'esecuzione delle indagini: l'attivazione da remoto del microfono del dispositivo bersaglio per l'esecuzione d'intercettazioni "tra presenti" limitatamente alla circostanza in cui il virus venga inoculato su dispositivi elettronici portatili[23]. Pertanto, in base all'art. 266, comma 2-*bis*, c.p.p., introdotto dall'art. 4 del d.lgs. n.216/2017, l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico «*è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, c.p.p.*»[24].

La scelta del legislatore dipende dal fatto che il captatore informatico, permettendo l'esecuzione d'intercettazioni ubiquitarie, ha determinato l'insorgere, nella prassi, di numerosi interrogativi concernenti la compatibilità dello strumento investigativo in esame con la disciplina delle intercettazioni di comunicazioni tra presenti che contempla

[22] Cfr. artt. 82,83,84, lett. *a), b), c), d*) ed *e)* l.103/2017.

[23] Sul tema della disciplina introdotta dal d.lgs. n.216/2017 sul captatore informatico cfr. *infra* Cap.3 § 3.

[24] Il comma 2-*bis* dell'art. 266 c.p.p. ha subito due interventi di modifica. Il primo con l'art. 1, comma 3 e 4, lett.*a)* e *b)*, l. 3/2019 (c.d. legge "spazza-corrotti" o "anticorruzione") che, modificando l'assetto normativo delineato dagli artt. 266, comma 2-*bis*, e 267, comma 1, c.p.p., estende il campo applicativo della disciplina sulle intercettazioni eseguite mediante inserimento del virus *trojan horse* anche ai reati dei pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p. Il secondo con l'art. 2, comma 1, lett. *c)* del d.l. 161/2019 che ha disposto l'impiego del captatore informatico per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'art. 4 c.p.p. Sul tema cfr. *infra* Cap.3 § 3.2 e § 3.2.1.

il dovere di indicazione specifica nel decreto autorizzativo dei luoghi in cui avvengono le operazioni.

È importante segnalare che, ad eccezione di alcune disposizioni dotate di efficacia immediata [25], l'entrata in vigore del decreto in questione, prevista inizialmente per il 26 luglio 2018, è stata oggetto di numerose proroghe[26].

Il 31 Dicembre 2019, giorno in cui la Riforma "Orlando" sarebbe dovuta entrare in vigore, il Consiglio dei Ministri con il decreto legge del 30 dicembre 2019, n. 161, recante "*Disposizioni urgenti in materia di intercettazioni*", ha modificato la disciplina contenuta nel d.lgs. 216/2017.

Prima di procedere ad una compiuta analisi delle intercettazioni di comunicazioni "tra presenti" realizzate per mezzo del captatore informatico, si rende necessario analizzare le norme in materia d'intercettazioni di comunicazioni di cui gli artt. 266 e ss. del c.p.p., così come modificati dal d.lgs. 216/2017 e, da ultimo, dal d.l. 161/2019.

2.1 Nozione d'intercettazione di comunicazioni

L'intercettazione di comunicazioni, regolata espressamente dal capo IV del titolo III del c.p.p., è catalogata tra i mezzi di ricerca della prova ed è compiutamente disciplinata dagli artt. 266 e ss. c.p.p.

La Corte costituzionale nella sent.81 del 1993[27] ha definito le intercettazioni come «*quelle tecniche che consentono di apprendere, nel momento stesso in cui viene espresso, il contenuto di una conversazione o di una comunicazione, contenuto che, per le modalità con le quali si svolge, sarebbe altrimenti inaccessibile a quanti non siano parte della comunicazione medesima*».

Un'esaustiva definizione di intercettazione è stata però delineata dalla Corte di Cassazione nella sentenza Torcasio[28] che ha fatto riferimento alla captazione occulta e

[25] Cfr. art. 6, d.lgs. 216/2017

[26] L'art. 2 del d.l. 25 luglio 2018, n. 91 aveva posticipato l'applicazione della normativa introdotta dal d.lgs. 217/2017 al 31 marzo 2019, prorogata al 31 luglio 2019 dall'art. 11 della Legge Bilancio 2019 e poi rinviata al 31 Dicembre 2019 dall'art. 9, comma 2, d.l. 14 Giugno 2019, n. 53.

[27] Corte cost. sent., 26 ottobre 1993, n.81, in www.giustcost.org

[28] Cass.,sez.un.,24 settembre 2003, n.36747, Torcasio, in *C.e.d. Cass*., Rv. 225465.

contestuale di una comunicazione o conversazione tra due soggetti che agiscono con l'intenzione e con modalità da escludere altri. Inoltre, in questa decisione, la Corte specifica che l'attività captativa deve essere realizzata da un soggetto terzo, estraneo alla comunicazione, con strumenti tecnici di percezione tali da vanificare le cautele ordinariamente attuate dagli interlocutori per conservare il carattere riservato della conversazione[29].

Da questa definizione si evince che i tratti peculiari del mezzo di ricerca della prova in esame sono: la segretezza, l'utilizzo di particolari strumenti di percezione e la terzietà del captante.

Per ciò che concerne il requisito della segretezza, si richiede che i soggetti comunichino tra loro con l'intento di escludere estranei dal contenuto della conversazione.

Infatti si ritiene che non costituisca intercettazione un'espressione del pensiero, anche rivolta ad un soggetto determinato, che venga effettuata in modo da renderla percepibile a terze persone, come ad esempio parlare ad alta voce in pubblico [30].

Per quanto riguarda, invece, l'utilizzo di particolari strumenti di percezione idonei a violare la riservatezza del colloquio tra gli interlocutori, colui che capta utilizza strumenti tecnici di percezione invasivi, utili a superare le elementari cautele che garantiscono la libertà e segretezza del colloquio[31].

L'utilizzo di dispositivi elettronici per la captazione, tra i requisiti delle intercettazioni, è quello che maggiormente caratterizza questo mezzo di ricerca della prova in quanto senza il ricorso a strumenti così sofisticati, potrà aversi soltanto una forma di interferenza in una conversazione privata[32].

Per ciò che concerne, poi, la terzietà e la clandestinità, colui che capta deve essere estraneo al colloquio e operare in modo clandestino.

Da ciò ne consegue che la registrazione fonografica di un colloquio da parte di un soggetto che è attivamente partecipe di quella conversazione o comunque ad opera di una persona che è ammessa ad assistervi non è riconducibile alla nozione di intercettazione in quanto

---

[29] *Ibidem.*

[30] C.DI MARTINO-T.PROCACCIANTINI, *Le intercettazioni telefoniche*, Padova, 2001, p.17.

[31] P.TONINI, *Manuale di procedura penale*, Milano, 2017, p. 395.

[32]Ad esempio, ascoltare una conversazione origliando alla porta di uno degli interlocutori. Cfr. G.ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano,1983, p.41.

difetta del requisito della clandestinità. Tutt'al più, in una simile circostanza, si potrà parlare di una memorizzazione fonica di un fatto storico della quale l'autore può disporre legittimamente come prova nel processo a norma dell'art. 234 c.p.p, salvo che non vi osti un divieto probatorio[33] .

Tuttavia, alcuni Autori sostengono che la conoscenza delle attività captative da parte di uno degli interlocutori non escluda l'intercettazione[34]. In base a questo orientamento la segretezza è un diritto positivo perfetto che appartiene ad entrambi i partecipanti alla conversazione e, conseguentemente, se si riconoscesse al consenso di uno solo degli interlocutori il potere di rendere superfluo il decreto del giudice o del pubblico ministero che dispone l'intercettazione, si attribuirebbe al singolo partecipante alla conversazione il potere di interferire unilateralmente nella sfera giuridica altrui. Una situazione di questo tipo sembrerebbe configurare un diritto potestativo in assenza, però, di una disposizione di legge che lo disponga espressamente. A sostegno di questa opinione sussiste una precisa argomentazione testuale, ricavabile dall'art. 266, lett. f), c.p.p. laddove consente le intercettazioni nel caso si realizzi il reato di molestie o disturbo delle persone tramite il telefono ed è evidente che, in una simile circostanza, è possibile l'esecuzione di un'intercettazione con il consenso della persona offesa che sarà a conoscenza di essere ascoltata[35].

L'intercettazione, dunque, è un'attività che può avere ad oggetto sia «*conversazioni o comunicazioni telefoniche e altre forme di telecomunicazione*» (come prevede l'art 266 c.p.p.) sia «*il flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi*» (*ex* art 266-*bis*) [36]. Inoltre, il codice, in presenza degli stessi requisiti, ammette le intercettazioni di comunicazioni tra presenti o ambientali *ex* art. 266, comma 2, c.p.p.[37]. Con questa espressione s'intende la circostanza in cui due o più

[33]E.APRILE-F.SPEZIA, *Le intercettazioni telefoniche ed ambientali, innovazioni tecnologiche e questioni giuridiche,* Milano, 2004, p.2.

[34]Si veda A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p.21; allo stesso modo C.DI MARTINO-T.PROCACCIANTINI, *op.cit.*, p.21 e P.BARILE-E.CHELI, *op.cit.*,p.751.

[35] A. CAMON, *op. cit*., p. 20-21.

[36] Si veda *infra* § 3.

[37] Si veda *infra* § 4.

individui si scambiano comunicazioni mentre si trovano nello stesso luogo senza dover ricorrere a strumenti di trasmissione a distanza.

Questa tipologia d'intercettazione di regola si realizza al di fuori del privato domicilio ma può eccezionalmente essere eseguita nei luoghi di privata dimora *ex* art.614 c.p se sussiste il fondato motivo di ritenere che in questi luoghi «*si stia svolgendo l'attività criminosa*»[38]. Diversamente dagli altri mezzi di ricerca della prova (ispezioni, perquisizioni sequestri), l'intercettazione si qualifica non per il suo carattere *"*coattivo*"*, ma per le sue modalità "insidiose". Come la perquisizione, è un atto "a sorpresa" ma ne differisce perché "occulto", infatti mentre la perquisizione ammette un contestuale controllo sullo svolgimento delle operazioni, mediante eventuale assistenza o rappresentanza da parte di persona di fiducia, l'intercettazione invece si svolge ad insaputa dei dialoganti[39].

2.2 Limiti di ammissibilità delle intercettazioni

Nel rispetto della riserva di giurisdizione di cui all'art. 15 della Cost., l'art. 267 c.p.p. statuisce che il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione per l'esecuzione delle intercettazioni.

Le intercettazioni possono essere disposte esclusivamente nei procedimenti relativi ai reati previsti dall'art. 266 comma 1 c.p.p.[40], rubricato, infatti, "condizioni di ammissibilità". Questa disposizione, per indicare i reati rispetto ai quali è possibile

---

[38] Si veda *infra* § 4.1.

[39] P.BALDUCCI, *op.cit* , p.1.

[40] Si veda art. 266 comma 1 c.p.p.: «*L'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione è consentita nei procedimenti relativi ai seguenti reati:*
a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'articolo 4;
b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma articolo 4;
c) delitti concernenti sostanze stupefacenti o psicotrope;
d) delitti concernenti le armi e le sostanze esplosive;
e) delitti di contrabbando;
f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, molestia o disturbo alle persone col mezzo del telefono.
f bis) delitti previsti dall' articolo 600 ter, terzo comma, del codice penale, anche se relativi al materiale pornografico di cui all'articolo 600 quater.1 del medesimo codice, nonché dall'art. 609-undecies.
f-ter) delitti previsti dagli articoli 444, 473, 474, 515, 516 e 517-quater del codice penale.
f-quater) delitto previsto dall'articolo 612-bis del codice penale».

procedere alle attività captative, ricorre sia ad un criterio quantitativo, basato sull'entità della pena edittale, sia a un criterio qualitativo riferito a quei reati per il cui accertamento le intercettazioni si rivelano uno strumento di grandissima utilità (come ad esempio le molestie a mezzo del telefono) [41].

Nel caso in cui l'intercettazione venga eseguita al di fuori dei casi previsti dall'art 266, comma 1, c.p.p. i risultati probatori così ottenuti saranno inutilizzabili a norma dell'art. 271 c.p.p[42].

Bisogna, inoltre, evidenziare che esistono ulteriori limitazioni all'esecuzione delle intercettazioni *ratione personae* perché sussistono determinati soggetti nei confronti dei quali, in virtù della funzione esercitata, si ravvisa un divieto di disporre il controllo realizzato per mezzo delle intercettazioni.

Si pensi ai deputati e ai senatori (art. 68, commi 2 e 3, Cost.), salvo il caso in cui la Camera di appartenenza autorizzi le operazioni d'intercettazione. Le intercettazioni, inoltre, non possono essere disposte nei confronti dei parlamentari europei (art. 10, comma 1 lett.a del Protocollo sui privilegi e sulle immunità delle Comunità Europee, ratificato con l. n. 437 del 3 Maggio 1996), dei soggetti rispetto ai quali è necessaria l'autorizzazione a procedere *ex* art. 343 c.p.p., del Presidente del Consiglio dei Ministri (art. 10, comma 1, l.cost. n. 1 del 16 Gennaio 1989), dei Giudici Costituzionali (art. 3 comma 2 l. n. 1 del 9 Febbraio 1948) e del Presidente della Repubblica (art. 7 comma 3, l. n. 219 del 5 Giugno 1989).

Infine, l'art. 103, comma 5, c.p.p. vieta le intercettazioni delle comunicazioni o conversazioni dei difensori, degli investigatori privati autorizzati e incaricati in relazione al procedimento, dei consulenti tecnici e loro ausiliari.

[41] P.TONINI-C.CONTI, *Il diritto delle prove penali*, I ed., Milano, 2012, p.395.

[42] Si veda *infra* § 2.6.

2.3 Il procedimento di autorizzazione all'esecuzione delle intercettazioni

Il giudice per le indagini preliminari autorizzerà le operazioni captative con decreto motivato solo quando reputerà sussistenti «*gravi indizi di reato*» e riterrà l'intercettazione «*assolutamente indispensabile ai fini della prosecuzione delle indagini*» ai sensi dell'art.267, comma 1, c.p.p.

Il termine indizio di cui l'art. 267 c.p.p. assume un significato diverso da quello cui fa riferimento l'art. 192, comma 2, c.p.p. in quanto in quella sede vengono indicati i criteri per la valutazione della prova logica indiziaria sufficiente per affermare la responsabilità dell'imputato, mentre l'art. 267 c.p.p. richiede la sussistenza di elementi che facciano presumere la commissione di un reato ricompreso nell'elenco tassativo di cui gli artt. 266 e 266 *bis* c.p.p [43]. Da ciò consegue che indizi di reato necessari per disporre l'intercettazione, oltre ad essere gravi, non devono anche essere precisi e concordanti, come esige l'art. 192 c.p.p. ai fini del giudizio, perché, in questo modo, si avrebbe il paradosso di richiedere per l'espletamento dell'intercettazione un livello probatorio pari a quello chiesto per la pronuncia di una sentenza di condanna. Si tratta, infatti, di due provvedimenti diversi, da un lato una sentenza e dall'altro un atto investigativo e sarebbe, quindi, ingiustificato richiedere «*la stessa severità per la valutazione del materiale latu sensu probatorio*»[44].Tanto è vero che la Suprema Corte, in una recente pronuncia, ha affermato che « *la motivazione del decreto di autorizzazione delle intercettazioni non deve esprimere una valutazione sulla fondatezza dell'accusa, ma solo un vaglio sull'effettiva serietà del progetto investigativo*»[45]. Per contro sebbene la locuzione "gravi indizi di reato" non si riferisca all'assoluta certezza sull'esistenza del reato non sembrerebbe neppure corretto farla coincidere con la locuzione "serietà del progetto investigativo" che si connota per la sua estrema vaghezza[46].

---

[43] P. BALDUCCI, *op.cit*., p.108.

[44] A.CAMON, *op.cit.*, p.71.

[45] Cass. pen., sez.III, 2 dicembre 2014, n.14954, in *C.e.d. Cass*., Rv. 263045.

[46] V. GIGLIO, *op. cit.*, p.73.

È necessario, inoltre, segnalare la distinzione finalistica tra i gravi indizi di reato e i gravi indizi di colpevolezza cui fa riferimento l'art. 273 c.p.p., quale presupposto per l'applicazione di misure cautelari personali.

I gravi indizi di colpevolezza, infatti, si sostanziano in tutti quegli elementi di natura logica o rappresentativa che non valgono, di per sé, a provare oltre ogni ragionevole dubbio la responsabilità dell'indagato ma, costituendo una qualificata probabilità di colpevolezza, attraverso l'acquisizione di ulteriori elementi saranno idonei a dimostrare tale responsabilità[47]. Mentre i gravi indizi di reato di cui l'art. 267 c.p.p. riguardano gli elementi di prova sufficienti da soli ad affermare la sussistenza di un reato rispetto al quale possono essere legittimatamene disposte le intercettazioni, senza che tali elementi convergano necessariamente verso un soggetto determinato qualificandolo come probabile autore del reato che può essere anche ignoto nel momento in cui vengono disposte le intercettazioni[48].

Per quanto concerne la valutazione dei gravi indizi di reato l'art. 267, comma 1 *bis*, c.p.p. prevede l'applicazione dell'art. 203 c.p.p. e, conseguentemente, le dichiarazioni confidenziali[49] degli informatori della polizia giudiziaria potranno essere poste a fondamento degli indizi soltanto nella circostanza in cui gli informatori cessino di essere anonimi e vengano esaminati come testimoni o come persone informate sui fatti. In questo modo il legislatore del 2001 ha posto fine ad un indirizzo giurisprudenziale che ammetteva l'esecuzione delle operazioni d'intercettazione anche sulla base di una notizia confidenziale contenuta nell'informativa trasmessa al pubblico ministero [50].

Il primo presupposto dei gravi indizi di reato che legittima il ricorso alle operazioni captative, è propedeutico al secondo requisito richiesto dall'art.267 c.p.p. che consiste nell'assoluta indispensabilità ai fini della prosecuzione delle indagini.

---

[47] Cass. pen., sez. un., 1 agosto 1995, n.11, Costantino ed altro, in *C.e.d. Cass*., Rv. 202002.

[48] Cass. pen., sez. VI, 18 Giugno 1999, n. 9428, Patricelli, in *C.e.d. Cass*., Rv. 214127.

[49] Per qualificare una fonte come confidenziali si veda Cass. pen., sez. VI,18 settembre 2017, n. 42566, in *Guida al diritto*, 2017, 41, 96 : la Corte in questa e pronuncia ha indicato la sussistenza di due requisiti per poter considerare una fonte confidenziale, il primo è rappresentato dal carattere della segretezza derivante dall'intento del dichiarante di rimanere anonimo per ragioni di opportunità e sicurezza, invece il secondo requisito è rappresentato dal rapporto fiduciario tra chi confida la notizia e chi la riceve.

[50] E.APRILE-F.SPEZIA, *op.cit*, p.9.

In una visione ispirata dal principio della inviolabilità e segretezza delle comunicazioni il ricorso alle intercettazioni dovrebbe sempre rappresentare *l'extrema ratio* e il giudizio sulla sussistenza della indispensabilità dovrebbe essere espresso *ex ante* sulla base del quadro probatorio disponibile al momento dell'emanazione del decreto.

Si sottolinea come il secondo presupposto abbia la funzione essenziale di collocare temporalmente in una fase avanzata le operazioni d'intercettazione precludendone l'uso quale atto iniziale delle indagini in quanto la locuzione *"*prosecuzione delle indagini*"* le presuppone già iniziate[51].

Quindi, ciò significa che il giudice, nel procedimento "ordinario", sulla base degli atti che gli vengono trasmessi dal pubblico ministero, valuta la sussistenza dei suddetti presupposti indefettibili per l'esecuzione delle operazioni captative e concede l'autorizzazione con decreto motivato. Conseguentemente il pubblico ministero, a norma dell'art.267, comma 3, c.p.p., dispone l'intercettazione mediante decreto con cui determina le modalità e il termine di durata delle operazioni che per i procedimenti di criminalità ordinaria è fissato in quindici giorni [52].

La Corte di cassazione ha riconosciuto al pubblico ministero la facoltà di sospendere per ragioni inerenti alle indagini il termine di durata delle operazioni captative per poi farlo riprendere quando le esigenze che ne hanno comportato la sospensione vengano meno, senza che sia necessaria un'autorizzazione ad hoc da parte del giudice delle indagini preliminari[53].

Il termine di quindici giorni previsto per le operazioni può essere prorogato dal giudice per le indagini preliminari per periodi successivi sempre di quindici giorni purché permangano i presupposti che hanno determinato l'autorizzazione all'esecuzione delle intercettazioni[54].

Dal dettato dell'art. 267, comma 3, c.p.p. emerge come, sebbene spetti al pubblico ministero la valutazione in ordine alla durata delle operazioni d'intercettazione, il legislatore nel caso di proroga ha devoluto al giudice «*la valutazione sulla necessità di*

[51] L'intercettazione, quindi, non può essere utilizzata come strumento per l'acquisizione della notizia di reato. Cfr. P. BALDUCCI., *op. cit.* p. 115.

[52] A.CAMON, *op.cit*., p.138.

[53] Cass.pen.sez. VI, 23 marzo 2011, n.11682, in in *C.e.d. Cass*., Rv. 249724.

[54] G. CONSO-V. GREVI-M. BARGIS, *Compendio di procedura penale, VII ed*., Padova, 2014, p.391.

comprimere oltre il termine ordinario, la sfera di riservatezza delle comunicazioni private»[55].

La regola che attribuisce la determinazione della durata dell'attività captativa al pubblico ministero discende logicamente dalla circostanza che le intercettazioni sono un atto investigativo ed è il pubblico ministero il soggetto responsabile delle operazioni istruttorie.

Qualora il giudice emetta un decreto autorizzativo nel quale dispone una durata delle operazioni d'intercettazione superiore a quella indicata dal pubblico ministero nella sua richiesta, si determina una violazione dell'art 267 con la conseguente inutilizzabilità dei risultati ottenuti dall'attività d'intercettazione[56].

La Suprema Corte non ha, però, avallato questo orientamento ed in una recente pronuncia[57] ha sostenuto che il decreto di autorizzazione del giudice non è vincolato dalla richiesta del pubblico ministero. Nel caso di specie il pubblico ministero aveva richiesto le intercettazioni per una durata di quindici giorni per uno dei reati di cui all'elenco dell'art. 266 c.p.p. e il giudice per le indagini preliminari aveva concesso l'autorizzazione per un periodo di quaranta giorni, riferendosi ad una diversa ipotesi di reato che rientra nell'ambito di applicazione dell'art. 13 della legge 203/1991. Il giudice ha, quindi, riqualificato la richiesta del pubblico ministero in presenza dei sufficienti indizi previsti per la disposizione delle attività captative nei delitti di criminalità organizzata[58].

L'art. 267,comma 2, c.p.p. attribuisce in via eccezionale al *dominus* delle indagini il potere di attivare un procedimento di autorizzazione nei casi di urgenza; si tratta di una procedura *ex abrupto* che consente al pubblico ministero, quando sussiste un fondato motivo che dal ritardo possa derivare un grave pregiudizio per le indagini, di disporre l'intercettazione con decreto motivato che va comunicato "immediatamente" o comunque "non oltre le ventiquattro ore" al giudice per le indagini preliminari. Il legislatore ha,

---

[55] E.APRILE-F.SPEZIA, *op.cit*,p.48.

[56] V. GIGLIO, *op. cit.*, p.70.

[57] Si veda in tal senso Cass. pen. sez.VI, 21 Luglio 2015, n.34809, in *C.e.d. Cass*., Rv. 264447: «*Il Tribunale reggino, dinanzi al quale essa era stata già sollevata, l'ha correttamente ritenuta infondata, richiamando la giurisprudenza di questa Corte di Cassazione - che deve essere ribadita in questa sede - sul potere del GIP di riqualificare la richiesta del PM in presenza di sufficienti indizi di delitti di criminalità organizzata, sebbene essa faccia esclusivo riferimento alla disciplina dettata dagli artt. 266 e segg. cod. proc. pen*.».

[58] *Ibidem.*

quindi, sottoposto il decreto d'urgenza ad una procedura di convalida che prevede un controllo giurisdizionale successivo. Il giudice entro le quarantotto ore dal provvedimento decide sulla convalida con decreto motivato e, nel caso di diniego, le intercettazioni non potranno proseguire ed i relativi risultati saranno inutilizzabili[59].

Conclusivamente a norma dell'art. 267, comma 5, c.p.p. è prevista l'istituzione presso l'ufficio del pubblico ministero di un registro riservato nel quale vengono riportati in ordine cronologico sia i decreti che regolano le intercettazioni con l'indicazione dell'inizio e del termine delle operazioni captative sia i provvedimenti del giudice che le autorizzano, convalidano e prorogano. Questa norma è preordinata a garantire una documentazione completa dei provvedimenti giurisdizionali in tema d'intercettazioni e conseguentemente le annotazioni devono essere tempestive e aggiornate costantemente[60].

Nel caso di irregolare indicazione di inizio e fine delle operazioni nel registro di cui l'art. 267, comma 5, c.p.p. non si determina l'inutilizzabilità dei risultati dell'attività captativa[61]e allo stesso modo non opera l'inutilizzabilità anche nel caso di mancata indicazione nei verbali dei nominativi degli ufficiali di polizia giudiziaria che hanno preso parte alle operazioni d'intercettazione[62].

[59] P. BALDUCCI., *op. cit.* p. 143.

[60] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 116.

[61] Cass.Pen., Sez. VI, 28 luglio 2015, n.33231, in *C.e.d. Cass*., Rv. 264462.

[62] Cass.Pen., Sez. III, 17 Febbraio 2015, n.20418, in *C.e.d. Cass*., Rv.263625.

2.4 Esecuzione delle operazioni d'intercettazione

Il pubblico ministero o l'ufficiale di polizia giudiziaria, sulla base di una specifica delega, secondo quanto disposto dall'art.267, comma 4, c.p.p., provvedono all'esecuzione materiale delle intercettazioni.

È la polizia giudiziaria a occuparsi della realizzazione delle operazioni captative tanto è vero che il disposto dell'art. 268, comma 4, c.p.p. prevede l'immediata trasmissione dei verbali e le registrazioni al pubblico ministero[63].

L'art.268, comma 1, c.p.p. dispone che «*Le comunicazioni intercettate sono registrate e delle operazioni è redatto verbale*».

Il verbale, il cui contenuto è regolato dall'art. 89 disp. att. c.p.p., deve essere connotato da analiticità e deve necessariamente indicare gli estremi del decreto che ha disposto l'intercettazione, la data delle operazioni, specificando l'ora d'inizio e di cessazione di ogni singola attività captativa e le modalità di registrazione[64]. In riferimento a quest'ultimo elemento del verbale dovranno essere indicati gli eventuali inconvenienti tecnici come pause, sovrapposizioni e smagnetizzazioni. Si tratta di problematiche che si verificano in maniera molto frequente durante l'esecuzione delle attività captative e proprio da questa considerazione discende la necessità di una redazione contestuale del verbale e contemporanea all'ascolto delle conversazioni intercettate[65].

A tal proposito l'art. 373, comma 4, c.p.p. dispone che la documentazione degli atti d'indagine deve necessariamente realizzarsi nel corso del loro compimento ovvero immediatamente dopo quando ricorrono insuperabili circostanze[66].

L'omissione del verbale, in ragione del rinvio dell'art.271 c.p.p. al primo comma dell'art.268 c.p.p., determina un divieto d'uso dello stesso rispetto al quale opera il regime di rilevabilità di cui l'art. 191, comma 2, c.p.p.[67].

Secondo quanto disposto dall'art.268, comma 2, c.p.p. nel verbale la polizia giudiziaria trascrive, anche sommariamente, il contenuto delle conversazioni intercettate.

---

[63] L.FILIPPI, *L'intercettazione di comunicazioni*, 1997, Milano, p.121.

[64] A.CAMON, *op.cit.*, p.163-164.

[65] *Ibidem.*

[66] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p.127.

[67] A.CAMON, *op.cit.*, p.167.

Si tratta dei cd. "brogliacci d'ascolto" che rivestono una funzione essenziale già nel corso delle indagini preliminari per chiedere al giudice l'applicazione di misure cautelari. Nel corso della fase di trascrizione sommaria sussiste un alto rischio di errori e fraintendimenti che potrebbero modificare completamente il senso delle conversazioni captate, andando così ad inficiare il valore probatorio dell'intercettazione stessa[68].

Il legislatore delegato con d.lgs. n. 216/2017 è intervenuto in maniera incisiva sulla fase esecutiva delle operazioni d'intercettazioni apportando delle modifiche significative all'art. 268 c.p.p.

Uno degli obiettivi perseguiti dalla delega parlamentare era quello di aumentare il grado di tutela della riservatezza dei soggetti sottoposti alle intercettazioni soprattutto nei confronti di chi è occasionalmente coinvolto nell'attività captativa ed estraneo alle indagini.

All'uopo è stato introdotto il comma 2 *bis* all'art. 268 c.p.p. che dispone il divieto di trascrivere anche sommariamente tre categorie di comunicazioni o conversazioni: quelle irrilevanti ai fini della prosecuzione delle indagini sia per l'oggetto che per i soggetti coinvolti, quelle concernenti i dati personali sensibili *ex* art 4, comma 1, lett *d)* d.lgs. 196 /2003 ed infine quelle relative alle conversazioni, anche indirette, con i difensori ai sensi dell'art. 103 ,comma 7, c.p.p[69].

I maggiori elementi di criticità nel nuovo comma 2 *bis* si riscontrano principalmente nell'individuazione di conversazioni irrilevanti in relazione ai "soggetti coinvolti", in quanto, nonostante sia indiscusso il fatto che uno degli obbiettivi della legge delega è quello di tutelare la riservatezza delle persone occasionalmente coinvolte nel procedimento, applicare pedissequamente e in maniera rigorosa questo principio porterebbe all' impossibilità di trascrivere un colloquio contenente elementi utili per le indagini solo perché si è realizzato tra soggetti estranei al procedimento. Per questo

[68] P.TONINI-C.CONTI, *op.cit*., p. 400.

[69]La modifica apportata dall'art. 2, co. 1, lett. a), d.lgs. n. 216 del 2017 al co. 7 dell'art. 103 c.p.p., mantenendo immutata la sanzione dell'inutilizzabilità dei risultati dell'intercettazione che concerne il procedimento tra l'avvocato e i suoi ausiliari nonché tra questi soggetti e l'assistito, dispone ora il divieto di trascrizione, anche solo sommario, qualora l'intercettazione sia stata ugualmente effettuata. Sul tema cfr. F.GIUNCHEDI, *Appunti su alcune criticità sulla nuova disciplina delle intercettazioni,* in *Archivio Penale, Speciale Riforme,* 2018.

motivo si ritiene che una simile interpretazione del comma in esame non possa essere sicuramente accolta[70].

Per superare l'ambiguità del disposto del comma 2 *bis* dell'art. 268 c.p.p. una soluzione potrebbe essere quella di considerare congiuntamente i due presupposti dell'irrilevanza per "l'oggetto della conversazione" e per i "soggetti coinvolti"[71].

Una simile interpretazione limiterebbe l'operatività del divieto di trascrizione solo nel caso in cui gli interlocutori siano esterni al procedimento penale e l'oggetto del colloquio sia estraneo al *thema probandum* come delineato dall'art. 187 c.p.p. Tuttavia, questa prospettazione non tiene conto, ad esempio, del fatto che l'indagato non è mai un soggetto irrilevante per il procedimento e la trascrizione sommaria delle sue conversazioni, anche qualora non fossero inerenti al *thema probandum*, sarebbe quindi sempre ammissibile. Da questa considerazione si evidenzia l'opportunità di valutare i due presupposti richiesti dall'comma 2 *bis* dell'art. 268 c.p.p. come criteri alternativi anziché cumulativi[72].

Una possibile spiegazione del riferimento ai soggetti coinvolti che, inoltre, non sono indicati neppure nel successivo comma 2 *ter* dell'art. 268 c.p.p., potrebbe essere quella di ritenere l'introduzione di questa locuzione frutto di una «*svista legislativa, anziché di una scelta consapevole, e che possa quindi essere "sterilizzata" in via interpretativa*»[73].

L' art. 268 c.p.p., comma 2 *bis*, prevede che nel caso in cui venga intercettata una conversazione rispetto alla quale operi un divieto di trascrizione, nel verbale redatto dalla polizia giudiziaria devono essere annotati, in riferimento a quella conversazione, la data, l'ora ed il dispositivo sul quale è intervenuta l'intercettazione.

L'introduzione di questa peculiare procedura per le conversazioni irrilevanti serve ad eliminare ogni possibile riferimento al contenuto del dialogo in vista della sua futura distruzione[74].

---

[70] G. GIOSTRA-R. ORLANDI, *Nuove norme in tema di intercettazioni, Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p.7-8.

[71] G. GIOSTRA-R. ORLANDI, *ibidem*.

[72] G. GIOSTRA-R. ORLANDI, *ibidem*.

[73] G. GIOSTRA-R. ORLANDI, *ibidem*.

[74] D. PRETTI, *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in *Dir. pen. cont.*,2018, 1, p. 193.

È funzionale, invece, a temperare il rigore del comma 2 *bis* dell'art. 268 c.p.p. il comma 2 *ter* della medesima disposizione che prevede la possibilità per il pubblico ministero, con decreto motivato, di trascrivere nel verbale le conversazioni e le comunicazioni di cui al comma 2 *bis* «*quando ne ritiene la rilevanza per i fatti oggetto di prova. Può altresì disporre la trascrizione nel verbale, se necessarie a fini di prova, delle comunicazioni e conversazioni relative a dati personali definiti sensibili dalla legge*».

Il dettato della disposizione in esame evidenzia subito una distinzione tra le comunicazioni irrilevanti e le comunicazioni contenenti dati sensibili, in quanto le prime possono essere sempre trascritte qualora il pubblico ministero le ritenga "rilevanti" per i fatti oggetto di prova, mentre le seconde possono essere trascritte soltanto se "necessarie a fini di prova"[75].

L'art. 267, comma 4, c.p.p., al fine di permettere al pubblico ministero di disporre la trascrizione delle conversazioni di cui al comma 2 *bis* dell'art. 268 c.p.p., prevede che «*l'ufficiale di polizia giudiziaria provvede a norma dell'art.268 c.p.p. comma 2 bis informando preventivamente il pubblico ministero con annotazione sui contenuti delle comunicazioni e conversazioni*».

Da questa disposizione ne discende che la polizia giudiziaria, dopo aver effettuato una preliminare diagnosi sulla rilevanza della comunicazione o conversazione, deve procedere ad informare preventivamente il pubblico ministero con un'annotazione sui contenuti, permettendo così a quest'ultimo di conoscere tutti quei casi in cui sia dubbia la rilevanza di una specifica comunicazione o conversazione intercettata. È evidente come il contenuto della sopracitata annotazione inevitabilmente riguarderà le argomentazioni degli interlocutori spese nel dialogo captato, risolvendosi, quindi, in una trascrizione

[75]Cfr. Relazione illustrativa allo «*Schema di decreto legislativo recante disposizioni in materia di intercettazione di conversazioni o comunicazioni» (472-bis), consultabile on line sui siti internet di Camera (www.camera.it) e Senato (www.senato.it) : «Il vincolo è più rigoroso in relazione alle conversazioni contenenti dati sensibili, come definiti dalle vigenti disposizione di legge nel senso che la loro emersione deve essere altresì "necessaria" ai medesimi fini di prova; ciò vuoi dire che, di regola, i dati sensibili emergenti dalle comunicazioni intercettate sono destinati a rimanere del tutto riservati, quando non sia possibile stabilire un nesso essenziale tra la loro conoscenza e l'attività probatoria. In questo senso s'intende dare attuazione alla delega nella parte in cui discorre di conversazioni contenenti dati sensibili ai sensi dell'articolo 4, comma l, lettera d), del codice di cui al decreto legislativo 30 giugno 2003, n. 196, che non siano pertinenti all'accertamento delle responsabilità per i reati per cui si procede ovvero irrilevanti. La delega cioè sembra prescrivere un più penetrante obbligo ai fini dell'utilizzazione di conversazioni coinvolgenti dati sensibili, la cui trascrizione è imposta solo se, oltre che rilevanti, siano necessarie all'accertamento dei fatti*».

sommaria in apparente contrasto con il divieto di trascrizione di cui l'art. 268 comma 2 *bis*[76].

Secondo le indicazioni della Relazione illustrativa del d.lgs. n. 216/2017, l'obbligo di annotazione della polizia giudiziaria *ex* art. 267, comma 4, c.p.p. sussisterebbe soltanto nei casi in cui vi siano dubbi sulla rilevanza o meno di una specifica captazione e non opererebbe invece per tutte le ipotesi di conversazioni irrilevanti[77].

In questo modo si crea un doppio binario a seconda che le conversazioni siano state ritenute dalla polizia giudiziaria certamente irrilevanti oppure siano ritenute dalla stessa di dubbia rilevanza. Nel primo caso la polizia giudiziaria procederà alla sola indicazione nel verbale degli estremi identificati della conversazione o comunicazione captata, mentre nel secondo caso provvederà a redigere l'annotazione sui contenuti a cui seguirà il decreto del pubblico ministero che potrà o meno disporre la trascrizione[78].

Questa impostazione ha comportato l'insorgere di numerose critiche, poiché, limitando l'operatività dell'art. 267, comma 4, c.p.p. ai soli casi dubbi, si determina la creazione di una "zona grigia" contenente conversazioni e comunicazioni rispetto alle quali esiste soltanto un'indicazione nel verbale degli estremi e il cui contenuto è accessibile soltanto mediante l'ascolto diretto. Conseguentemente queste comunicazioni non sono né trascritte né annotate e, quindi, la dimensione della sopra indicata zona grigia dipende dalla sicurezza con cui la polizia giudiziaria procede a formulare una diagnosi di irrilevanza. Pertanto, questa diagnosi potrebbe rivelarsi errata in quanto espressa in assenza di una conoscenza complessiva di tutti gli elementi raccolti nelle indagini[79].

Per quanto riguarda la fase strettamente esecutiva delle operazioni d'intercettazioni l'art. 268, comma 3, c.p.p. prevede espressamente che le operazioni captative debbano realizzarsi con impianti installati presso la Procura della Repubblica e non, quindi, per mezzo d'impianti situati presso gli uffici della polizia giudiziaria operante. Tuttavia, nel

---

[76] D. PRETTI, *op. cit,* p. 194.

[77] Cfr. Relazione illustrativa allo «*Schema di decreto legislativo recante disposizioni in materia di intercettazione di conversazioni o comunicazioni» (472-bis) consultabile on line sui siti internet di Camera (www.camera.it) e Senato (www.senato.it): «in particolare, gli ufficiali di polizia giudiziaria hanno l'obbligo di informare il pubblico ministero, con apposita annotazione ai sensi dell'art.357 c.p.p., nei casi in cui sia dubbio se procedere a trascrizione, nel verbale, di dette conversazioni».*

[78] D. PRETTI, *op. cit,* p. 195.

[79] G. GIOSTRA-R. ORLANDI, *op. cit.,* p.10.

caso in cui gli impianti della procura risultino insufficienti o inidonei e sussistono eccezionali ragioni d'urgenza, il pubblico ministero con decreto motivato può autorizzare che le operazioni si realizzino con impianti del pubblico servizio o situati presso gli uffici della polizia giudiziaria.

Le eccezionali ragioni d'urgenza si riferiscono alle ipotesi in cui non è possibile attendere il ripristino di una situazione che consenta l'utilizzo degli impianti locati presso le procure[80]. La violazione di queste prescrizioni determina l'inutilizzabilità delle intercettazioni disposte illegittimamente ai sensi dell'art.271 comma 1 c.p.p.

Dell'insufficienza o inidoneità degli impianti delle procure e delle eccezionali ragioni d'urgenza deve esserne dato conto nel decreto autorizzativo del pubblico ministero. Sul punto la Suprema Corte ha però evidenziato che la motivazione sulle eccezionali ragioni d'urgenza assorbe i profili tecnico organizzativi inerenti all'insufficienza e inidoneità degli impianti che non devono quindi essere illustrati autonomamente[81].

Al comma 3 *bis* dell'art 268 c.p.p ,che ammette il ricorso ad impianti appartenenti a privati per l'esecuzione delle operazioni captative inerenti alle comunicazioni informatiche o telematiche, è stato introdotto con il d.lgs. n. 216/2017 un inciso che permette all'ufficiale di polizia giudiziaria impegnato nelle operazione d'intercettazione realizzate con il captatore informatico su dispositivi elettronici portatili, di avvalersi per le sole operazioni di avvio e cessazione delle operazioni di persone munite di specifiche competenze tecniche.

[80] E.APRILE-F.SPEZIA, *op.cit*,p.28.

[81] Cass.pen, sez.V, 23 Giugno 2017, n.49040, in *C.e.d. Cass.*, Rv.271852.

2.5 Le attività successive alla captazione

Una delle più importanti novità della riforma introdotta dal d.lgs. 216/2017 è l'eliminazione dell'udienza di stralcio che è stata sostituita dal meccanismo di acquisizione delle intercettazioni al fascicolo delle indagini di cui gli artt. 268 *bis*, 268 *ter* e 268 *quater* c.p.p.

Il legislatore delegato ha introdotto una procedura "bifasica"[82], disponendo il deposito delle intercettazioni e la successiva acquisizione attraverso un contraddittorio tra le parti di tipo cartolare e, solo quando risulta necessario, il giudice può fissare l'udienza al fine di disporre l'acquisizione e lo stralcio delle comunicazioni irrilevanti e inutilizzabili[83]. Questa procedura non coincide con quanto prescritto dall'art.268 commi 4, 5, 6, 7 e 8 c.p.p. abrogati.

Secondo la disciplina previgente, la polizia giudiziaria provvedeva a trasmettere al pubblico ministero le registrazioni e i verbali che venivano depositati presso la segreteria della procura ammettendo, tuttavia, che il deposito potesse essere posticipato fino alla chiusura delle indagini preliminari. Successivamente i difensori delle parti venivano avvisati della facoltà di esaminare gli atti e di prendere conoscenza, anche mediante ascolto, delle registrazioni depositate entro il termine fissato dal pubblico ministero ed eventualmente prorogato dal giudice[84].

In questo modo si realizzavano le premesse per la predisposizione del contraddittorio tra il pubblico ministero e i difensori che costituiva il momento cruciale dell'udienza di stralcio, preordinata alla cernita ed alla selezione delle conversazioni ed altre forme di comunicazioni, ivi comprese quelle informatiche o telematiche, costituenti l'esito delle operazioni captative[85].

---

[82] O.MAZZA, *Le nuove intercettazioni*, in A.SCALFATI-M.DEL TUFO (a cura di) *Leggi penali tra regole e prassi, Ius novum*, Torino, 2018, p.16.

[83] Si veda *infra* § 2.5.1.

[84] G. CONSO-V. GREVI-M. BARGIS, *op. cit.*, p 393.

[85] G. CONSO-V. GREVI-M. BARGIS, *ivi* ,p.394.

In effetti il pubblico ministero e le parti private hanno l'onere di chiedere al giudice per le indagini preliminari l'acquisizione delle intercettazioni coerentemente con il sistema accusatorio dove la prova è ammessa a richiesta di parte[86].

Secondo quanto disposto dall'abrogato comma 6 dell'art. 268 c.p.p., una volta scaduto il termine riconosciuto ai difensori per prendere cognizione di tutti gli atti depositati, il giudice fissava la data dell'udienza di stralcio e ne dava avviso sia al pubblico ministero che al difensore almeno ventiquattro ore prima.

Al giudice, in questa fase, veniva riconosciuto un limitato potere di filtro in quanto disponeva l'acquisizione delle conversazioni e delle comunicazioni indicate dalle parti stesse non "manifestamente irrilevanti" *ex* art. 268, comma 6, c.p.p. e procedeva anche d'ufficio allo stralcio delle registrazioni e dei verbali delle intercettazioni di cui era vietata l'utilizzazione ai sensi dell'art 271 c.p.p. o di altre disposizioni di legge[87]. Conclusa l'udienza di stralcio il giudice procedeva alla «*perizia trascrittiva*»[88], vale a dire alla trascrizione integrale delle registrazioni ammesse osservando le forme, i modi e le garanzie prescritte per la perizia *ex* art. 268, comma 7, c.p.p.[89], fatta salva la possibilità per i difensori in ogni caso di estrarre copia delle trascrizioni e disporre la registrazione delle stesse sul nastro. Le trascrizioni disposte dal giudice, essendo espressione di atti per loro natura non ripetibili, venivano inserite nel fascicolo per il dibattimento formato a norma dell'art. 431 c.p.p[90].

La disciplina introdotta dal d.lgs. 216/2017 si differenzia in maniera sostanziale da quella previgente esposta, soprattutto laddove prevede che la procedura selettiva di cui gli artt. 268 *bis*, 268 *ter*, 268 *quater* c.p.p. precede ed è autonoma all'udienza di trascrizione delle conversazioni e si colloca obbligatoriamente nel corso delle indagini preliminari.

---

[86] P.TONINI, *op. cit,* p.409.

[87] P.TONINI-C.CONTI, *op.cit*, p. 404.

[88] P.TONINI-C.CONTI, *ivi*, p.403.

[89] È necessario evidenziare come l'esperto che procederà alla trascrizione a norma dell'art. 268 comma 7 c.p.p. non può essere considerato un mero trascrittore ma dovrà possedere un adeguata professionalità tecnica per poter fornire indicazioni, quando necessarie, ad esempio sull'intonazione della voce, la lunghezza delle pause, in quanto si tratta di tutti elementi che possono incidere sul senso delle comunicazioni. Da ciò ne discende logicamente che il perito dovrà essere considerato l'interprete del senso e del contenuto dei dati vocali. Cfr C. cost. sent. n.336, 8 Ottobre 2008, in www.giustcost.org

[90] G. CONSO-V. GREVI-M. BARGIS, *op. cit.,* p.395.

L'art. 268 *quater*, comma 6, c.p.p. prevede, invero, che «*alle operazioni di acquisizione provvede il giudice per le indagini preliminari che ha autorizzato, convalidato o prorogato le intercettazioni*»[91].

Una significativa modifica è stata apportata, poi, dal legislatore delegato all'art. 268, comma 4, c.p.p. che oggi dispone la trasmissione immediata da parte della polizia giudiziaria, dopo la scadenza del termine indicato per lo svolgimento delle operazioni nei provvedimenti di autorizzazione o di proroga, dei verbali e delle registrazioni per la loro conservazione nell'archivio riservato di cui l'art. 269 c.p.p.

Ne consegue che gli atti relativi alle intercettazioni non vengono più inseriti nel fascicolo del pubblico ministero di cui l'art. 373, comma 5, c.p.p. nel quale confluiscono tutti gli atti d'indagine[92].

Quando per la prosecuzione delle indagini è necessario che l'ufficiale di polizia giudiziaria, delegato all'ascolto, consulti le risultanze già acquisite, il pubblico ministero dispone con decreto il differimento della trasmissione dei verbali e delle registrazioni, determinando contestualmente le prescrizioni per assicurare la tutela del segreto sul materiale non trasmesso.

Il nuovo art. 268 *bis* c.p.p. prevede che entro il termine di cinque giorni dalla conclusione delle operazioni il pubblico ministero depositi annotazioni[93], verbali, registrazioni, decreti di autorizzazione, convalida, proroga e, contestualmente, formi l'elenco di conversazioni o comunicazioni e flussi informatici o telematici che ritiene rilevanti ai fini di prova. Il deposito deve essere effettuato non in segreteria, come statuiva il previgente art. 268 c.p.p. ma nell'archivio riservato istituito presso l'ufficio del pubblico ministero ai sensi dell'art. 89 *bis* disp. att. c.p.p.[94].

L'art 268 *bis*, comma 2, c.p.p. dispone, inoltre, che i difensori delle parti vengano immediatamente informati del deposito ed abbiano la facoltà di esaminare gli atti, visionare l'elenco formato dal pubblico ministero, ascoltare le registrazioni e prendere

---

[91] O.MAZZA, *op. cit.,* p.17.

[92] D. PRETTI, *op. cit,* p196.

[93] La disposizione in esame prescrive, quindi, anche il deposito delle annotazioni disciplinate dall'art. 267 comma 4 c.p.p., vale a dire quelle che la polizia giudiziaria trasmette per demandare al pubblico ministero la valutazione di rilevanza di singole intercettazioni ai fini della successiva trascrizione.

[94] G. GIOSTRA-R. ORLANDI, *op. cit.,* p.17.

cognizione dei flussi. Dal mancato avviso discende la nullità del successivo provvedimento di acquisizione delle conversazioni intercettate a norma degli artt. 178 comma 1, lett *c)* e 180 c.p.p., a causa della mancata assistenza e rappresentanza dell'imputato[95].

Il legislatore in sede di riforma sembra, sul punto, aver recepito quanto disposto dall'abrogato comma 6 dell'art. 268 c.p.p., seppure con una significativa divergenza. L'attuale secondo comma dell'art. 268-*bis* c.p.p. riconosce ai difensori la facoltà di prendere cognizione dell'elenco di comunicazioni o conversazioni e dei flussi informatici e telematici rilevanti ai fini di prova predisposto dal pubblico ministero. Da ciò ne consegue che l'ambito esaminabile dai difensori è circoscritto all'elenco formato dal pubblico ministero che deve controllare l'effettiva rilevanza delle captazioni ai fini di prova, escludendo il materiale non rilevante, mentre, secondo la normativa abrogata, i difensori potevano ascoltare l'intera massa di registrazioni e conoscere tutti i flussi di comunicazioni informatiche o telematiche[96].

La *discovery* di tutti gli atti si realizza nel corso delle indagini preliminari e dovrebbe precedere il deposito degli esiti delle indagini stesse ai sensi dell'art 415-*bis* c.p.p.

Questa conclusione discende dal fatto che l'ostensione delle captazioni *ex* art.268 *bis* c.p.p. è funzionale a consentire ai difensori delle parti di venire a conoscenza delle operazioni eseguite, mentre il deposito di cui l'art. 415-*bis* c.p.p. permette alla difesa dell'indagato di esercitare le facoltà di cui l'art. 415-*bis* comma 3 c.p.p. al fine di dissuadere il pubblico ministero dall'esercizio dell'azione penale[97].

Per quanto concerne l'acquisizione delle comunicazioni, delle conversazioni e dei flussi informatici e telematici al fascicolo delle indagini, il legislatore delegato con l'art. 268 *ter* c.p.p. ha introdotto due distinti meccanismi procedurali.

Il primo è descritto dal comma 1 dell'art. 268-*ter* c.p.p. e riguarda esclusivamente l'acquisizione delle conversazioni o comunicazioni utilizzate per l'adozione di una misura cautelare. In questa ipotesi il legislatore ha stabilito che il pubblico ministero

---

[95] O.MAZZA, *op. cit.,* p.68.

[96] O.MAZZA, *ivi,* p.69.

[97] G. GIOSTRA-R. ORLANDI, *op. cit.,* p.18.

inserisca i verbali e gli atti concernenti le comunicazioni utilizzate ai fini cautelari all'interno del fascicolo di cui all'art.373,comma 5, c.p.p.[98].

Il ricorso alla procedura appena descritta è subordinato all'accoglimento della richiesta di adozione di una misura cautelare nel corso delle indagini preliminari. In effetti il termine "adozione" utilizzato nel comma 1 dell'art. 268-*ter* c.p.p. non lascia spazio ad interpretazioni alternative che vi riconducano anche i casi in cui il giudice abbia rigettato la richiesta della pubblica accusa[99].

Fuori dal caso in cui sia stata adottata una misura cautelare, l'art. 268-*ter*, comma 2, c.p.p., prevede un secondo meccanismo procedurale, disponendo che entro cinque giorni dal deposito il pubblico ministero presenti al giudice per le indagini preliminari la richiesta di acquisizione delle comunicazioni o conversazioni e dei flussi di comunicazioni informatiche o telematiche contenuti nell'elenco formato a norma dell'art 268-*bis*, comma 1, c.p.p. dandone contestuale comunicazione ai difensori.

Entro il termine di dieci giorni dalla ricezione dell'avviso di cui l'art. 268 *bis* comma 2 c.p.p. ai difensori è riconosciuta la possibilità di richiedere sia l'acquisizione di comunicazioni intercettate di rilievo probatorio omesse dal pubblico ministero sia l'eliminazione dei dati che quest'ultimo ha chiesto ma che risultano inutilizzabili o dei quali sia vietata la trascrizione anche sommaria nel verbale, in quanto irrilevanti *ex* art. 268 comma 2 *bis* c.p.p.[100]. Il suddetto termine può essere prorogato dal giudice per un periodo non superiore a dieci giorni quando sussistono rilevanti ragioni inerenti alla complessità del procedimento e al numero delle intercettazioni.

Il termine di dieci giorni riconosciuto ai difensori è, secondo alcuni Autori, espressione di un vero e proprio sbilanciamento della posizione del difensore rispetto a quella del

[98] Il d.lgs. n.216/2017 ha modificato contestualmente gli artt.291, 292, 293 c.p.p., nell'art 291 comma 1 c.p.p. è stato introdotto un inciso che abilita il Pubblico Ministero a trasmettere, allorché richiede una misura cautelare al Giudice delle indagini preliminari, i verbali delle trascrizioni sommarie, limitatamente alle comunicazioni e conversazioni rilevanti. E 'stato, dal legislatore, ulteriormente aggiunto il comma 1 *ter* dell'art. 291 c.p.p. che consente d'inserire nella richiesta cautelare, quando necessario, solo i brani essenziali alle conversazioni intercettate. Nell'art 292 c.p.p. è stato introdotto il comma 2 *quater* che introduce una disposizione speculare per l'ordinanza cautelare. Infine, nell'art. 293 c.p.p. è stato aggiunto il comma 3 che attribuisce al difensore il diritto di esaminare e di copiare i verbali delle comunicazioni e conversazioni rilevanti ai fini cautelari e il diritto di ottenere la trasposizione delle relative registrazioni sui idonei supporti.

[99] D. PRETTI, *op. cit,* p. 205.

[100] Si veda *supra* § 2.3.

pubblico ministero[101] perché ,in primo luogo, quest'ultimo, a differenza dei difensori, conosce già il contenuto delle comunicazioni registrate durante l'esecuzione delle operazioni captative attraverso la "relazione di servizio" trasmessa dai soggetti incaricati allo svolgimento delle intercettazioni e non deve attendere la conclusione delle stesse[102]. Diversamente i difensori vengono a conoscenza della stessa esistenza di un'attività captativa da parte dell'autorità inquirente soltanto nel momento dell'avviso di cui l'art. 268 *bis*, comma 2, c.p.p. ed in un ristretto lasso di tempo di dieci giorni devono individuare dei brani di registrazione non elencati dal pubblico ministero ma potenzialmente utili per confutare l'impostazione accusatoria al fine di richiederne l'acquisizione[103].

Per compensare il poco tempo concesso ai difensori per l'acquisizione delle registrazioni e per l'individuazione di quelle inutilizzabili o non trascrivibili l'art. 268 *ter*, comma 5, c.p.p. consente ai difensori di perfezionare le rispettive richieste presentate nei termini ordinari con integrazioni e memorie fino alla decisione del giudice. La stessa facoltà è riconosciuta al pubblico ministero[104].

Il successivo comma 6 introduce un'ulteriore ipotesi di modifica unilaterale del materiale di cui si chiede l'acquisizione: il pubblico ministero con riferimento alle comunicazioni o conversazioni utilizzate nel corso delle indagini preliminari per l'adozione di una misura cautelare può domandare al giudice l'eliminazione dal fascicolo dei verbali e delle registrazioni rispetto alle quali ritiene sussistente, in forza di elementi sopravvenuti, l'irrilevanza.

Questa disposizione è giustificata dalla circostanza che l'eventuale riascolto di determinate registrazioni permette di attribuire alle stesse una diversa valutazione. Si pensi, ad esempio, al caso in cui nel corso della comunicazione intercettata venga fatto riferimento al nominativo di un soggetto omonimo rispetto ad uno dei coindagati e qualora da un'ulteriore conversazione emergano elementi dai quali risulti questa omonimia, sarà evidente che il soggetto non intendeva riferirsi al coindagato ma ad un

[101] Si veda O.MAZZA, *op. cit.*, p. 72; allo stesso modo G. GIOSTRA-R. ORLANDI, *op. cit.*, p. 20.

[102] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 130.

[103] O.MAZZA, *op. cit.*, p. 74.

[104] G. GIOSTRA-R. ORLANDI, *op. cit.*, p. 22

suo omonimo e conseguentemente non vi sarà ragione di mantenere la registrazione nel materiale acquisibile[105].

2.5.1 La decisione del giudice e la conservazione della documentazione

La procedura di selezione delle comunicazioni e conversazioni rilevanti ad opera del giudice è descritta dall'art.268 *quater* c.p.p.

Dal dato codicistico emergono due meccanismi procedurali di selezione: in primo luogo l'art. 268 *quater,* comma 1, c.p.p. prevede una procedura *de plano* connotata dalla mancata fissazione di un'udienza e da un contraddittorio meramente cartolare. Il giudice, decorsi cinque giorni dalla presentazione delle richieste, procederà all'ascolto delle conversazioni e con ordinanza, emessa in camera di consiglio senza l'intervento del pubblico ministero e dei difensori, disporrà l'acquisizione delle conversazioni e comunicazioni indicate dalle parti, salvo che siano manifestatamente irrilevanti, ordinando anche d'ufficio lo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione[106].

Il giudizio di manifesta irrilevanza è necessariamente meno stringente rispetto a quello di rilevanza di cui al precedente art. 268, commi 2 *bis* e 2 *ter,* c.p.p. e interesserà esclusivamente quelle intercettazioni rispetto alle quali non sia stato introdotto alcun contraddittorio, ovvero rispetto alle quali la difesa non abbia chiesto l'esclusione. Allo stesso modo il giudice procederà allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione[107].

L'art. 268 *quater*, comma 2, c.p.p., disciplinando la seconda procedura di selezione delle intercettazioni, dispone che il giudice emetterà, qualora risulti "necessario", l'ordinanza di acquisizione all'esito dell'udienza camerale con tempestivo avviso al pubblico ministero e ai difensori. È probabile che il giudice ricorrerà a questo meccanismo procedurale, ad esempio, quando ritenga, tenendo conto della complessità delle questioni

[105] O.MAZZA, *op. cit.,* p. 79.

[106] G. GIOSTRA-R. ORLANDI, *op. cit.,* p. 24.

[107] D. PRETTI, *op. cit,* p. 202-203.

sottese alle richieste delle parti, di non poter pervenire a un convincimento in ordine all'acquisizione neppure ascoltando le registrazioni[108].

In questo caso non si può parlare di una vera e propria udienza di stralcio poiché lo scopo dell'udienza *ex* art. 268 *quater,* comma 2, c.p.p. è quello di fornire al giudice, nel contraddittorio delle parti, adeguati elementi per decidere sull'acquisizione delle conversazioni e comunicazioni indicate dalle parti[109].

Con l'ordinanza di acquisizione viene meno il segreto sugli atti e i verbali delle conversazioni che confluiscono nel fascicolo di cui l'art. 373,comma 5, c.p.p. del pubblico ministero a norma dell'art. 268 *quater,* comma 3, c.p.p. Quelli non acquisiti sono immediatamente restituiti ai sensi dell'art 268 *quater,* comma 5, c.p.p. al pubblico ministero per la conservazione nell'archivio riservato. I brani acquisiti nella maggioranza dei casi saranno già trascritti anche sommariamente dalla polizia giudiziaria nei relativi verbali; tuttavia, nella circostanza in cui vengano acquisite comunicazioni o conversazioni su richiesta dei difensori che non siano state trascritte, il giudice ne ordinerà la trascrizione sommaria a cura del pubblico ministero[110].

Relativamente alla conservazione della documentazione, l'art. 269, comma 1, c.p.p. è stato sostituito dal legislatore delegato.

[108] G. GIOSTRA-R. ORLANDI, *op. cit.,* p. 25.

[109] O.MAZZA, *op. cit.,* p.81.

[110] D. PRETTI, *op. cit,* p.204.

Oggi prevede che i verbali e le registrazioni delle intercettazioni non siano più conservati integralmente presso il pubblico ministero che ha disposto le operazioni captative ma che i verbali e le registrazioni e ogni altro atto ad esse relativo vengano conservati integralmente in un archivio riservato, disciplinato dall'art. 89 *bis* disp att. c.p.p.[111].

Secondo alcuni Autori la locuzione "ogni altro atto ad esse relativo" di cui l'art.269 c.p.p. non risulta essere connotata da sufficiente chiarezza poiché si discute se questa espressione sia idonea a ricomprendere ad esempio anche le annotazioni con le quali la polizia giudiziaria chiede la proroga dell'attività oppure un'informativa con la quale propone una nuova pista investigativa che riporta il contenuto di una conversazione[112].

L'introduzione dell'archivio riservato ha comportato una contestuale modifica dell'art. 92 disp. att. c.p.p. concernente la trasmissione dell'ordinanza che dispone la misura cautelare con l'introduzione del comma 1 *bis* secondo il quale : «*Contestualmente sono restituiti al pubblico ministero, per la conservazione nell'archivio riservato di cui l'art. 89 bis, gli atti concernenti le comunicazioni e conversazioni intercettate ritenute dal giudice non rilevanti o inutilizzabili*».

La documentazione a cui fa riferimento l'art. 269 c.p.p. risulta essere coperta dal segreto, fatta ad eccezione per le registrazioni e i verbali già acquisiti al fascicolo delle indagini[113].

Il legislatore ha, inoltre, sostituito un inciso del comma 2 e ciò ha comportato che la distruzione a tutela della riservatezza può essere chiesta solo per le registrazioni non

---

[111] Cfr. art. 89 *bis* att.c.p.p. :« *Archivio riservato delle intercettazioni*
1. Presso l'ufficio del pubblico ministero è istituito l'archivio riservato previsto dall'articolo 269, comma 1, del codice, nel quale sono custoditi le annotazioni, i verbali, gli atti e le registrazioni delle intercettazioni a cui afferiscono.
2. L'archivio è gestito, anche con modalità informatiche, e tenuto sotto la direzione e la sorveglianza del procuratore della Repubblica, con modalità tali da assicurare la segretezza della documentazione custodita. Il procuratore della Repubblica impartisce, con particolare riguardo alle modalità di accesso, le prescrizioni necessarie a garantire la tutela del segreto su quanto ivi custodito.
3. All'archivio possono accedere, secondo quanto stabilito dal codice, il giudice che procede e i suoi ausiliari, il pubblico ministero e i suoi ausiliari, ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto, i difensori delle parti, assistiti, se necessario, da un interprete. Ogni accesso è annotato in apposito registro, gestito con modalità informatiche; in esso sono indicate data, ora iniziale e finale, e gli atti specificamente consultati.
4. I difensori delle parti possono ascoltare le registrazioni con apparecchio a disposizione dell'archivio, ma non possono ottenere copia delle registrazioni e degli atti ivi custoditi».

[112] G. CASCINI, *Il Pubblico Ministero*, in G. GIOSTRA-R. ORLANDI, *op. cit,*, p. 188.

[113] Cfr. art 269 comma 1 *bis* c.p.p.

acquisite mentre in precedenza era richiedibile per tutta la documentazione non necessaria al procedimento[114].

Secondo quanto disposto dal comma 3 dell'art. 269 c.p.p., la distruzione nei casi in cui è prevista viene eseguita sotto controllo del giudice e dell'operazione è redatto verbale.

2.6 Utilizzabilità dei risultati delle intercettazioni

L' art. 270 comma 1 c.p.p. dispone che *«i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza»*.

Tale esclusione probatoria è inquadrata nell'ambito della tutela costituzionale dell'inviolabilità del diritto alla libertà e segretezza delle comunicazioni di cui l'art. 15 Cost. che subirebbe un'indebita restrizione qualora la sua garanzia non comportasse il divieto di divulgazione o di utilizzazione successiva delle notizie di cui si è venuti a conoscenza a seguito dell'esecuzione di intercettazioni legittime e preordinate all'accertamento di determinati reati[115].

È, inoltre, evidente come l'utilizzo dei risultati dell'intercettazione in un altro procedimento precluderebbe la garanzia del previo atto motivato dell'autorità giudiziaria sul diverso fatto, rispetto al quale difetterebbe del tutto il controllo giurisdizionale in ordine all'esistenza dei presupposti dell'intercettazione[116].

Tuttavia la seconda parte del comma 1 dell'art. 270 c.p.p. introduce una deroga, se pur parziale, a questo divieto di utilizzazione ammettendo la possibilità di utilizzare i risultati delle intercettazioni in procedimenti diversi preordinati all'accertamento di reati rispetto ai quali è obbligatorio l'arresto in flagranza di cui l'art. 380 c.p.p.[117].

Qualora ricorrano i presupposti per l'operatività di questa deroga, il comma 2 dell'art. 270 c.p.p., così come modificato dal d.lgs. 216/2017, prevede che i verbali e le

[114] V. GIGLIO, *op. cit.*, p. 96-97.

[115] Corte cost., 23 luglio 1991, n.366, in www.giustcost.org

[116] L.FILIPPI, *op.cit.*, p.182.

[117] P. BALDUCCI, *op.cit.*, p.175 .

registrazioni delle intercettazioni siano depositati presso l'autorità competente per il diverso procedimento e si applichino le disposizioni di cui gli artt. 268 *bis*, 268 *ter* e 268 *quater* c.p.p. . Quest'obbligo di deposito riguarda esclusivamente gli atti indicati dall'art. 270, comma 2, c.p.p., vale a dire i verbali e le registrazioni; per quanto riguarda la mancata inclusione dei decreti autorizzativi nel compendio depositato nel procedimento *ad quem* la giurisprudenza ha chiarito non essere prevista alcuna conseguenza sanzionatoria[118].

La *ratio* di questa eccezione al divieto di inutilizzabilità dei risultati delle intercettazioni in un procedimento diverso va riscontrata nel fatto che sussistono reati idonei a destare particolare allarme sociale e conseguentemente il legislatore ha operato un bilanciamento fra il diritto alla libertà e segretezza delle comunicazioni e quello rappresentato dall'interesse pubblico alla repressione dei reati e al perseguimento in giudizio di coloro che delinquono[119].

Al fine di salvaguardare il nucleo essenziale del diritto di cui l'art. 15 Cost., il legislatore ammette l'utilizzo dei risultati delle intercettazioni in procedimenti diversi soltanto nella circostanza in cui questi ultimi risultino "indispensabili" per l'accertamento di alcuno dei delitti indicati nell'art. 380 c.p.p.[120] .

Il presupposto dell'indispensabilità non deve essere interpretato in maniera riduttiva nel senso di ricorrere ai risultati delle intercettazioni in un procedimento diverso solo quando quest'ultime rappresentano l'unica fonte di prova disponibile ma «*anche qualora esistessero altri strumenti di convincimento, le bobine potrebbero essere acquisite, purché l'alternativa condanna-proscioglimento non sia risolubile senza di esse*»[121].

Dall'analisi del presupposto testuale si evidenzia come non sarebbe ammissibile un'acquisizione dei risultati delle intercettazioni in un procedimento diverso per altri scopi, ad esempio quando risultino funzionali solo alla commisurazione della pena[122].

---

[118] Cass. pen., sez.un., 23 novembre 2004, n. 45189, in *C.e.d. Cass*., Rv. 229246.

[119] Corte cost., 24 febbraio 1994, n.63, in www.giustcost.org

[120] P. BALDUCCI, *op.cit*., p. 176.

[121] A.CAMON, *op.cit*., p.301.

[122] *Ibidem.* Si veda *contra* Cass. pen., sez. VI, 26 Marzo 1996, Sollecito, n.5363, in *C.e.d. Cass*., Rv.205075: «nel *senso che tale utilizzazione sia possibile non solo quando i risultati in questione siano indispensabili all'accertamento del fatto-reato altrimenti non dimostrabile con diversa rilevante prova d'accusa. Deve invece ritenersi che "l'indispensabilità dell'accertamento" vada riferita a tutta l'imputazione, compresi i fatti relativi alla punibilità, alla determinazione della pena ed alla qualificazione del reato medesimo in rapporto alle circostanze attenuanti o aggravanti*»,

Per contro dalla giurisprudenza recente emerge come il presupposto dell'indispensabilità venga interpretato in maniera estensiva, riconoscendone la sussistenza anche nell'ipotesi di accertamento non soltanto del fatto di reato ma dell'intera imputazione, dunque anche per i fatti inerenti la punibilità, la determinazione della pena, le circostanze del reato[123]. Inoltre, l'indispensabilità potrebbe ricorrere anche quando le captazioni servano come riscontri per il rafforzamento di dichiarazioni accusatorie[124].

Un elemento di criticità posto dall'art.270 c.p.p. è rappresentato dall'identificazione del concetto di "procedimento diverso".

È innanzitutto escluso che il frazionamento di un procedimento unitario possa dar luogo a diversità di procedimenti, in quanto l'art. 270 c.p.p. si applica a procedimenti distinti *ab origine*[125].

Da ciò ne consegue che in base alla giurisprudenza prevalente il concetto di procedimento diverso deve riferirsi non a dati meramente formali, come il numero del procedimento o il titolo del reato oggetto d'iscrizione nell'apposito registro, bensì alla sostanziale diversità del fatto storico[126].

In maniera speculare la nozione d'identico procedimento esclude l'operatività del divieto di utilizzazione di cui l'art. 270 c.p.p. : un procedimento è considerato identico o il medesimo solo quando tra il contenuto dell'originaria notizia di reato oggetto del decreto autorizzativo del giudice *ex* art. 267 c.p.p. e quello dei reati per cui si procede vi sia una stretta connessione sotto il profilo oggettivo di cui l'art. 12 c.p.p., probatorio o finalistico che ne evidenzi l'appartenenza ad un unico sostanziale filone investigativo [127].

Inoltre, il divieto di utilizzazione dei risultati delle intercettazioni in procedimenti diversi riguarda solo la circostanza in cui i risultati vengano utilizzati come elementi di prova e non anche la possibilità di utilizzarli come notizia di reato al fine di avviare nuove indagini e di acquisire nuove fonti probatorie[128].

---

[123] Cass. pen., sez. II, 18 febbraio 2015, n.12625, Moi, in *C.e.d. Cass.*, Rv. 262927.

[124] *Ibidem*.

[125] Cass. pen., sez.V, 14 luglio 2017, n.43977, in *C.e.d. Cass.*, Rv. 271754.

[126] Cass. pen., sez.II ,1 aprile 2015, n.19730, in *C.e.d. Cass*., Rv.263527.

[127] Cass. pen., sez. un., 26 giugno 2014, n.32697, in *C.e.d. Cass*., Rv. 259777.

[128] Cass. pen. sez. III , 29 gennaio 2015, n.12536, in *C.e.d. Cass*., Rv.262999.

Bisogna, infatti, evidenziare che sussiste l'obbligo da parte del pubblico ministero che venga a conoscenza di un fatto criminoso di dare avvio alle indagini e, allo stesso tempo, la polizia giudiziaria che, nell'esercizio delle sue funzioni, abbia preso cognizione di una *notitia criminis,* ha il dovere comunicarlo senza ritardo al pubblico ministero che procederà all'iscrizione nel registro delle notizie di reato di cui l'art. 335 c.p.p.[129].

Il Dlgs. 216/2017 non è intervenuto in maniera incisiva sul disposto dell'art. 270 c.p.p. limitandosi ad aggiungere il comma 1 *bis* che preclude l'utilizzabilità ai fini di prova dei risultati delle intercettazioni tra presenti acquisiti tramite captatore informatico per reati diversi da quelli a cui si riferisce il decreto autorizzativo, fatta eccezione dell'ipotesi in cui siano indispensabili per l'accertamento di reati per i quali sia obbligatorio l'arresto in flagranza.

Per quanto riguarda i divieti di utilizzazione il legislatore ha affidato all'art.271 c.p.p. la tenuta garantistica dell'intera disciplina delle intercettazioni, disponendo la massima sanzione processuale, quella dell'inutilizzabilità, per evidenziare che le informazioni ottenute in modo illegittimo non possono supportare le tesi accusatorie[130].

Si tratta di un'inutilizzabilità speciale in quanto è determinata dalla violazione delle regole di formazione di una specifica prova, per contro è generale l'inutilizzabilità disciplinata dall'art. 191, comma 1, c.p.p. collegata a tutte le prove acquisite in violazione di legge e rilevabile anche d'ufficio in ogni stato e grado del procedimento[131].

L'inutilizzabilità colpisce non l'intercettazione in quanto tale bensì i suoi risultati che possono, a seconda dei casi, rivestire sia la natura di prova, tipica nella fase del giudizio, sia quella d'indizi propria della fase delle indagini preliminari[132].

L'art. 271 c.p.p. prevede diverse ipotesi d'inutilizzabilità delle intercettazioni tra le quali la Corte costituzionale ha individuato i cosiddetti "vizi procedurali" che «*attengono a comunicazioni di per sé non inconoscibili che avrebbero potuto essere legittimamente captate se fosse stata seguita la procedura corretta*» [133]e si sostanziano in violazioni di

---

[129] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 198.

[130] V. GIGLIO, *op. cit.*, p. 141.

[131] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 214.

[132] Cass. pen., sez.un., 20 novembre 1996, n.21, Glicora ed altri, in *C.e.d. Cass*., Rv. 206955.

[133] Cort. cost., sent.,15 gennaio 2013, n.1, in www.giustcost.org

«*regole procedurali che prescindono dalla qualità dei soggetti coinvolti e dal contenuto delle comunicazioni captate*»[134].

L'art. 271, comma 1, c.p.p. individua le inutilizzabilità procedurali : si tratta delle ipotesi in cui le intercettazioni sono state eseguite fuori dai casi previsti dalla legge oppure sono state realizzate non rispettando i presupposti e le forme del provvedimento di esecuzione e di autorizzazione secondo quanto disposto dall'art. 267 c.p.p. Infine, questa disposizione prevede come vizio procedurale il caso in cui le intercettazioni sono realizzate non osservando quanto disposto dai commi 1 e 3 dell'art. 268 c.p.p., vale a dire senza registrare le comunicazioni e senza redigere il verbale sommario delle operazioni oppure sono state compiute al di fuori degli impianti installati nella procura della repubblica senza che sussistano ragioni d'urgenza[135].

Un ulteriore vizio di natura procedurale è previsto dal comma 1*bis* dell'art. 271 c.p.p., introdotto dal d.lgs. 216/2017, che prevede l'inutilizzabilità dei dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore nel dispositivo bersaglio e ogni altro dato acquisito oltre i limiti di luogo e di tempo fissati nel decreto autorizzativo. Il legislatore non ha chiarito, però, il significato da attribuire alla locuzione "operazioni preliminari" e si ritiene che quest'ultime dovrebbero sostanziarsi nelle attività tecniche che servono a verificare l'efficienza del captatore informatico[136].

[134] *Ibidem.*

[135] P .TONINI, *op. cit.,* p. 412.

[136] V. GIGLIO, *op. cit.,* p. 142.

Il comma 2 dell'art. 271 c.p.p. vieta l'uso delle intercettazioni che abbiano ad oggetto conversazioni o comunicazioni delle persone indicate nell'elenco dell'art. 200 ,comma 1, c.p.p.[137]. Il divieto riguarda ovviamente le comunicazioni che abbiano ad oggetto fatti conosciuti in ragione di un rapporto professionale e cessa se gli interessati abbiano già deposto su di essi. Questa norma rappresenta una proiezione del diritto di astensione che viene riconosciuto ai soggetti indicati nell'art. 200 c.p.p. in sede di testimonianza [138]e trattandosi di un'inutilizzabilità che colpisce i dati relativi ai fatti conosciuti a causa della professione, non è preclusa la possibilità di sottoporre a controllo le utenze di questi soggetti ma si vieta l'utilizzazione dei risultati inerenti a informazioni specifiche[139] . Le intercettazioni riconosciute come inutilizzabili, secondo quanto disposto dall'art. 271, comma 3, c.p.p., per ordine del giudice devono essere distrutte in ogni stato e grado del procedimento, salvo che costituiscano il corpo del reato. Anche se la disposizione in esame non contiene un'espressa previsione in ordine alle modalità procedurali da seguire per la distruzione, la Corte costituzionale ritiene che debba essere seguita una procedura camerale nel contraddittorio fra le parti[140].

L'inutilizzabilità delle intercettazioni non preclude che le stesse possano essere utilizzate come impulso per l'esecuzione di nuove indagini poiché la giurisprudenza di legittimità ha evidenziato come il decreto autorizzativo delle intercettazioni può trovare il suo fondamento anche in una notizia di reato desunta da intercettazioni inutilizzabili[141].

---

[137] Si veda Art. 200 c.p.p.: «*Non possono essere obbligati a deporre su quanto hanno conosciuto per ragione del proprio ministero, ufficio professione, salvi i casi in cui hanno l'obbligo di riferirne all'autorità giudiziaria:*
a) i ministri di confessioni religiose, i cui statuti non contrastino con l'ordinamento giuridico italiano;
b) gli avvocati, gli investigatori privati autorizzati, i consulenti tecnici e i notai;
c) i medici e i chirurghi, i farmacisti, le ostetriche e ogni altro esercente una professione sanitaria;
d) gli esercenti altri uffici o professioni ai quali la legge riconosce la facoltà di astenersi dal deporre determinata dal segreto professionale.
Il giudice, se ha motivo di dubitare che la dichiarazione resa da tali persone per esimersi dal deporre sia infondata, provvede agli accertamenti necessari. Se risulta infondata, ordina che il testimone deponga.
Le disposizioni previste dai commi 1 e 2 si applicano ai giornalisti professionisti iscritti nell'albo professionale, relativamente ai nomi delle persone dalle quali i medesimi hanno avuto notizie di carattere fiduciario nell'esercizio della loro professione. Tuttavia se le notizie sono indispensabili ai fini della prova del reato per cui si procede e la loro veridicità può essere accertata solo attraverso l'identificazione della fonte della notizia, il giudice ordina al giornalista di indicare la fonte delle sue informazioni».

[138] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 227.

[139] A.CAMON, *op.cit*., p.134.

[140] Cort. cost. sent., 15 Gennaio 2013, n.1, in www.giustcost.org

[141] Cass. pen., sez.I , 2 marzo 2010, n.16293, in *C.e.d. Cass*., Rv.246656.

2.7 Il Decreto legge, 30 Dicembre 2019, n. 161: "la riforma della riforma".

Come analizzato nei paragrafi precedenti, le modifiche introdotte dal d.lgs. 216/2017 alla disciplina delle intercettazioni presentano profili di criticità compiutamente evidenziati da numerosi Autori[142]. Non sorprende, quindi, che il Consiglio dei Ministri sia intervenuto nuovamente sulla disciplina delle intercettazioni con il Decreto legge, n.161/2019.

Il legislatore con il suddetto decreto opera, da un lato, un «*restyling conservativo*»[143] ripristinando lo *status quo ante* attraverso la riproposizione della disciplina tradizionale dell'istituto delle intercettazioni; dall'altro introduce elementi di novità al fine di adeguare il sistema normativo alle sfide proprie dell'era tecnologica[144].

La "riforma della riforma" attuata con il d.l. 161/2019 interviene sul d.lgs. 216/2017 con l'intento di raggiungere un nuovo equilibrio tra esigenze investigative e tutela della privacy[145].

Al fine di tutelare la riservatezza delle conversazioni apprese durante le operazioni di intercettazione, la novella modifica le tecniche di selezione delle conversazioni e delle comunicazioni captate che costituiranno oggetto dei brogliacci di ascolto. Il comma 4 dell'art. 267 c.p.p.[146], pertanto, viene depurato dagli innesti del d.lgs. 216/2017, conferendo così al pubblico ministero il potere d'individuare il materiale pertinente alle indagini e di avvalersi, eventualmente, dell'ausilio dell'ufficiale di polizia giudiziaria.

---

[142] Sui profili critici della normativa introdotta dal d.lgs. 216/2017 si veda G. GIOSTRA-R. ORLANDI, *op. cit.*, O.MAZZA, *op. cit.*, V. GIGLIO, *op. cit.*, D. PRETTI, *op. cit*, A.SCALFATI, *La riforma della giustizia penale*, Torino, 2017, p. 279 ss., G. SPANGHER, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giust.pen.web*, 2018, p. 1 ss., G. SPANGHER, *La riforma Orlando. Modifiche al Codice penale, al Codice di procedura penale e all'Ordinamento Penitenziario*, Pisa, 2017, p. 111 ss.

[143] W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia d'intercettazioni*, in *Sistema Penale*, 2020, 1, p.65.

[144] W. NOCERINO, *ivi*, p.67.

[145] W. NOCERINO, *ivi*, p.63.

[146] Si veda art. 2, comma 1, lett. d), punto 3, d.l. 161/2019: « *d) all'articolo 267: 3) al comma 4, l'ultimo periodo è soppresso*».

In questo modo il d.l. 161/2019 semplifica la procedura di selezione del materiale rilevante, eliminando quella forma di coordinamento prevista tra gli organi inquirenti dall'art. 268, commi 2-*bis* e 2-*ter*, c.p.p.[147], introdotta dal d. lgs. 216/2017.

Il legislatore, infatti, provvede all'abrogazione del comma 2-*ter* dell'art. 268 c.p.p.[148] e modifica il comma 2-*bis* dell'art. 268 c.p.p. disponendo che i brogliacci di ascolto redatti dalla polizia giudiziaria possono essere rettificati dal pubblico ministero il quale «*dà indicazioni e vigila affinché nei verbali non siano riportate espressioni lesive della reputazione delle persone o quelle che riguardano dati personali definiti sensibili dalla legge, salvo che si tratti di intercettazioni rilevanti ai fini delle indagini*»[149].

Sempre intervenendo sul disposto dell'art. 268 c.p.p. per bilanciare l'interesse alla riservatezza dei dati appresi con l'esigenza di garantire la trasparenza delle operazioni d'intercettazione, il d.l. 161/2019 perfeziona la procedura di deposito e funzionamento dell'archivio digitale.

[147] Sul tema dei profili di criticità dei commi 2-*bis* e 2-*ter* dell'art. 268 c.p.p. come modificato dal d.lgs 216/2017 si veda *supra* 2.4.

[148] Si veda art. 2, comma 1, lett. e, punto 2, d.l. 161/2019: «*all'art. 267 c.p.p.: 2) il comma 2-ter è abrogato*».

[149] Si veda art. 2, comma 1, lett. e, punto 1, d.l. 161/2019, all'articolo 268 c.p.p.: il comma 2-bis è sostituito dal seguente: «2-*bis. Il pubblico ministero dà indicazioni e vigila affinché' nei verbali non siano riportate espressioni lesive della reputazione delle persone o quelle che riguardano dati personali definiti sensibili dalla legge, salvo che si tratti di intercettazioni rilevanti ai fini delle indagini*».

Il novellato comma 4 dell'art. 268 c.p.p. prevede che «*i verbali e le registrazioni sono immediatamente trasmessi al pubblico ministero per la conservazione nell'archivio di cui all'articolo 269, comma 1. Entro cinque giorni dalla conclusione delle operazioni, essi sono depositati presso l'archivio di cui all'articolo 269, comma 1, insieme ai decreti che hanno disposto, autorizzato, convalidato o prorogato l'intercettazione, rimanendovi per il tempo fissato dal pubblico ministero, salvo che il giudice non riconosca necessaria una proroga*»[150]. La stessa disposizione, inoltre, al comma 5, prevede che «*se dal deposito può derivare un grave pregiudizio per le indagini, il giudice autorizza il pubblico ministero a ritardarlo non oltre la chiusura delle indagini preliminari*»[151], conformemente all'abrogato art. 268-*bis* c.p.p.

[150] Si veda art. 2, comma 1, lett. e, punto 3, d.l. 161/2019, all'art. 268 c.p.p.: il comma 4 è sostituito dai seguenti: «*4. I verbali e le registrazioni sono immediatamente trasmessi al pubblico ministero per la conservazione nell'archivio di cui all'articolo 269, comma 1. Entro cinque giorni dalla conclusione delle operazioni, essi sono depositati presso l'archivio di cui all'articolo 269, comma 1, insieme ai decreti che hanno disposto, autorizzato, convalidato o prorogato l'intercettazione, rimanendovi per il tempo fissato dal pubblico ministero, salvo che il giudice non riconosca necessaria una proroga.*
5. Se dal deposito può derivare un grave pregiudizio per le indagini, il giudice autorizza il pubblico ministero a ritardarlo non oltre la chiusura delle indagini preliminari.
6. Ai difensori dell'imputato è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, per via telematica hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche. Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione e di quelli che riguardano categorie particolari di dati personali, sempre che non ne sia dimostrata la rilevanza. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima.
7. Il giudice, anche nel corso delle attività di formazione del fascicolo per il dibattimento ai sensi dell'articolo 431, dispone la trascrizione integrale delle registrazioni ovvero la stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento.
8. I difensori possono estrarre copia delle trascrizioni e fare eseguire la trasposizione della registrazione su idoneo supporto. In caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono richiedere copia su idoneo supporto dei flussi intercettati, ovvero copia della stampa prevista dal comma 7».

[151] *Ibidem*

Sul funzionamento dell'archivio "digitale" dal combinato disposto dei novellati artt. 269 c.p.p.[152] e 89 bis disp. att. c.p.p.[153] si evince che lo stesso debba essere tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica e gestito con modalità tali da assicurare la segretezza della documentazione custodita e garantire il monitoraggio degli accessi. Nell'archivio digitale saranno custoditi i verbali, le annotazioni, gli atti e le registrazioni delle intercettazioni che vi permangono fino a sentenza irrevocabile, fatta salva la possibilità per gli interessati, quando la documentazione non è necessaria per il procedimento, di chiederne la distruzione al giudice che ha autorizzato o convalidato l'intercettazione[154]. Ai sensi del riformulato art 269, comma 1, c.p.p., al giudice per le indagini preliminari e ai difensori dell'imputato è consentito l'accesso per l'ascolto delle conversazioni e comunicazioni registrate[155].

---

[152] Si veda art. 2, comma 1, lett. f, d.l. 161/2019 : all'art. 269 c.p.p. il comma 1 è sostituito da seguente:« *I verbali e le registrazioni, e ogni altro atto ad esse relativo, sono conservati integralmente in apposito archivio gestito e tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica dell'ufficio che ha richiesto ed eseguito le intercettazioni. Al giudice per le indagini preliminari e ai difensori dell'imputato per l'esercizio dei loro diritti e facoltà è in ogni caso consentito l'accesso all'archivio e l'ascolto delle conversazioni o comunicazioni registrate;*
2) il comma 1-bis è abrogato;
3) il comma 2 è sostituito dal seguente: «2. Salvo quanto previsto dall'articolo 271 comma 3, le registrazioni sono conservate fino alla sentenza non piu' soggetta a impugnazione. Tuttavia gli interessati, quando la documentazione non è necessaria per il procedimento, possono chiederne la distruzione, a tutela della riservatezza, al giudice che ha autorizzato o convalidato l'intercettazione. Il giudice decide in camera di consiglio a norma dell'articolo 127».

[153]Si veda art. 2, comma 2, lett b), d.l. 161/2019: l'articolo 89-bis è sostituito dal seguente:
«Art. 89-bis (Archivio delle intercettazioni).
1. Nell'archivio digitale istituito dall'articolo 269, comma 1, del codice, tenuto sotto la direzione e la sorveglianza del Procuratore della Repubblica, sono custoditi i verbali, gli atti e le registrazioni delle intercettazioni a cui afferiscono.
2. L'archivio è gestito con modalità tali da assicurare la segretezza della documentazione relativa alle intercettazioni non necessarie per il procedimento, ed a quelle irrilevanti o di cui è vietata l'utilizzazione ovvero riguardanti categorie particolari di dati personali come definiti dalla legge o dal regolamento in materia. Il Procuratore della Repubblica impartisce, con particolare riguardo alle modalità di accesso, le prescrizioni necessarie a garantire la tutela del segreto su quanto ivi custodito.
3.All'archivio possono accedere, secondo quanto stabilito dal codice, il giudice che procede e i suoi ausiliari, il pubblico ministero e i suoi ausiliari, ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto, i difensori delle parti, assistiti, se necessario, da un interprete. Ogni accesso è annotato in apposito registro, gestito con modalità informatiche; in esso sono indicate data, ora iniziale e finale, e gli atti specificamente consultati.
4. I difensori delle parti possono ascoltare le registrazioni con apparecchio a disposizione dell'archivio e possono ottenere copia delle registrazioni e degli atti quando acquisiti a norma degli articoli 268 e 415-bis del codice. Ogni rilascio di copia è annotato in apposito registro, gestito con modalità informatiche; in esso sono indicate data e ora di rilascio e li atti consegnati in copia.»

[154] W. NOCERINO, *op. cit.*, p. 70.

[155] W. NOCERINO, *op. cit.*, p. 71.

2.7.1 L'udienza di stralcio

Il d.lgs. 216/2017 aveva provveduto all'eliminazione dell'udienza di stralcio[156] sostituendola con il meccanismo di acquisizione delle intercettazioni al fascicolo delle indagini di cui gli artt. 268-*bis*, 268-*ter* e 268-*quater* c.p.p.

Il legislatore con il d.l. 161/2019 procede all'abrogazione di queste disposizioni, ripristinando il tradizionale *iter* dell'udienza di stralcio.

Ai sensi della prima parte del comma 6 dell'art. 268 c.p.p.: «*Ai difensori dell'imputato è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, per via telematica hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche*»[157].

Da una prima lettura di questa disposizione si rileva che la facoltà di esaminare gli atti è accordata al solo rappresentante dell'imputato, unico legittimato ad operare un controllo sulla rilevanza delle intercettazioni. Una simile interpretazione dell'art. 268, comma 6, c.p.p. potrebbe comportare una contrazione del diritto delle parti di accedere agli atti e una «*menomazione del contraddittorio in fase di acquisizione che non pare coerente con la recente tendenza legislativa a irrobustire le prerogative procedimentali della persona offesa dal reato*»[158].

Una volta decorso il termine di cui ai commi 4 e 5 dell'art. 268 c.p.p., si procede all'udienza di stralcio alla quale hanno diritto di partecipare il pubblico ministero e i difensori che devono essere avvisati almeno ventiquattro ore prima. In conformità a quanto sancito nella prima parte del disposto dell'art. 268 comma 6 c.p.p., si ritiene che la presenza sia limitata ai soli difensori dell'imputato e al pubblico ministero poiché sarebbe poco coerente prevedere un intervento allargato alle altre parti private, di fatto escluse dall'esame preliminare degli atti e delle registrazioni[159].

Nel corso dell'udienza di stralcio il giudice per le indagini preliminari dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano irrilevanti. L'art. 268, comma 6, c.p.p.

---

[156] Sul tema dell'eliminazione dell'udienza di stralcio si veda *supra* § 2.5

[157] Si veda art. 2, comma 1, lett. e, punto 3 d.l. 161/2019.

[158] W. NOCERINO, *op. cit.*, p. 72.

[159] W. NOCERINO, *op. cit.*, p. 76.

riconosce, inoltre, al giudice un limitato potere di filtro, accordandogli la facoltà di procedere anche d'ufficio allo stralcio non solo delle registrazioni e dei verbali di cui è vietata l'utilizzazione, ma anche di quelli che riguardano categorie particolari di dati personali[160].

Conclusa la fase dell'acquisizione, il giudice procede, quindi, alla perizia trascrittiva disponendo la trascrizione delle registrazioni ammesse. La formulazione dell'art. 268, comma 7, c.p.p. ricalca fedelmente quella originaria del Codice dell'88. Il legislatore, tuttavia, conformemente ad una pratica propria del diritto vivente, prevede un termine ordinatorio per il giudice che può disporre la trascrizione anche nel corso dell'attività di formazione del fascicolo per il dibattimento ai sensi dell'art. 431 c.p.p.[161]. La *ratio* di questa disposizione va ricercata nella prassi per cui l'udienza di stralcio si svolge nel corso del dibattimento e solo eccezionalmente durante le indagini preliminari.

Il legislatore, pertanto, consente al giudice dell'udienza preliminare di procedere alla nomina del perito anche alla conclusione dell'udienza preliminare, anticipando così il procedimento di trascrizione prima ancora del giudizio[162]. Depositata la perizia trascrittiva, i difensori, ai sensi dell'art. 268, comma 8, c.p.p., possono estrarre copia delle trascrizioni e far eseguire la trasposizione della registrazione su un supporto idoneo. In caso d'intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono richiedere la stampa in forma intellegibile dei dati *ivi* contenuti[163].

[160] Si veda art. 2, comma 1, lett. e, punto 3 d.l. 161/2019.

[161] Si veda art. 2, comma 1, lett. e, punto 3 d.l. 161/2019.

[162] W. NOCERINO, *op. cit*., p. 75.

[163] Si veda art. 2, comma 1, lett. e, punto 3 d.l. 161/2019.

3. Le intercettazioni informatiche e telematiche

Le intercettazioni di comunicazioni informatiche o telematiche sono un mezzo di ricerca della prova di indubbia utilità perché consentono la captazione di flussi telematici di dati, informazioni e comunicazioni che si realizzano per mezzo la posta elettronica, la messaggistica istantanea e i servizi di telefonia.

L'art. 266 *bis* c.p.p. permette la captazione del flusso di comunicazioni relativo a sistemi informatici o telematici nei procedimenti concernenti i reati di cui l'art. 266 c.p.p. e in quelli relativi a reati commessi attraverso l'ausilio di tecnologie informatiche o telematiche.

Oggetto d'intercettazione *ex* art. 266 *bis* c.p.p. è qualunque attività che comporti l'invio di dati da un computer all'altro ovvero da un microprocessore ad una sua periferica[164].

Per sistema informatico s'intende «*un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche parziale) di tecnologie informatiche che sono caratterizzate, per mezzo di una attività di "codificazione" e "decodificazione", dalla "registrazione" o "memorizzazione" tramite impulsi elettronici, su supporti adeguati, di "dati", cioè, di rappresentazioni elementari di un fatto, effettuata attraversi simboli (bit) in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme più o meno vasto di informazioni organizzate secondo una logica che consente loro di esprimere un particolare significato per l'utente*»[165].

L'art. 226 *bis* c.p.p. abr. si riferiva unicamente alle intercettazioni telefoniche o telegrafiche e, grazie al rinvio di cui l'art. 623 *bis* c.p., anche quelle effettuate con collegamento su filo ad onde guidate, mentre l'art. 266 *bis* c.p.p. vigente riguarda ogni forma di telecomunicazione.

La genericità di questa disposizione, oltre a permettere il più vasto ambito di applicazione possibile, attraverso la locuzione "altre forme di telecomunicazioni" consente anche un automatico adeguamento della norma alle acquisizioni della scienza e della tecnologia nell'ambito delle telecomunicazioni[166].

---

[164] G. BUONOMO, *Profili penali dell'informatica*, Milano, 1994, p. 153.

[165] Cass. pen., sez. un., 26 marzo 2015, n.17325, in *C.e.d. Cass.*, Rv. 263020.

[166] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.*,p. 46.

Se si assume che le comunicazioni telematiche possano rientrare nella nozione di telecomunicazione di cui l'art. 266 c.p.p., la disposizione di cui l'art. 266 *bis* c.p.p nella parte in cui consente le intercettazioni nei reati di cui l'art. 266 c.p.p. sembra essere ripetitiva. Tuttavia si ritiene che il contenuto precettivo fondamentale della disposizione in esame sia la parte in cui viene estesa la possibilità di procedere ad intercettazioni nell'ambito delle indagini relative a reati commessi mediante l'uso di tecnologie informatiche o telematiche che non sono certamente ricompresi nell'elenco dell'art. 266 c.p.p.[167].

4. Intercettazioni ambientali o inter praesentes

Le intercettazioni di conversazioni tra presenti, disciplinate dall' art. 266 comma 2 c.p.p., si caratterizzano per il fatto che la conversazione captata non avviene servendosi di un particolare mezzo di diffusione del segnale, quale il telefono, ma tra persone che si trovano in uno stesso ambiente.

La captazione si realizza attraverso dispositivi tecnici, idonei a riprendere e registrare segnali sonori e visivi, che vengono collocati nell'ambiente in cui si trovano gli interlocutori, per questa ragione questa forma di intercettazione è definita "ambientale"[168].

Come per le intercettazioni ordinarie, la disciplina di cui gli artt. 266 e ss. c.p.p. è applicabile a quelle ambientali quando ricorrano tutti gli elementi che caratterizzano il concetto normativo d'intercettazione[169] e, quindi, il dialogo deve essere riservato, l'ascolto reso possibile da particolari congegni meccanici o elettronici ed il captante deve essere un soggetto terzo[170].

Le intercettazioni tra presenti *ex* art. 266, comma 2, c.p.p possono essere eseguite per tutte le categorie di reati indicati nel comma precedente della medesima disposizione qualora

[167] P. BALDUCCI, *op.cit.*, p.23.

[168] V. GIGLIO, *op. cit.*, p. 29.

[169] A.CAMON, *op.cit.*, p. 17.

[170] Si veda *supra* § 2.1.

sussistano i presupposti di cui l'art. 267 c.p.p.; ossia gravi indizi di reato e assoluta indispensabilità ai fini della prosecuzione delle indagini[171].

Il d.lgs. 216/2017 è intervenuto in maniera incisiva sul comma 2 dell'art. 266 c.p.p. prevedendo espressamente che l'intercettazione tra presenti possa realizzarsi anche mediante l'inserimento in un dispositivo elettronico portatile di un captatore informatico.

Il legislatore ha operato, in materia d'intercettazioni ambientali, una *summa divisio* a seconda che la captazione si svolga o meno in uno dei luoghi indicati dall'art. 614 c.p. Nel primo caso, oltre ai requisiti indicati nell'art. 267 c.p.p., deve sussistere «*il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa*» secondo quanto disposto dall'art. 266, comma 2, c.p.p.[172].

Questo presupposto non è richiesto nella circostanza in cui l'intercettazione domiciliare debba essere effettuata per l'accertamento dei delitti di criminalità organizzata di cui all'art. 13 d.l. n.152/1991.

Per quanto riguarda il profilo strettamente operativo di esecuzione delle intercettazioni ambientali, al fine di captare in maniera occulta le conversazioni tra soggetti presenti, la polizia giudiziaria si avvale d'apparati mobili quali ad esempio le microspie, radiospie, piccoli apparecchi di registrazione o potenti microfoni, non essendo idonei per l'esecuzione di questo tipo d'intercettazione gli strumenti installati presso le procure della Repubblica[173].

---

[171] *Ibidem.*

[172] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 59.

[173] F. CAPRIOLI, *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in *Riv. it. dir. proc. pen.*, 1991, p.171.

4.1 Intercettazioni ambientali domiciliari

La limitazione posta dall'art.266 comma 2 c.p.p. alle intercettazioni ambientali eseguite all'interno del domicilio solo nel caso in cui *ivi* si stia svolgendo l'attività criminosa trova la sua giustificazione nella necessità di tutelare oltre la libertà e segretezza delle comunicazioni di cui l'art. 15 Cost anche l'inviolabilità del domicilio di cui l'art. 14 Cost[174].

Una parte della dottrina, criticando l'introduzione dell'ulteriore presupposto dello svolgimento dell'attività criminosa per le intercettazioni ambientali domiciliari, sostiene che al diritto alla libertà e segretezza delle comunicazioni dovrebbe essere riconosciuto il medesimo grado di tutela a prescindere dal luogo nel quale si realizza la conversazione captata[175]. Mentre è necessario evidenziare come il domicilio assuma un significato diverso rispetto a quello di mera delimitazione di un ambito spaziale poiché deve essere considerato una nozione giuridica autonoma e preordinata a difendere un interesse « *i cui confini esorbitano dalla protezione accordata al diritto di proprietà* »[176].

Il presupposto richiesto dall'art. 266, comma 2, c.p.p. dello svolgimento dell'attività criminosa nei luoghi di privata dimora è ritenuto sussistente, secondo alcuni Autori, in presenza di sufficienti atti di preparazione o esecuzione di uno dei reati indicati dall'art. 266 comma 1 c.p.p. e fino a quando gli atti preparatori non raggiungono la soglia del tentativo l'intercettazione ambientale sarà preclusa[177].

Un'autorevole dottrina sostiene, inoltre, che l'articolo determinativo che precede l'espressione "attività criminosa" indica un rapporto d'identità con il fatto oggetto delle indagini e di conseguenza per lo svolgimento delle operazioni d'intercettazione non sarà sufficiente il fondato motivo di ritenere sussistente lo svolgimento di qualsiasi attività criminosa, ma deve trattarsi propriamente dell'attività per la quale sono in corso le indagini[178].

---

[174] P. BALDUCCI, *op.cit.*, p. 93.

[175] F. CAPRIOLI, *op. cit.*, p. 172.

[176] A.CAMON, *op.cit*., p. 182.

[177] G. FUMU, "*Commento all'art. 266*", in "*Commento al nuovo codice di procedura penale*", (a cura di) M. Chiavario, vol. II,, Torino, 1990, p. 778.

[178] F. CORDERO, "*Procedura Penale*", Milano, 2012, p. 840.

Da ciò ne deriva l'impossibilità di disporre le intercettazioni per reati a consumazione istantanea[179].

Tuttavia, queste opzioni interpretative non tengono conto del fatto che il legislatore nell'art. 266, comma 2, c.p.p. pone l'accento non sullo svolgimento dell'attività criminosa ma sul "fondato motivo" di ritenere sussistente quest'attività. Pertanto, la disposizione in esame non richiede che la suddetta attività debba essere effettivamente sussistente ma che attraverso un giudizio *ex ante*, nel momento dell'emanazione del provvedimento autorizzativo delle intercettazioni, ragionevolmente può ritenersi che in uno dei luoghi di cui l'art. 614 c.p. si stia svolgendo l'attività criminosa[180].

Inoltre, l'attività criminosa della quale si ritiene in corso lo svolgimento potrà essere diversa ed ulteriore da quella emersa nel corso delle indagini[181].

4.1.1 La nozione di privata dimora

Una corretta analisi della disciplina delle intercettazioni ambientali presuppone la definizione della nozione di domicilio.

La Costituzione disciplina il domicilio nell'art. 14 sancendo che «*il domicilio è inviolabile*» e «non *si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi previsti dalla legge secondo le garanzie previste dall'art. 13* », precisando, inoltre, che «*gli accertamenti e ispezioni per motivi di sanità ed incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali*». Sebbene detta clausola costituzionale non definisca espressamente il domicilio, l'art.14 Cost. deve essere interpretato nel senso di garantire la tutela costituzionale non soltanto al luogo nel quale un soggetto ha stabilito la sede principale dei suoi interessi[182],ma anche ogni altro luogo in cui la persona riesca ad isolarsi dal mondo esterno, al fine di evitare ogni forma

[179]F. CORDERO, *Ibidem.*

[180] P. BALDUCCI, *op.cit.*, p. 98.

[181] Cass. pen., sez. VI, 21 novembre 1997, n. 4533, Avantaggiato, in *C.e.d. Cass.*, Rv.210316

[182] Cfr. art. 43, comma 1, c.c. «Il domicilio di una persona è nel luogo in cui essa ha stabilito la sede principale dei suoi affari e interessi».

d'intrusione nella sua sfera privata spazialmente delimitata dove può svolgere in piena riservatezza e senza interferenze esterne ogni attività individuale e collettiva[183].

L'art. 614 c.p. a cui fa riferimento l'art. 266, comma 2, c.p.p. punisce la condotta di chi «*s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo*» e pertanto, identifica il domicilio con "l'abitazione altrui", "la privata dimora" e le "appartenze".

Per quanto riguarda l'individuazione dei luoghi a cui fa riferimento l'art. 614 c.p. sussiste una ricca casistica giurisprudenziale ed elaborazione dottrinale che permette di risolvere i dubbi interpretativi concernenti la locuzione privata dimora[184].

Un primo elemento che consente di specificare questo concetto è il tempo di permanenza di un soggetto in determinato luogo che, anche non sostanziandosi in un soggiorno duraturo, deve presentare un pur minimo grado di stabilità [185].

Sul tempo di permanenza una questione controversa affrontata dalla Corte di cassazione riguarda la riconducibilità dell'abitacolo di un veicolo al concetto di privata dimora.

Privilegiando il presupposto della stabilità in un determinato luogo la Corte ha ritenuto che « *l'abitacolo non può considerarsi luogo di privata dimora, in quanto sfornito dei confort necessari minimi per potervi risiedere in modo stabile* »[186] e neppure può essere considerata un'appartenenza di privata dimora in quanto non è collegato da un rapporto funzionale di accessorietà o di servizio con la stessa[187]. Per contro analizzando il profilo della funzione adempiuta dal luogo in questione, la Corte, in un'altra pronuncia, ha esteso all'abitacolo dell'autovettura il concetto di privata dimora evidenziando che il mezzo di trasporto può essere adibito all'espletamento di attività strettamente personali come ad esempio riposo, alimentazione, svago o può essere utilizzato per svolgere un'attività lavorativa, con la conseguente applicabilità della disciplina prevista dall'art. 266, comma

[183] T. MARTINES, *Diritto Costituzionale*, Milano, 2010, p.550.

[184] P. BALDUCCI, *op.cit.*, p 19.

[185] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 61.

[186] Cass. pen., sez.I ,22 Gennaio 1996, n.1904, Porcaro, in *C.e.d. Cass.*, Rv. 203799.

[187] *Ibidem.*

2, c.p.p.[188]. Da questa pronuncia si evince che un luogo può essere adibito a privata dimora a prescindere dalla sua abitabilità.

Una volta riconosciuto che la funzione assolta da un luogo di privata dimora è proteggere la vita privata del titolare, permettendogli di svolgere tutte quelle attività strettamente personali (riposo, alimentazione ecc.), risulta con chiarezza che non tutti i luoghi rispetto ai quali al titolare è riconosciuto il diritto di escludere terzi estranei non graditi costituiscono una privata dimora perché lo *jus exludendi alios ex* art. 614 c.p. è funzionale a tutelare il diritto alla riservatezza nell'espletamento di alcune manifestazioni della vita privata della persona[189]. Seguendo questa impostazione non costituisce una privata dimora il deposito di una società commerciale, al quale accedono un numero indiscriminato di persone, tranne che nelle ore di chiusura quando il titolare può svolgere attività di indole privata[190].

Controversa in giurisprudenza è la possibilità di ricondurre alla nozione di privata dimora la *toilette* di un bagno pubblico. Un primo orientamento giurisprudenziale risolve negativamente la questione reputando che in questo caso non sussista un rapporto di stabilità tra il luogo e il soggetto che ne usufruisce[191].

Un secondo orientamento sostiene che la tutela costituzionale dell'inviolabilità del domicilio si estende a tutti quei luoghi che consentono sia una temporanea disponibilità degli stessi sia un'area di intimità e riservatezza. Pertanto, chi usufruisce di una toilette di un bagno pubblico non rinuncia alla propria riservatezza e può anche temporalmente opporsi all'ingresso di altri soggetti: da ciò ne discende che al bagno pubblico deve essere riconosciuta la medesima tutela della privata dimora[192].

Per contro le Sezioni unite, in una importante decisione concernente la videoregistrazione di comportamenti comunicativi in ambito domiciliare, hanno evidenziato che il concetto

[188] Cass.pen., sez. I, 3 Marzo 1997, n. 3901, Telese, in *C.e.d. Cass*., Rv. 207379.

[189] Cass., sez. I, 20 dicembre 1991, n. 5032, Marsella, in *C.e.d. Cass*., Rv.190009.

[190] C.DI MARTINO-T.PROCACCIANTINI, *op. cit.* p. 62.

[191] Si veda Cass. pen., sez.VI, 10 gennaio 2003, n. 3443, Mostra, in *C.e.d. Cass*., Rv. 224743; allo stesso modo Cass. pen., sez.VI, 10 gennaio 2003, n.6962, Cherif Ahmed, in *C.e.d. Cass*., Rv. 223733 e Cass. pen., sez. VI, 19 novembre 2005, n. 11654, Siciliano, in *C.e.d. Cass*., Rv. 233689.

[192] Cass.pen., sez. IV, 16 marzo 2000, n.7063, Viskovic, in *C.e.d. Cass*., Rv. 217688.

di domicilio non può coincidere con ogni ambiente, come il bagno pubblico, idoneo a garantire intimità e riservatezza[193].

Il domicilio sicuramente è espressione di un rapporto tra la persona e un luogo, generalmente chiuso, in cui si svolge la vita privata ed è idoneo a garantire la riservatezza; si ritiene, però, che la relazione tra il titolare e il suddetto luogo deve essere tale da giustificare la tutela anche quando la persona è assente. Da ciò ne discende che la toilette non può essere considerata un domicilio neppure nel tempo in cui è occupata da una persona perché chiunque può entrare in un bagno pubblico, quando è libero. Di conseguenza la polizia giudiziaria può accedervi indipendentemente dalla sussistenza delle condizioni che legittimano le attività ispettive[194].

È proprio dopo queste considerazioni che la Corte ha evidenziato come il tratto caratterizzante la privata dimora sia la stabilità in quanto « *è solo questa, anche se intesa in senso relativo, che può trasformare un luogo in un domicilio, nel senso che può fargli acquistare autonomia rispetto alla persona che ne ha la titolarità*»[195].

Al fine di fornire alla nozione di privata dimora un maggior grado di chiarezza le Sezioni unite della Cassazione sono intervenute in una recentissima sentenza[196], per risolvere la questione della riconducibilità o meno alla nozione di privata dimora dei luoghi di lavoro.

La Corte in questa decisone ha enucleato tre criteri che devono necessariamente sussistere affinché si possa parlare di privata dimora: l'utilizzazione del luogo per lo svolgimento della vita privata (riposo, svago, alimentazione, lavoro ecc.), una durata apprezzabile del rapporto tra il luogo e la persona che deve essere connotato da stabilità e non da mera occasionalità ed infine l'impossibilità per i terzi di accedere al suddetto luogo senza il consenso del titolare.

Una volta chiariti i presupposti che devono sussistere affinché si possa parlare di privata dimora le Sezioni unite, risolvendo la questione concernente i luoghi di lavoro, evidenziano che rientrano nella nozione di privata dimora esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente

[193] Cass. pen. sez.un., 28 Marzo 2006, n.26795, Prisco, in *C.e.d. Cass.*, Rv. 234270.

[194] *Ibidem*

[195] *Ibidem*

[196] Cass. pen. sez.un., 23 Marzo 2017, n.31345, *C.e.d. Cass*., Rv. 270076.

atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare[197].

5. Le videoriprese investigative

Il termine videoripresa indica la registrazione, per mezzo di strumenti di captazione visiva, di quanto accade in un luogo all'insaputa dei soggetti che si trovano in esso ; le videoriprese possono essere eseguite sia in un luogo pubblico che in un luogo di privata dimora[198].

Nonostante sussistano delle affinità tra le riprese effettuate dai "privati" e quelle investigative, sia per l'utilizzo di identici strumenti di captazione, sia per quanto riguarda il materiale rappresentativo ricavato dall'esecuzione delle stesse, le videoregistrazioni effettuate dai privati si connotano per non perseguire direttamente la finalità di accertamento dei reati ed inoltre il privato, sotto il profilo soggettivo, è del tutto estraneo all'attività della polizia giudiziaria. Pertanto, proprio la loro estraneità al procedimento penale, in quanto prove precostituite rispetto allo stesso, permette di inquadrare le videoriprese eseguite da privati nell'ambito della "prova documentale" *ex* art. 234 c.p.p., sia che la ripresa venga eseguita in uno spazio pubblico, sia che venga effettuata in un luogo di privata dimora[199]. Tanto è vero che l'art. 234, comma 1, c.p.p consente non esclusivamente l'acquisizione di scritti ma anche di «*altri documenti che rappresentano fatti, persone o cose, mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo*».

Se l'individuazione della disciplina processuale applicabile non suscita particolari problemi per quanto riguarda le videoriprese effettuate da privati, molto più complesso è il regime delle videoriprese eseguite dalla polizia giudiziaria con finalità investigative.

La videosorveglianza investigativa si rivela uno strumento particolarmente utile al fine dell'accertamento dei reati perché è dotata di un'altissima capacità dimostrativa degli elementi di cui consente la raccolta.

---

[197] *Ibidem.*

[198] P .TONINI, *op. cit.*, p.421.

[199] A.SCALFATI, *Le indagini atipiche*, Torino, 2014, p.143.

In molti casi questo potente strumento di ricerca della prova ha sostituito il vecchio "appostamento" che richiedeva notevoli risorse, un numero consistente di operatori e soprattutto presentava un alto rischio di essere scoperti. Oggi, invece, è sufficiente predisporre una o più telecamere i cui segnali vengono automaticamente trasmessi ad un ufficio, dove la polizia giudiziaria, con ulteriori ausili tecnici, potrà controllare ogni movimento dell'indagato[200].

In assenza di un'espressa disciplina legislativa, le videoriprese sono state oggetto di numerosi interventi da parte della Corte costituzionale e della Corte di cassazione.

In materia una pronuncia cardine è rappresentata da una sentenza interpretativa di rigetto[201] con la quale la Corte costituzionale ha dichiarato l'infondatezza della questione di illegittimità costituzionale concernente gli artt. 189 e da 266, 266 *bis*, 267, 268, 270 e 271 c.p.p. in relazione agli artt. 3 e 14 Cost.

In questa decisione la Corte ha elaborato la distinzione fondamentale tra videoregistrazioni dirette a captare atti di natura comunicativa (ad esempio due soggetti che avendo il timore di essere sottoposti ad intercettazione ambientale con microspie acustiche comunicano a gesti) e comportamenti non diretti all'intenzionale trasmissione di messaggi. Nel primo caso, secondo la Corte si è in presenza di una limitazione del diritto alla libertà e segretezza delle comunicazioni di cui l'art. 15 Cost. e dovrà, di conseguenza, essere applicata la disciplina delle intercettazioni di cui gli artt. 266 e ss c.p.p. perché si è in presenza di una forma d'intercettazione «*che si differenzia da quella operata tramite gli apparati di captazione sonora solo in rapporto allo strumento tecnico di intervento*»[202]. Qualora ,poi, la videoripresa di atti avente natura comunicativa dovesse realizzarsi all'interno di un domicilio si applicherà la disciplina di cui l'art. 266 comma 2 c.p.p. concernente le intercettazioni ambientali domiciliari[203].

La Corte di cassazione nelle successive pronunce ha accolto la distinzione operata dalla Corte costituzionale tra comportamenti aventi natura comunicativa e non; un intervento

---

[200] A. MANGANELLI-F. GABRIELLI, *Investigare. Manuale pratico delle tecniche d'indagine*, Padova, 2007, p. 150.

[201] Cort. cost., 24 aprile 2002, n.135 in www.giustcost.org

[202] I*bidem*.

[203] Si veda. *supra* § 3.1.

fondamentale in materia è rappresentato dalla sentenza Prisco[204] nella quale le Sezioni unite, ribadendo quanto prospettato dalla Corte costituzionale, precisano che quando l'intercettazione audiovisiva si realizza all'interno del domicilio si applicherà la disciplina di cui l'art. 266,comma 2, c.p.p. e potrà, di conseguenza, essere disposta solo se sussiste in fondato motivo che *ivi* si stia svolgendo l'attività criminosa. Per contro in tutti gli altri luoghi si seguirà la disciplina ordinaria delle intercettazioni.

Per quanto riguarda, invece, la videoregistrazione di comportamenti non comunicativi la Consulta perviene ad una tripartizione a seconda che si realizzi in luoghi domiciliari, pubblici o riservati. Se l'intercettazione di comportamenti non diretti all'intenzionale trasmissione dei messaggi si realizza all'interno del domicilio, protetto dal disposto dell'art. 14 Cost. che ne sancisce l'inviolabilità, in assenza di una espressa disciplina legislativa le videoriprese saranno inutilizzabili e non potranno essere acquisite al procedimento come prove atipiche *ex* art. 189 c.p.p., non potendo rientrare in questa categoria di prove quelle fondate su un'attività vietata dalla legge[205].

Nel caso della *toilette* di un locale pubblico o il *privé* di una discoteca, si tratta di luoghi che, secondo le Sezioni unite, per difetto del requisito di stabilità[206] non rientrano nella nozione di domicilio ma, nonostante ciò, sono caratterizzati da un'aspettativa di riservatezza maggiore rispetto ai luoghi pubblici.

In questo caso la norma di riferimento è l'art. 2 della Cost. che protegge la riservatezza e non l'art. 14 Cost. La Costituzione, infatti, non riconosce al diritto alla riservatezza una tutela analoga a quella apprestata dall'art. 14 Cost. per il domicilio e in assenza di una specifica disciplina legislativa le videoriprese di comportamenti non comunicativi che lo sacrificano saranno suscettibili di utilizzazione a norma dell'art. 189 c.p.p. [207].

L'ultima categoria di luoghi individuata dalla Corte nella sentenza Prisco[208] sono i luoghi pubblici rispetto ai quali non sussiste alcuna aspettativa di riservatezza: qui le

---

[204] Cass. pen. sez.un., del 28 Marzo 2006, n.26795, Prisco.

[205] A.SCALFATI, *op.cit.*, p.153.

[206] Si veda *supra* § 4.1.1.

[207] Cass. pen. sez.un., 28 Marzo 2006, n.26795, Prisco.

[208] *Ibidem.*

videoriprese possono essere effettuate liberamente dalla polizia giudiziaria e utilizzabili come prova atipica *ex* art. 189 c.p.p. [209].

La Corte costituzionale è, poi, intervenuta nuovamente sul tema delle videoregistrazioni di mere immagini effettuate nei luoghi domiciliari introducendo un ulteriore elemento discretivo[210]. Secondo il giudice delle leggi affinché operi la protezione di cui l'art. 14 Cost. non basta che un certo comportamento si realizzi all'interno di un luogo di privata dimora ma è necessario che esso si realizzi con modalità tali da non renderlo visibile a terzi. Di conseguenza quando l'azione pur svolgendosi in luoghi di privata dimora viene liberamente osservata da terzi estranei (come nel caso della persona che si pone sul balcone prospiciente la strada ed è osservata dai passanti senza che si debba ricorrere a telecamere munite di zoom) le videoriprese sono sottoposte alla medesima disciplina di quelle effettuate in luoghi pubblici e saranno, quindi, liberamente disposte dalla polizia giudiziaria e utilizzabili come prova atipica[211].

Secondo la Corte, quindi, le videoriprese investigative all'interno del domicilio sono tali se necessitano di strumenti che consentano di superare una barriera che si frappone tra la generalità dei consociati e l'attività filmata. Invece, nella circostanza in cui la condotta ripresa sia accessibile visivamente da chiunque, senza ricorrere a particolari dispositivi tecnici per la captazione, si è fuori dall'ambito di tutela prefigurato dall'art.14 Cost[212].

[209] Cass. pen., sez. II, 24 aprile 2007, n. 35300, Caruso, in *C.e.d. Cass.*, Rv. 237848.

[210] Corte Cost., 7 maggio 2008, n.149 in www.giustcost.org

[211] *Ibidem.*

[212] *Ibidem.*

Capitolo II

IL TROJAN HORSE COME STRUMENTO D'INDAGINE

SOMMARIO: 1. Le indagini informatiche. – 2. Il *trojan horse*: sistema informatico di controllo remoto. – 3. Tutela della privacy dell'utente nei sistemi di messaggistica istantanea. – 3.1 Intercettazioni di comunicazioni mediante captatore informatico. – 4. Ulteriori impieghi investigativi dei "*remote control system*". – 4.1 Uso del virus *trojan horse* in funzione *Keylogger*, *Screenshot* e *Screencast*. – 4.2 Definizione di "perquisizioni *on line*" e inquadramento nei mezzi tipici di ricerca della prova previsti dal c.p.p. – 4.2.1 Le perquisizioni *on line* come mezzo atipico di ricerca della prova *ex* art.189 c.p.p. – 4.2.2 La perquisizione on line e il domicilio informatico. – 4.2.3 Considerazioni conclusive sul tema delle perquisizioni *on line*.– 5. Il *trojan horse* nell'esperienza europea.

1. *Le indagini informatiche*

La scienza e la tecnologia sono diventati elementi imprescindibili per la quotidianità di ciascun individuo, condizionandone vari aspetti.

Lo sviluppo tecnologico è inarrestabile ed ha determinato cambiamenti radicali in ogni settore della vita umana sul piano sociale, culturale ed economico.

Uno degli aspetti più significativi nei quali si può cogliere l'ingerenza della tecnologia nella vita di ogni persona è il settore specifico delle comunicazioni in relazione al quale l'avvento di strumenti quali *WhatsApp*, *Skype* e *Facebook* ha ridotto notevolmente le distanze tra gli individui che oggi possono relazionarsi con un'immediatezza e una velocità sorprendenti.

Ne consegue che si può affermare, senza alcun dubbio, che ciascun individuo è munito di due identità, non sempre coincidenti: un'identità digitale che si estrinseca nei *social networks* e nell'uso spesso compulsivo del *personal computer* e dello *smartphone*, e un'identità reale.

Alla luce di queste considerazioni è tangibile come la rivoluzione tecnologica influisca ed abbia un impatto decisivo sia sulla tipologia delle condotte criminose che in concreto possono essere messe in atto dagli individui, sia sullo sviluppo di nuovi strumenti investigativi per la ricerca delle prove.

Per quanto riguarda il primo aspetto, con il termine *computer crimes*[213] si fa riferimento a quella tipologia di reati nei quali il sistema informatico[214] rappresenta uno degli elementi costitutivi dell'illecito, come ad esempio l'accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.) ovvero la frode informatica (art. 640-*quinquies* c.p.).

Oltre che come elementi costitutivi della fattispecie incriminatrice, gli strumenti informatici o telematici in concreto possono essere utilizzati per agevolare la realizzazione di numerosi reati. Si pensi, ad esempio, alla diffusione di materiale pedopornografico *on line* o alle attività preparatorie di un attentato terroristico che trovano nella rete internet un validissimo ausilio per la pianificazione dell'attacco[215].

L'innovazione tecnologica, quindi, ha avuto un ruolo determinante nello sviluppo della "criminalità informatica", categoria che annovera una molteplicità di fattispecie incriminatrici realizzate attraverso la rete internet o con strumenti informatici e telematici e che, se pur non definita giuridicamente, compare in una pluralità di fonti europee e sovranazionali come la Convenzione sul *Cybercrime* disposta dal Consiglio d'Europa e

---

[213] I cd. *computer crimes* sono stati introdotti dalla legge 23 dicembre 1993, n.547, recante modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, su cui poi è intervenuta la legge 18 Marzo 2008, n.48.

[214]Si veda art 1 Convenzione del Consiglio d'Europa sulla criminalità informatica di Budapest del 23 novembre 2001: «*il "sistema informatico" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*».

[215] R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet,* in *Dir. pen. cont.*, 20 settembre 2012, p.6.

adottata a Budapest in data 23 novembre del 2001, ratificata dal nostro paese con la legge 18 Marzo 2008, n.48 [216].

Tra i molteplici obiettivi perseguiti dalla Convenzione di Budapest principale era quello di uniformare la disciplina delle fattispecie di reato di diritto penale sostanziale, connesse con la *cyber* criminalità, previste nei singoli ordinamenti degli Stati aderenti. Questo importante strumento di diritto uniforme, inoltre, ha innovato le procedure penali dei paesi sottoscrittori, in modo tale da assicurare l'efficacia delle indagini relative all'accertamento dei *computer crimes* e di tutti quei reati commessi con l'ausilio di mezzi di informatici e telematici[217] .

Infatti, le innovazioni introdotte da questa Convenzione nel nostro ordinamento hanno determinato: una riorganizzazione dei cd. reati informatici anche mediante l'elaborazione *ex novo* di specifiche fattispecie incriminatrici; l'introduzione di una forma di responsabilità amministrativa da reato dell'ente *ex* dlgs.231/2001 nell'ipotesi di commissione di un illecito informatico; la modifica dell'art 132 del d.lgs. 196/2003 in tema di *data retention*[218] ed infine, e questo è l'aspetto più rilevante, sono state introdotte numerose modifiche del Codice di procedura penale relative all'acquisizione della prova in ambiente informatico o telematico e all'utilizzo degli strumenti di acquisizione della stessa[219]. Si pensi, ad esempio, per quanto riguarda la modalità di acquisizione della prova

---

[216] R. FLOR , *ibidem*.

[217] A.CAJANI-G.COSTABILE, *Gli accertamenti informatici nelle investigazioni penali : una prospettiva europea, Information Technologies in the criminal investigation : a European perspective,* Forlì, 2011, p.19.

[218] Si veda art.132 d.lgs. 196/2003 comma 4 *ter* : « *Il Ministro dell´interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell´Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell´articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi*.».

[219] F. BRAVO, *Indagini informatiche e acquisizione della prova nel processo penale*, in *Criminologia, Vittimologia e Sicurezza*,2010, 4, p. 232.

informatica, alle ispezioni e perquisizioni di sistemi informatici e telematici disciplinate dagli artt. 244, comma 2, e 247, comma 1-*bis*, c.p.p. che richiedono l'adozione di misure tecniche idonee a conservare i dati originali e ad impedirne l'alterazione.

Da queste considerazioni emerge come lo scenario investigativo risulti essere radicalmente cambiato, in quanto gli organi inquirenti si confrontano sempre più frequentemente con mezzi di ricerca della prova di matrice informatica , basti pensare al "captatore informatico" o "*trojan horse"* [220], un virus che una volta installato, furtivamente, all'interno di un sistema informatico consente di controllare da remoto il dispositivo infettato, di accedere alla memoria e di gestirne a distanza tutte le periferiche (microfono e videocamera).

Il captatore informatico è, quindi, uno strumento di indubbia utilità per l'esecuzione delle indagini, perché consente di eseguire intercettazioni, perquisizioni e il sequestro a distanza dei dati memorizzati nel dispositivo bersaglio.

La Polizia Giudiziaria si avvale sempre più frequentemente di strumenti informatici tecnicamente così avanzati che, come il captatore, risultano molto utili per l'accertamento e la repressione dei reati, tuttavia è lecito domandarsi se il loro utilizzo, così invasivo della sfera individuale, sia compatibile con i diritti e le libertà garantiti dalla Costituzione.

In effetti uno svantaggio delle indagini informatiche è quello di non permettere un accesso selettivo ad informazioni esclusivamente rilevanti per l'accertamento del reato, poiché nell'espletamento delle indagini, gli organi inquirenti entrano in contatto con una moltitudine di dati, con il rischio che si determini un pregiudizio alla riservatezza dell'indagato.

Le indagini informatiche possono essere suddivise in due categorie a seconda della conoscibilità o meno dell'atto investigativo: le indagini cd. palesi che ricomprendono tutte quelle attività investigative effettuate fisicamente su supporti materiali di memorizzazione di dati come le perquisizioni, i sequestri, le ispezioni, rilievi e accertamenti urgenti; le indagini occulte (o segrete) che permettono l'acquisizione telematica del dato digitale che viene colto nella sua dimensione dinamica come il

[220]Si veda *infra* § 2.

pedinamento elettronico, le indagini *under cover on line,* il monitoraggio di siti, *cloud computing*[221]*, l'Osint*[222] ed infine il captatore informatico[223].

Il ricorso da parte dell'organo inquirente a questi sofisticati strumenti di ricerca della prova consente la raccolta di tutti quei dati che, essendo memorizzati sia nei dispositivi personali (smartphone e *personal computer*) sia nelle piattaforme digitali (socialnetworks, siti di *e-commerce* e mappe *on line*), costituiscono il patrimonio informativo della persona.

Da ciò ne consegue che le indagini informatiche, ammettendo l'acquisizione indiscriminata e automatica di dati inerenti alla persona, sono dotate di un carattere proattivo rivolto tanto alla repressione dei reati quanto all'analisi di dati per la ricerca delle notizie di reato[224].

---

[221] La *digital forensic* del *cloud computing* è una disciplina che studia il crescente utilizzo di reti, computer e dispositivi di memorizzazione digitale impiegati in infrastrutture cloud, sfruttati per attività criminali *hi tech* e tradizionali. Secondo la definizione del *National Institute of Standards and Tecnology* (NIST), il *cloud computing* è un modello che fornisce un accesso rapido e pratico *on demand,* via internet a un gruppo di infrastrutture condivise che può essere rilasciato con la minima interazione del fornitore. In www.sicurezzaegiustizia.com

[222] *OSINT*, acronimo di *Open Source Intelligence*, è una disciplina strettamente collegata al mondo della *cyber intelligence*, e rappresenta la raccolta notizie che devono essere trasformate in "conoscenza", attraverso fasi di validazione, di conferma e di attribuibilità certa della cosiddetta fonte di diffusione. In www.sicurezzaegiustizia.com

[223] M. TORRE, *Il Captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali,* Milano, 2017, p.11.

[224] G. GIOSTRA-R. ORLANDI, *op.cit.* p.212.

2. Il Trojan Horse: sistema informatico di controllo remoto

Il captatore informatico è conosciuto con il nome di "*trojan horse"* o cavallo di Troia che esemplifica al meglio la natura decettiva di questo *software*[225], all'apparenza utile per l'utente che viene indotto, tramite un abile stratagemma, ad installarlo nel proprio computer.

Il *trojan horse* è, prima di ogni altra cosa, un virus[226] che appartiene al più ampio *genus* dei *malware,* un termine che indica in maniera generica qualsiasi *software* preordinato a danneggiare un computer, i dati appartenenti agli utenti e qualsiasi sistema informatico sul quale viene eseguito.

Il captatore informatico consente di controllare da remoto ogni singola funzione del dispositivo bersaglio.

Più nel dettaglio, è possibile eseguire una classificazione di tutte le operazioni intrusive in tre gruppi: le attività preordinate ad acquisire le informazioni scambiate sul dispositivo, le operazioni volte a controllarne l'*hardware*[227]ed infine le attività per il controllo dei contenuti (cartelle e *file).*

Nel primo gruppo sono comprese tutte quelle attività che permettono di acquisire ogni tipo d'informazione digitale presente nel dispositivo: *e-mail*, *chat*, immagini, video, documenti e telefonate sia in entrata che in uscita. Mentre nel secondo gruppo rientrano tutte le operazioni che consentono di prendere il controllo dell'*hardware* del dispositivo infettato trasformandolo in una vera e propria microspia ambientale idonea a registrare le conversazioni che si svolgono in prossimità dell'apparato infettato, di fotografare e riprendere l'ambiente circostante. Infine, fanno parte del terzo gruppo di operazioni intrusive tutte quelle attività che permettono di modificare lo stato del dispositivo, ad esempio cancellando i *file ivi* contenuti o inserendone di nuovi[228].

---

[225] Per *software* s'intende l'insieme dei programmi che consentono il funzionamento di un computer (si contrappone a *hardware*, che designa la pura macchina). In www.andreaminini.com

[226] Per virus s'intende un programma che comincia a diffondersi nel dispositivo bersaglio all'insaputa dell'utente che lo ha inavvertitamente installato sul proprio computer. In www.andreaminini.com

[227] Per *hardware* s'intende l'insieme delle componenti fisiche, non modificabili (alimentatori, elementi circuitali fissi, unità di memoria, ecc.), di un sistema di elaborazione dati (in contrapposizione a *software*). In www.andreaminini.com

[228] G. ZICCARDI, *Parlamento Europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Archivio Penale*,2017, 1, p. 247-248.

Il dato caratterizzante il *trojan horse,* dal quale emerge l'evidente utilità investigativa di questo strumento, è la "remotizzazione", vale a dire la possibilità di estrapolare tutti i dati contenuti nel dispositivo bersaglio "a distanza", senza che sia necessario per gli investigatori essere fisicamente nelle vicinanze o, comunque, nel raggio d'azione del dispositivo nel quale viene inoculato il virus.

Il captatore informatico permette di manovrare a distanza il dispositivo, detto *target,* sul quale viene installato attraverso un'architettura di tipo *client/server,* vale a dire un modello di comunicazione e di suddivisione dei compiti tra gli utenti (*client*) di una rete di calcolatori e uno o più calcolatori (*server*) che distribuiscono informazioni o offrono servizi applicativi.

Quando il virus *trojan* viene inoculato in un dispositivo, il *server* si installa nel sistema informatico bersaglio aprendo una *backdoor,* una sorta di "porta di servizio" che permette ad un soggetto, tramite il programma *client,* di accedere ed intervenire da remoto sul dispositivo *target*.

Il *client,* definito anche *controller,* consente di eseguire sul *target* qualsivoglia operazione intrusiva, persino la rimozione definitiva del *server*.

Il *trojan horse* può essere inoculato in un sistema informatico a distanza, per mezzo di programmi ingannevoli, oppure mediante un intervento tecnico diretto sul dispositivo qualora se ne abbia la disponibilità fisica. Nel primo caso l'utente può venire indotto, ad esempio, ad aprire l'allegato di una mail contenente informazioni note e utili, oppure il virus può essere inoculato nel sistema tramite il *download* di un aggiornamento di sicurezza o tramite un semplice *screensaver*.

Questi espedienti che, traendo in inganno l'utente, permettono l'installazione del virus nel dispositivo bersaglio, possono essere propriamente definiti «*tecniche di ingegneria sociale*»[229].

Per comprendere in maniera efficace il funzionamento del virus si può far riferimento, a titolo esemplificativo, al caso in cui quest'ultimo venga inoculato in uno *smartphone*, mediante il *download* di un allegato di una mail apparentemente inoffensiva per l'utente, al fine di eseguire un'intercettazione.

[229] M. ZONARO, *Il Trojan: Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento d'intercettazione*, in *Parola alla Difesa*, 2016, 1, p. 165.

Il cellulare è munito di una serie di parti come la fotocamera o il microfono che sono componenti *hardware* e funzionano interagendo tramite il sistema operativo, il *trojan* s'inserisce a livello del sistema operativo, permettendo all'*hacker* di accendere da remoto la fotocamera, di registrare video, scattare foto e anche di aggiungere o rimuovere dati dal dispositivo infettato.

Il *trojan,* a differenza di altri virus, non si propaga nei file contenuti nel *target* o negli altri dispositivi che entrano in contatto con esso, ma si limita a consentire ad un soggetto, tramite una semplice connessione internet, di controllare qualsiasi aspetto del dispositivo bersaglio, mentre l'ignaro utente continuerà ad usare il proprio computer normalmente. Tanto è vero che una volta che viene eseguito il programma che occulta il virus, il *server* si installa automaticamente mentre il programma che funge, per così dire, "da cavallo" continua a funzionare normalmente, svolgendo tutte le operazioni e funzioni che l'utente si aspetta da quest'ultimo.

La forza intrusiva del *trojan* è determinata, quindi, proprio dal fatto che il programma installato nel dispositivo, funzionando in maniera corretta, non genera nell'utente il dubbio che il sistema sia stato compromesso.

Ciò che permette al captatore informatico di insediarsi furtivamente in un dispositivo è il fatto che in rete la trasmissione di dati avviene secondo un sistema di "impacchettamento" (c.d. tecnica di "commutazione di pacchetto"): la comunicazione viene suddivisa in diverse parti (i pacchetti) e ogni pacchetto risulta inserito in rete in maniera autonoma per essere poi ricongiunto agli altri pacchetti al momento della ricezione da parte del destinatario della comunicazione. La trasmissione dei pacchetti si realizza per mezzo di "protocolli di comunicazione" adottati dalle diverse applicazioni che sfruttano la rete *Internet* per veicolare le comunicazioni.

Ogni singolo pacchetto contiene l'indicazione dell'indirizzo IP[230] del destinatario e del mittente di questi specifici dati.

Gli sviluppatori dei *virus trojan* fanno sì che tra il dispositivo infettato e il *server* ricevente s'interpongano una serie di altri *server,* detti *Proxy,* che occultano l'I.P. del server dell'*hacker*[231].

---

[230] Per IP s'intende *internet protocol address,* un'etichetta numerica che identifica univocamente un dispositivo detto *host* collegato a una rete informatica che utilizza *l'Internet Proto*col come protocollo di rete. In www.andreaminini.com

[231] M. ZONARO, *op.cit*., p. 166.

Per poter eseguire tutte queste operazioni preordinate all'inoculazione del virus, è necessario disporre di strumenti tecnologici all'avanguardia e di ingenti investimenti di capitale, ragion per cui risulterebbe difficile affidare la gestione esclusiva alla polizia giudiziaria poiché sarebbe necessario creare specifici reparti muniti di personale altamente specializzato. Una soluzione potrebbe essere quella di affidare la ricerca e lo sviluppo del *trojan* ad aziende private [232].

Basti pensare che l'esecuzione di un'intercettazione tramite il *trojan* richiede una serie di operazioni preventive, come lo studio del soggetto nei cui confronti è disposta la captazione, in modo da poter attuare la tecnica di "ingegneria sociale" più adeguata per riuscire, ad esempio, a persuaderlo ad aprire l'allegato di una *mail* a lui indirizzata, consentendo così al *server* di installarsi nel dispositivo bersaglio.

Il legislatore nell'ambito della riforma del regime delle intercettazioni introdotta dalla Legge 103/2017 ed affidata al Governo per l'attuazione di dettaglio, ha tenuto conto solo in parte della complessità e dell'alto grado di specializzazione richiesto per l'utilizzo del *trojan horse* nelle indagini. Tanto è vero che l'art.4 del d.lgs. 216/2017[233] ha aggiunto un inciso al comma 3-*bis* dell'art.268 del c.p.p. permettendo all'ufficiale di Polizia giudiziaria, impegnato ad eseguire attività d'intercettazione con il captatore informatico su dispositivi elettronici portatili, di avvalersi dell'ausilio di persone munite di specifiche competenze tecniche limitatamente, però, alle fasi di avvio e cessazione delle registrazioni[234]. La ragione di questa limitazione che permette la collaborazione di esperti solo in fasi predeterminate dell'attività captativa deve essere ricercata nella necessità di prevenire il più possibile il rischio che soggetti estranei abbiano accesso ai dati dell'intercettazione e possano, quindi, abusare delle loro conoscenze[235].

Nonostante la cooperazione tra pubblico e privato nell'ambito della *cyber-security* sia un risultato promosso e auspicato dall' Unione Europea[236] occorre evidenziare come una

---

[232] M. ZONARO, *ivi*, p.167.

[233] Decreto legislativo 29 dicembre 2017, n.216, Disposizioni in materia d'intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'art.1, commi 82,83 e 84, lettere *a), b),c),d)* ed *e),* della legge 23 giugno 2017, n.103.

[234] Sul tema cfr. *infra* Cap. III § 3.1.

[235] V.GIGLIO, *Manuale delle intercettazioni, il nuovo regime normativo, i principi e la giurisprudenza*, Bologna, 2018, p.92.

simile forma d'interazione necessiti la predisposizione di una struttura con un basso grado di complessità, in modo da ingenerare nei soggetti coinvolti una relazione di fiducia basata sulla predisposizione di meccanismi di controllo reciproco.

Questa esigenza diventa ineludibile quando oggetto di cooperazione è l'utilizzo e lo sviluppo di uno strumento d'indagine così invasivo quale il *trojan horse,* si pensi alla circostanza in cui una simile tecnologia di *spyware* venga acquistata da imprese private che non agiscono come garanti dell'interesse nazionale ma operano secondo logiche di mercato.

Sebbene sia, quindi, auspicabile una *patnership* pubblico-privata per la gestione del captatore informatico, non si può prescindere dalla necessità che l'autorità giudiziaria si avvalga di *software* predisposti da aziende responsabili, etiche e che agiscano in maniera conforme alla legge[237].

Una volta compreso, dal punto di vista tecnico, il funzionamento del captatore informatico e dopo aver evidenziato gli innumerevoli vantaggi nelle indagini che derivano dal suo utilizzo, si rende necessario analizzare uno dei suoi maggiori profili di criticità, che consiste nella difficoltà di riprodurre le azioni compiute dagli organi inquirenti. Ciò che viene svolto dal captatore non è riproducibile esattamente e risulta essere molto complicato ricreare un ambiente identico nel quale replicare l'azione del *trojan horse*.

I captatori, infatti, si connotano per il "polimorfismo", in altre parole si adattano al sistema informatico che devono attaccare e la versione di partenza del virus non sarà mai identica a quella che poi si installa sul dispositivo bersaglio e, inoltre, adottano delle tecniche di "offuscamento" per evitare di essere rintracciati dai *software* antivirus e *anti-malware*[238].

Occorre, poi, considerare la possibilità che al termine dell'attività di captazione il *virus trojan* si autodistrugga non lasciando così traccia della sua presenza.

---

[236] Sul tema bisogna segnalare che la Commissione UE ha avviato un gruppo di lavoro denominato *"European Public-Private Patnership for Resilience",* preordinato a promuovere la cooperazione tra privato e pubblico nello scambio efficace e rapido di informazioni sulle minacce cibernetiche, disponibile su *European Union Agency for Network and Information Security* (ENISA), www.enisa.eu

[237] F. PIEROZZI, *Il caso "Haking Team": quis custodiet ipsos custodes ?, Problematiche e sfide per una più efficiente patnership tra settore privato e agenzie d'intelligence nella cybersecurity*, in www.dsps.unifi.it, p.4-7.

[238] G. ZICCARDI, *op.cit*. p.251.

Se è quasi impossibile replicare le operazioni compiute dagli organi inquirenti per mezzo del captatore, diversa invece è la questione della "verificabilità" delle azioni compiute, vale a dire la possibilità di poter richiedere delle descrizioni dettagliate del comportamento del *trojan horse* attraverso la predisposizione di un sistema di raccolta dei dati digitali relativi all'investigazione.

Si pensi, a titolo esemplificativo, alla predisposizione di un registro, su un supporto inalterabile, contenente una copia dei *files* relativi a tutte le operazioni compiute dal captatore, di tutto il materiale acquisito nel corso dell'indagine e delle procedure di disinstallazione.

È necessario, infatti, tener conto della circostanza che i dati digitali raccolti nel corso dell'investigazione sono per loro natura intangibili, inevitabilmente a rischio di danneggiamenti e contraffazioni con un grave pregiudizio per i diritti delle parti. Da ciò ne consegue che è doveroso adottare delle misure idonee per l'acquisizione di dati informatici che garantiscano l'immodificabilità del contenuto della memoria del dispositivo nel quale è stato inoculato il virus, l'integrità dei dati acquisiti e la loro corretta conservazione[239].

Pertanto, ferma restando l'impossibilità di replicare l'attività del captatore visto il connaturato polimorfismo di questo strumento, l'attenzione del legislatore si è spostata sulla predisposizione di efficienti sistemi di verifica *ex post* delle operazioni intrusive realizzate attraverso il *trojan horse*.

Infatti, sempre nell'ambito della riforma sulle intercettazioni, l'art.5 del d.lgs. 216/2017 ha modificato l'art.89 del d.lgs 271/1989 [240] disponendo, nell'ipotesi d'intercettazione tra presenti per mezzo di captatore su dispositivi elettronici portatili, che le conversazioni intercettate vengano trasferite esclusivamente per mezzo dei *server* della Procura in modo da garantire la sicurezza e l'affidabilità della trasmissione dei dati, inoltre durante il trasferimento dovrà essere operato un controllo costante per assicurare la corrispondenza tra quanto intercettato e quanto trasmesso e registrato[241].

---

[239] G. GIOSTRA-R. ORLANDI, *op.cit.*, p.218.

[240] Decreto legislativo 28 luglio 1989, n. 271. Norme di attuazione, di coordinamento e transitorie del codice di procedura penale.

[241] Sul tema cfr. *infra* Cap. III § 3.3.

3. Tutela della privacy dell'utente nei sistemi di messaggistica istantanea, la crittografia end to end

Per privacy s'intende il diritto di ogni persona di tenere segreti quei fatti e le informazioni che riguardano la sua sfera personale. Tale diritto implica che i dati personali non possono essere divulgati senza il consenso del soggetto interessato che può regolarne e controllarne la diffusione.

Il diritto alla privacy, anche se non espressamente menzionato dalla Carta costituzionale, è meritevole di tutela in quanto trova un saldo ancoraggio nell' articolo 2 della Costituzione che impone allo Stato di salvaguardare e riconoscere i diritti inviolabili dell'uomo, tanto come singolo individuo che come membro delle formazioni sociali.

Il diritto alla privacy è, inoltre, richiamato nell'articolo 8 CEDU, il quale dispone che: «*ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio*».

Per quanto riguarda le fonti comunitarie, la Carta dei diritti fondamentali dell'Unione Europea nel secondo capo dedicato ai diritti di libertà, all'articolo 8, sancisce espressamente che ogni persona ha diritto alla protezione dei dati di carattere personale che devono essere trattati secondo lealtà per finalità determinate e con il consenso della persona interessata. È necessario, inoltre, segnalare che il 24 maggio 2016 è entrato in vigore il nuovo regolamento europeo n. 2016/679UE che, insieme alla direttiva n.2016/680UE, ridefinisce i confini del quadro normativo relativo alla tutela dei dati personali per tutti gli Stati membri dell'Unione europea. Il regolamento è direttamente applicabile in tutti i Paesi dell'Unione a decorrere dal 25 maggio 2018 ed è finalizzato ad uniformare a livello comunitario la disciplina della privacy.

Come detto, il progresso tecnologico nell'ambito delle comunicazioni ha inciso profondamente sulla vita privata degli individui, si pensi ad esempio al sempre più frequente ricorso ai sistemi di messaggistica istantanea che avvalendosi della rete Internet, permettono non solo la comunicazione verbale tra gli utenti, ma anche lo scambio di foto, documenti e altri *file* multimediali.

È evidente che l'utilizzo di questi sistemi, se da un lato ha una pluralità di risvolti positivi, dall'altro può determinare una circolazione incontrollata di dati personali[242]e sensibili[243], arrecando, così, un possibile *vulnus* alla privacy degli individui.

I sistemi di messaggistica più diffusi e utilizzati principalmente sugli *smartphone* sono *Whatsapp, Facebook, Messanger, Instagram e Skype*.

Con l'avvento di queste applicazioni, che vengono continuamente aggiornate dagli sviluppatori in modo da soddisfare le esigenze degli utenti, le conversazioni telefoniche realizzate per mezzo della rete fissa e della rete mobile sono diventate obsolete.

Ad esempio, programmi come *Skype* utilizzano la tecnologia *VOIP* che permette di effettuare una chiamata utilizzando la connessione *Internet*, in luogo della normale linea telefonica, il VOIP si serve dell'indirizzo *IP* rappresentato da una serie numerica che identifica in maniera univoca un dispositivo detto *host.* L' *host è* collegato ad una rete informatica che utilizza l'*Internet Protocol,* come protocollo di rete, infatti l'acronimo VOIP sta per *Voice Over Internet Protocol* vale a dire "Voce tramite protocollo Internet".

Per poter comprendere come le comunicazioni vengano trasmesse per mezzo dei sistemi di messaggistica istantanea, occorre partire dall'assunto che la navigazione tramite Internet avviene per mezzo di un sistema di "impacchettamento" delle informazioni[244]che poi vengono inviate al dispositivo destinatario. Questi pacchetti di dati sono immessi nella rete, alternativamente, "in chiaro" e quindi leggibili se intercettati, oppure "cifrati" ossia leggibili solo da chi possiede la chiave di decrittazione.

La maggior parte delle applicazioni di messaggistica istantanea, prima fra tutte *Whatsapp*, permette di crittografare i messaggi, le foto, i video, i messaggi vocali, le telefonate e i documenti scambiati, in modo da evitare che i dati personali degli utenti possano venire intercettati e conosciuti da terzi.

---

[242] Si veda art 4, lett. *b)*, Dlgs 196/2003 (Codice Privacy) che definisce dato personale «*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*».

[243] Si veda art 4, lett. *d)*, Codice Privacy che definisce i "dati sensibili" «*quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*».

[244] Si veda *supra* § 2.

Lo strumento che viene utilizzato per proteggere la privacy e la riservatezza degli utenti è la tecnologia denominata crittografia *end to end* che consente di occultare la trasmissione di comunicazioni e di dati creando una sorta di schermo crittografico, in modo che solo il destinatario e il mittente del messaggio potranno conoscerne il contenuto[245] .

Un eventuale soggetto terzo, che provi ad inserirsi nel trasferimento del messaggio, potrà visualizzare solo una stringa di caratteri incomprensibili e indecifrabili.

Per proteggere la privacy di tutti coloro che fruiscono dei sistemi di messaggistica istantanea, la crittografia *end to end* si avvale di due chiavi crittografiche: una chiave privata che, rimanendo nel dispositivo di uno degli interlocutori, serve a decrittare i messaggi in arrivo e una chiave pubblica che, una volta condivisa con l'altro soggetto parte della conversazione, sarà utilizzata per crittografare i messaggi in uscita. Con questo sistema le comunicazioni saranno leggibili solo dal dispositivo che ospita la chiave privata legata alla chiave pubblica utilizzata per le crittografie.

La crittografia opera automaticamente, non essendo necessario che chi fruisce dell'applicazione di messaggistica istantanea attivi qualche speciale impostazione o si adoperi per creare chat segrete; nella maggior parte dei casi, quindi, gli utenti non sono a conoscenza dei sistemi di sicurezza adoperati dagli sviluppatori di questi programmi.

Inoltre, la crittografia *end to end* è sempre attiva e non può essere disattivata neanche con l'espresso consenso degli interlocutori.

Le varie applicazioni di messaggistica istantanea come: *Whatsapp, Messanger e Telegram,* adottando la crittografia *end to end,* proteggono le comunicazioni e lo scambio di foto, video e altri file multimediali tra gli utenti, rendendole così non leggibili da parte di un eventuale *hacker*.

La crittografia *end to end,* quindi, è certamente funzionale a proteggere le comunicazioni e gli interessi dei comuni cittadini che utilizzano i sistemi di messaggistica istantanea , ma allo stesso tempo, è uno strumento utile per il perseguimento di scopi illeciti da parte, ad esempio, di un'organizzazione criminale.

[245] S. SERAFIN, *Whatsapp, Crittografia end to end e sicurezza, riflessi nel procedimento*, in *Cammino Diritto*, 2016, 4, p. 61-62.

Basti pensare allo scambio di informazioni tra membri di un'organizzazione terroristica per la preparazione di un attacco, oppure ai vantaggi che la crittografia può procurare ad un *pusher* intento ad organizzare uno scambio di droga.

Gli strumenti investigativi utilizzati dalle Procure permettono d'intercettare le conversazioni telefoniche, realizzate tramite rete fissa o rete mobile con il consenso dell'operatore di telefonia fissa o mobile che duplica la conversazione intercorrente tra due utenti.

Tuttavia queste tecniche di intercettazione non possono essere utilizzate in maniera efficace per captare le comunicazioni veicolate tramite la rete internet perché permetterebbero solo di stabilire quando il dispositivo viene effettivamente usato dall'indagato ma non di carpire il contenuto della comunicazione.

Considerando l'inutilità dei sistemi di intercettazione tradizionale per captare le più evolute forme di comunicazioni informatiche, si evince come il captatore informatico o *trojan horse* possa essere lo strumento tecnologicamente più avanzato per consentire l'attività di intercettazione da parte degli organi inquirenti, in quanto permette di captare i dati costituenti la conversazione di un soggetto che si avvale di un sistema di messaggistica istantanea , quando quest'ultimi risiedono "in chiaro" all' interno del dispositivo, dal momento che le applicazioni di messaggistica criptano i dati solo una volta che vengono immessi nella rete, trasformandoli in una stringa di numeri e codici incomprensibili.

4. Ulteriori impieghi investigativi dei "remote control systems"

Il virus *trojan horse* permette al suo utilizzatore di controllare da remoto il dispositivo infettato e di eseguire non solo una captazione delle comunicazioni in uscita e in entrata dall'apparato bersaglio ma anche il compimento di una pluralità di altre operazioni intrusive. Per questo motivo la dizione più corretta per qualificare questo poliedrico strumento investigativo è quella, volutamente ampia, di «*remote control systems»*[246] *(RCS)* o sistemi di controllo remoto, che permette di far rientrare nel suo ambito di applicazione tutte le molteplici funzioni investigative del *trojan horse.*

Le Sezioni unite della Corte di cassazione nella sentenza Scurato [247] hanno affrontato, tra i numerosi risvolti applicativi dell'impiego del captatore informatico, quello relativo alle intercettazioni di conversazioni tra presenti realizzate mediante l'attivazione da remoto del microfono di un dispositivo mobile nel quale era stato inoculato il virus.

In questa occasione le Sezioni unite, compiono un'attenta analisi di tutte le operazioni eseguibili attraverso l'inoculazione nel dispositivo bersaglio del *trojan horse,* pervenendo così ad una classificazione dei *remote control systems.*

Il virus *trojan* permette , infatti, di captare tutto il traffico dati in arrivo e in partenza dal dispositivo bersaglio (es. *email, file* multimediali e comunicazioni scambiate con i sistemi di messaggistica istantanea), di attivare da remoto il microfono captando in questo modo i colloqui che si svolgono nello spazio che circonda l'apparato infettato, di mettere in funzione la *web camera* permettendo così agli investigatori di carpire le immagini, di perquisire l'*hard disk* facendo copia totale o parziale delle unità di memoria del sistema informatico preso di mira, di captare tutto ciò che viene digitato sulla tastiera collegata dispositivo (*keylogger)* [248], di visualizzare ciò che appare sullo schermo dell'apparato bersaglio (*screenshot)*[249] ed infine di sfuggire agli antivirus in commercio.

Le operazioni eseguibili mediante lo strumento del captatore informatico possono essere suddivise nelle due categorie delle *online search* (anche dette *one time copy*) e delle *online surveillance.*

---

[246] M. TORRE, *op.cit,* p.13

[247] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato, in *C.e.d. Cass*., Rv. 266905.

[248] Si veda *infra* § 4.1

[249] *Ibidem*

L' *online search* comprende le operazioni che permettono di copiare i dati contenuti nell'apparato infettato, vale a dire la perquisizione e il sequestro a distanza di dati "statici" già memorizzati nel dispositivo nel quale è stato inoculato il virus, mentre l'*onlin*e *surveillance* riguarda, invece, la captazione del flusso telematico dei dati tra il sistema informatico e altre periferiche, questa categoria include le intercettazioni, le videoriprese e la profilazione dell'utente tramite *keylogger* e *screenshot*[250] .

Da questa classificazione emerge come le operazioni intrusive eseguibili attraverso l'inoculazione in un dispositivo bersaglio del virus *trojan horse* costituiscano un utilissimo strumento in mano agli organi inquirenti per l'accertamento e la repressione dei reati. Nonostante ciò è necessario evidenziare come la Corte costituzionale tedesca in due importanti pronunce abbia rilevato che i sistemi di controllo remoto benché , nella loro dimensione investigativa, si presentino come dei "validissimi alleati" per la lotta contro il terrorismo o la criminalità organizzata, allo stesso tempo comportino una fortissima compressione, se non addirittura un vero e proprio annullamento di diritti fondamentali della persona.

Ciò premesso, la Corte costituzionale tedesca con una sentenza del 2008 ha affrontato il tema delle investigazioni compiute con strumenti informatici che permettono l'acquisizione di dati "da remoto", arrivando a dichiarare l'illegittimità costituzionale dell'art 5, comma secondo, n. 11 della legge sulla protezione della Costituzione del Nord Reno-Westfalia, che consentiva all'*intelligence* tedesca il monitoraggio "da remoto" e l'accesso ai sistemi informatici collegati in rete.

La Corte tedesca ha ritenuto le disposizioni censurate confliggenti con un nuovo diritto, definito come il diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici, considerato come corollario ed espressione del diritto di dignità della persona[251].

Da questa pronuncia emerge come i dati personali dell'individuo, diffusi in rete, siano sicuramente un'espressione della personalità di quest'ultimo e, in quanto tali, sono

---

[250] M. TRESCA, *I programmi spia: il diritto alla privacy di fronte ai nuovi strumenti tecnologici d'indagine,*2006, in *Amministrazione in Cammino*,2016, 4, p.2.

[251] A. VENGONI-L. GIORDANO, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, nota a *Bundersverfassungsgericht, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09,* in *Dir. pen. cont.*, 8 Maggio 2016, p. 2.

meritevoli di tutela nei confronti di qualsiasi accesso occulto anche se compiuto dallo Stato.

La Corte tedesca ha, poi, ritenuto che le operazioni investigative suscettibili di comprimere questo nuovo diritto sono ammissibili solo se effettuate per il perseguimento della finalità di repressione dei reati e a condizione che venga rispettata la riserva di giurisdizione. È, inoltre, necessario un provvedimento autorizzativo del giudice che poi sorvegli l'espletamento di queste attività.

I Giudici tedeschi hanno sollecitato un intervento del legislatore affinché adottasse delle idonee cautele per impedire agli organi inquirenti di accedere a dati irrilevanti per le indagini o comunque per imporre la cancellazione o l'inutilizzabilità processuale di questi dati[252].

La Corte costituzionale tedesca nel 2016 statuisce nuovamente sul tema dei sistemi investigativi di acquisizione di dati da remoto, dichiarando l'incostituzionalità di alcune disposizioni legislative concernenti i poteri della polizia federale nell'ambito della lotta al terrorismo, riconoscendo però al legislatore il compito di ricercare un punto di equilibrio tra la necessità di proteggere la società dall'incombente minaccia del terrorismo internazionale e i diritti fondamentali dell'individuo. La Corte tedesca puntualizza che questo bilanciamento debba essere effettuato alla stregua del principio di proporzionalità, in base al quale i poteri investigativi che ingeriscono profondamente nella vita privata e nella privacy dei cittadini devono essere preordinati alla tutela di interessi "sufficientemente" rilevanti e nei casi in cui sia prevedibile un pericolo specifico a questi interessi[253].

I *remote control systems,* inoltre, sono stati oggetto di considerazione anche oltre i confini europei. Negli Stati Uniti l'intelligence dispone del *software* cosiddetto "*magic lantern",* ossia di un *keylogger,* inviato tramite e-mail o installato fisicamente nel dispositivo bersaglio, che consente di rilevare i tasti schiacciati dall'utilizzatore del computer e quindi di accedere alle *password* poste dall'indagato per proteggere le cartelle e i documenti.

---

[252] F. IOVENE, *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale,* in *Dir. pen. cont.*, 2014, 3, p.331.

[253]F. NICOLICCHIA, *I limiti fissati dalla Corte Costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano,* in *Archivio penale*,2017, 2, p. 4-5.

Trattasi di uno strumento d'indagine che deve essere autorizzato con un mandato del giudice e dipende dal riconoscimento di una "*reasonable expectation of privacy"* rispetto ai dati e a tutte le informazioni contenute in un personal computer[254]. Qualora l'attività investigativa interferisca con la ragionevole aspettativa di privacy del destinatario, essa potrà essere qualificata come "*search"* con la conseguente applicazione della c.d. "*Fourth Amendment Doctrine"* in base alla quale il Quarto emendamento della Costituzione americana protegge la persona, la corrispondenza e l'abitazione da perquisizioni e sequestri non disposti dal giudice con un *judicial warrant* [255]. Il compito di stabilire quando sussista una "*reasonable expectation of privacy"* con la conseguente applicazione delle garanzie costituzionali è stato assunto dalla Corte Suprema, il cui *case law* ha progressivamente delineato un sistema di regole volto a tracciare un equo bilanciamento tra esigenze investigative e tutela dei singoli, che passa attraverso la qualificazione di una determinata attività come perquisizione o sequestro[256].

4.1 Uso del virus trojan horse in funzione Keylogger, Screenshot e Screencast

La profilazione dell'utente mediante *keylogger*, *screenshot* e *screencast* rientra nella categoria dell'*online surveillance* nel cui ambito sono ricomprese le operazioni eseguibili attraverso l'inoculazione nel dispositivo *target* di un *trojan horse* che permettono la captazione dei dati tra il sistema informatico e le altre periferiche[257].

Il termine *keylogger* può essere scomposto in un sostantivo *key* (tasto) e in un verbo *to log* (registrare su un diario) : il significato della locuzione è, infatti, quello di registratore di tasti.

[254] F. IOVENE, *op.cit.*, p. 332.

[255] F. IOVENE, *Ibidem*.

[256] F. IOVENE, *Ibidem*.

[257] Si veda *supra* § 4.

Questo strumento informatico consente di captare tutto ciò che viene digitato sulla tastiera di un computer, *smartphone* o di qualsivoglia dispositivo elettronico munito di una tastiera fisica o virtuale.

Il *keylogger*, creando dei *file* di *log* contenenti tutti i dati intercettati che vengono visualizzati in tempo reale o in differita, da remoto, da parte di un soggetto esterno, realizza il cosiddetto *sniffing*, vale a dire l'intercettazione passiva dei dati veicolati in un sistema informatico.

Il *keylogger* può essere di tipo *hardware* e s*oftware.* Il primo consiste in un micro-dispositivo elettronico a cavetto, simile ad una prolunga, collegato tra la tastiera e lo schermo del computer che memorizza in un unico *file* di testo qualsiasi dato digitato sulla tastiera.

Ll *keylogger* di tipo *software*, invece, è un vero e proprio programma spia installato all'insaputa dell'utente per mezzo di un *trojan horse* che rimane in esecuzione nel dispositivo informatico bersaglio captando tutte le digitazioni che avvengono sulla tastiera, per poi registrarle in *files* di *log* ed inviarle ad un controllore esterno che agisce da remoto.

Lo *screenshot* e lo *screencast*, consentono, invece, di captare l'output video del dispositivo bersaglio. Il primo si sostanzia nell'istantanea (fermo immagine) del monitor dell'utente, mentre il secondo è un insieme di fotogrammi registrati in un video di ciò che l'utente visualizza sul proprio monitor.

La Corte di cassazione si è confrontata con il tema del captatore informatico utilizzato in funzione di *keylogger* nell'ambito di un procedimento concernente un'associazione per delinquere finalizzata al traffico di stupefacenti[258].

I presunti trafficanti utilizzavano i computer situati in alcuni *internet point* e, per mezzo di una serie di caselle di posta elettronica, inviavano e ricevevano *e-mail* al fine di comunicare assiduamente con i propri referenti.

I rapporti comunicativi di natura telematica si realizzavano sostanzialmente in due modi: in alcuni casi i messaggi di posta elettronica venivano trasmessi normalmente attraverso la rete telematica, in altri casi le *e-mail* venivano salvate in modalità "bozze", venendo così visionate dal destinatario che, inserendo le credenziali di accesso e la *password*, accedeva così alla casella di posta elettronica.

[258] Cass. pen., sez. IV, 28 Giugno del 2016, n.40903, in *C.e.d. Cass.*, Rv. 268228.

Mentre le *e-mail* in entrata e in uscita dai computer ubicati negli internet point frequentati dagli indagati sono state oggetto di un provvedimento d'intercettazione di flussi telematici ai sensi dell'art. 266-*bis* c.p.p., invece le comunicazioni lasciate nella cartella bozza, i messaggi inviati e ricevuti in precedenza, ma giacenti nelle diverse cartelle dell'*account,* sono stati acquisiti per mezzo dell'inoculazione nel computer di un virus *trojan horse* in funzione *keylogger* che ha permesso alla polizia giudiziaria di acquisire le *password* e le credenziali di accesso delle caselle di posta elettronica e di apprenderne così il contenuto.

Le *e-mail* inviate e ricevute dal destinatario in precedenza, archiviate nell'account, poiché si sostanziano di un flusso di dati già avvenuto anche in assenza di una loro captazione contestuale alla comunicazione , secondo quanto statuito dalla Corte, possono formare oggetto d'intercettazione, mentre le e-mail archiviate nella cartella bozza, non inviate al destinatario, devono essere acquisite per mezzo di sequestro di dati informatici *ex* art.254 *bis* c.p.p. .

La procedura utilizzata dall'organo inquirente, nel caso di specie, per acquisire le *e-mail* inviate, ricevute e quelle archiviate, non si è realizzata mediante la duplicazione della casella di posta elettronica da parte del gestore, con il conseguenziale inoltro dei messaggi scambiati al *server* della Procura della Repubblica. Gli inquirenti sono entrati direttamente, dopo aver acquisito le *password* per mezzo del *keylogger*, nell'account di posta elettronica *@hotmail.com* gestito da una società statunitense, il cui server è situato in territorio americano [259]. Su questo punto è intervenuta la stessa Corte che ha evidenziato come il decreto di sequestro *ex* art.254 e ss. c.p.p., avente ad oggetto le *e-mail* contenute nella cartella bozze di account straniero, non richiede, a pena di inutilizzabilità, il ricorso alla rogatoria attiva in quanto «*la detenzione consiste nell'avere la disponibilità della cosa, ossia nell'avere la possibilità di utilizzarla tutte le volte che si desidera pur nella consapevolezza che essa appartiene ad altri*»[260] .

Da questo ragionamento si evince che i dati contenuti in un *server* all'estero sono comunque detenuti dal soggetto che ha la titolarità delle credenziali di accesso e non dalla società che gestisce quel *server;* dalla piena disponibilità dei documenti virtuali depositati

[259] E.M.MANCUSO, *L'acquisizione di contenuti e-mail,* in A.SCALFATI (a cura di), *Le indagini atipiche,* Torino, 2014, p.53.

[260] Cass., Sez. IV, 28 Giugno del 2016, n. 40903.

nell'*account* di posta elettronica, ne discende logicamente l'attivazione della procedura di sequestro senza rogatoria[261].

Per quanto riguarda l'acquisizione delle password per mezzo del captatore informatico in funzione *keylogger* la Corte di cassazione ha statuito che «*si è usato il programma informatico così come si è da sempre usata la microspia per le intercettazioni telefoniche o ambientali. Normalmente, invece, il trojan viene inserito al fine di visualizzare in tempo reale l'attività che viene svolta su un determinato schermo*»[262].

L'assimilazione del virus *trojan horse* in funzione *keylogger* ad una comune microspia è stata, tuttavia, criticata da alcuni commentatori della sentenza in esame, poiché risulta difficile ricomprendere la digitazione sulla tastiera di un computer, necessaria ad accedere ad una casella di posta elettronica, nell'alveo della definizione di comunicazione e, inoltre, il captatore informatico presenta, rispetto alla semplice microspia ambientale, un'altissima capacità intrusiva.

Il *software,* pertanto, nel caso esaminato dalla Corte, sembra sia stato utilizzato per eseguire un'ispezione o una perquisizione di tipo elettronico[263].

A differenza delle e-mail contenute nella cartella bozze sottoposte a sequestro di dati informatici, le *e-mail* inviate e ricevute e "parcheggiate" nelle cartelle dell'account di posta elettronica sono state acquisite nel procedimento applicando la disciplina delle intercettazioni.

La Corte sul punto ha seguito un precedente indirizzo giurisprudenziale[264] in base al quale si reputa legittima l'acquisizione di messaggi aventi natura comunicativa, applicando la disciplina delle intercettazioni ai sensi degli artt. 266 e ss. c.p.p., anche nella circostanza in cui le conversazioni, che costituiscono un flusso di comunicazioni, non si realizzano contestualmente alla captazione.

---

[261] M.S. DE NOZZA, *E-mail parcheggiate su server all'estero, similitudini con il cloud compunting : La Parola alla Cassazione*, in *Sicurezza e Giustizia*,2016, 4, p.52.

[262] Cass., Sez. IV, 28 Giugno 2016, n.40903.

[263] Si veda L. GIORDANO, *Dopo le Sezioni Unite sul "Captatore Informatico" avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, *Dir. pen. cont.*,2017, 3, p. 186; allo stesso modo M. SENOR, *Di trojan-microspia, e-mail che non sono corrispondenza e della colpa veniale di chi usa server stranieri*, 26 Ottobre 2016, in www.filodiritto.com, p.6.

[264] Si tratta di un indirizzo giurisprudenziale che si è formato in materia alle chat di Blackberry, in tal senso si veda Cass. pen., sez. III, 10 Novembre 2015, n.50452 in C.e.d. Cass., Rv. 265615; allo stesso modo Cass. pen., sez.IV, 8 Aprile 2016, n.16670 in C.e.d. Cass., Rv.266983.

Il superamento del criterio della necessaria captazione in tempo reale rispetto alla comunicazione sembra avallare un'interpretazione delle disposizioni di cui gli artt. 266 e ss. c.p.p. che legittimerebbe un'intercettazione disposta "per il passato" idonea a captare le comunicazioni avvenute in precedenza. È evidente come una simile interpretazione sembra, però, contrastare con la funzione delle intercettazioni, un mezzo di ricerca della prova per antonomasia rivolto al futuro in quanto si realizza con tecniche che permettono di apprendere, nel momento stesso in cui viene espresso, il contenuto di una conversazione che si realizza contemporaneamente alla captazione [265].

Ciò che determina la decisione della Corte di disporre il sequestro delle *e-mail* salvate nella cartella bozze e l'intercettazione delle e-mail inviate e ricevute in precedenza, è il "criterio dell'inoltro", infatti i giudici di legittimità affermano che « *In realtà, alla luce del dettato normativo, nella giurisprudenza di questa Corte di legittimità, anche a Sezioni Unite, si rinvengono elementi per poter affermare che il discrimen perché ci sia stato o meno flusso informativo e quindi debba essere applicata la disciplina delle intercettazioni e non quella del sequestro, è nell'avvenuto inoltro delle e-mail da parte del mittente*[266]».

Invece di applicare il criterio della contestualità della captazione rispetto alla conversazione, la Suprema Corte, al fine di segnare il confine tra l'applicazione della disciplina del sequestro e di quella dell'intercettazione, dà rilevanza all'invio del messaggio da parte del mittente al destinatario.

4.2 Definizione di "perquisizioni on line" e inquadramento nei mezzi tipici di ricerca della prova previsti dal c.p.p.

Lo sviluppo tecnologico nell'ambito dell'informatica mette a disposizione degli utenti dispositivi elettronici sempre più compatti e idonei ad essere trasportati in ogni luogo con molta facilità rispetto al passato, quando i *personal computer* erano di dimensioni considerevoli e fissi sulle scrivanie.

I *tablet* e *gli smartphone* permettono agli utenti di videochiamare, dialogare e gestire le proprie *mail* da ogni luogo; gli sviluppatori hanno, inoltre, elaborato delle applicazioni

[265] L. GIORDANO, *op.cit.*, p.187.

[266] Cass., Sez. IV, 28 Giugno 2016, n.40903.

che permettono di conservare carte d'imbarco, biglietti ed altri documenti direttamente nello *smartphone,* rendendo in questo modo superfluo qualsiasi supporto cartaceo.
Appare, dunque, evidente come la moltitudine di funzioni che possono essere svolte al giorno d'oggi da questi dispositivi, li rendano i "custodi" di moltissimi dati sensibili, informazioni personali, immagini e video riservati dell'utente.
Ne consegue che tra i possibili risvolti operativi del *trojan horse,* le perquisizioni *on line* sono quelle che presentano la maggior forza intrusiva nella sfera privata dell'individuo poiché consentono di eseguire un occulto monitoraggio da remoto del dispositivo bersaglio permettendo, all'occorrenza, all'investigatore di ottenere una copia dei dati ivi memorizzati.
Per fornire un esempio, se oggetto di perquisizione è uno *smartphone* gli organi inquirenti potranno ottenere una copia dei file multimediali, dell'elenco delle chiamate, delle chat relative ai sistemi di messaggistica istantanea e tantissimi altri dati di pertinenza dell'indagato.
Le perquisizioni *on line,* realizzate tramite il *virus trojan,* sono ricomprese nell'ampio *genus* dei *remote control systems* e nello specifico vengono inquadrate, insieme al sequestro, nella categoria dell'*online search* [267].
I vantaggi derivanti da questo innovativo mezzo di ricerca della prova sono facilmente intuibili. Molto spesso, infatti, la prova di un illecito finisce per essere ricercata in dispositivi di memorizzazione digitale delle informazioni e non è infrequente che anche nel corso di indagini finalizzate all'accertamento di reati, non necessariamente informatici, emergano fonti di prova di natura digitale.
A questa peculiare forma di perquisizione non appare applicabile la disciplina degli artt. 247 e ss. del codice di rito poiché le perquisizioni *ivi* tipizzate sono preordinate alla ricerca del "corpo del reato" e delle "cose pertinenti al reato" sulle persone e in luoghi determinati, ovvero sono finalizzate ad eseguire in quest'ultimi l'arresto dell'imputato o dell'evaso o il sequestro del corpo del reato reperito durante la perquisizione.
Il mezzo di ricerca della prova previsto dal codice di rito pertanto è connotato dalla determinatezza del suo oggetto; in giurisprudenza[268] è predominante la tesi secondo la

[267] Si veda *supra* § 4.

[268] Si veda Cass. pen., sez VI, 14 settembre 1998, n.1934, in *C.e.d. Cass*., Rv. 211593; allo stesso modo Cass. pen., sez. II, 30 dicembre 2013, n.51867, in *C.e.d. Cass*., Rv. 258074.

quale il provvedimento che dispone la perquisizione non deve contenere l'indicazione puntuale delle cose pertinenti al reato o il corpo del reato. Si reputa, invero, sufficiente che esso indichi le ragioni in base alle quali sussiste il fondato motivo di ritenere che in un determinato luogo si trovino fonti di prova, conseguentemente gli inquirenti procederanno nel corso della perquisizione ad individuare tutti gli elementi necessari all'accertamento dei fatti[269] .

Le perquisizioni *on line* non sono preordinate a ricercare gli elementi indicati negli artt. 247 e ss. c.p.p.; esse consentono di duplicare tutti i documenti archiviati nel sistema informatico preso di mira e di apprendere quelli che in futuro verranno creati sullo stesso, permettendo, così, agli organi inquirenti di effettuare un monitoraggio continuativo dell'elaboratore elettronico nel quale è stato inoculato il virus.

Nelle perquisizioni tradizionali l'attività dell'autorità giudiziaria è subordinata alla consegna del decreto e dell'avviso concernente la facoltà di farsi assistere da un difensore; la perquisizione del domicilio soggiace, inoltre, a stringenti limiti temporali[270]. La previsione di questi adempimenti evidenzia che per quanto questo mezzo di ricerca della prova venga considerato un atto da compiersi a sorpresa, si tratta di un'attività necessariamente conosciuta dall'indagato. Prima di eseguire una perquisizione *ex* art. 249 c.p.p. è, infatti, consegnata una copia del decreto all'interessato con l'avviso di farsi assistere da una persona di fiducia e il medesimo avviso è consegnato dall'autorità giudiziaria, nell'atto di eseguire una perquisizione locale *ex* art.249 c.p.p., all'indagato se presente, e a chi abbia l'attuale disponibilità del luogo.

La perquisizione *on line,* invece, non è soggetta a simili incombenze e l'indagato ne resta all'oscuro per tutto il tempo necessario alla sua esecuzione fino alla *discovery* disposta alla conclusione delle indagini poiché il successo e l'esito positivo dell'operazione investigativa dipendono proprio dal fatto che si svolga all'insaputa del soggetto interessato [271].

Il tratto peculiare dello strumento investigativo in esame, come anticipato, è quello della "dinamicità" essendo finalizzato a raccogliere il maggior numero di dati possibili contenuti nel sistema informatico dell'indagato. Di conseguenza le perquisizioni on *line*

---

[269] A.SCALFATI, *op.cit.*, p.443.

[270] G. CONSO-V. GREVI-M. BARGIS, *op.cit.*, p 376.

[271] A.SCALFATI *op.cit.,* p.444.

appaiono prive della funzione descrittiva che caratterizza le ispezioni disciplinate dall'art. 244 e ss. del c.p.p., preordinate, invece, a "fotografare" una situazione di fatto suscettibile di modifica nel corso del tempo.

Conclusivamente questa forma di perquisizione, non rientra neppure nell'ambito di applicazione della disciplina delle intercettazioni *ex* artt. 266 e ss. del c.p.p., che si concretizzano nella «*captazione occulta e contestuale di una conversazione tra due o più soggetti che agiscono con l'intenzione di escludere soggetti esterni, adottando modalità tecniche di comunicazione idonee allo scopo*»[272]. Le perquisizioni *on line*, infatti, sono preordinate alla raccolta di un elevatissimo numero di dati informatici che non devono necessariamente sostanziarsi in una comunicazione intercorrente tra due utenti persone fisiche.

Al fine di valutare l'applicabilità della disciplina degli artt.266 e ss c.p.p. alle perquisizioni *on line,* si rende necessario considerare quanto disposto dalla Corte Costituzionale Tedesca[273] sul tema delle investigazioni compiute con strumenti informatici che permettono l'acquisizione di dati "da remoto".

I giudici tedeschi, in questa decisione, hanno sviluppato una diversa nozione di comunicazione che si sostanzia in un dialogo unidirezionale dell'utente con la rete, consentendo, così, di elaborare un concetto di telecomunicazione comprensivo di tutte le informazioni che sono virtualmente trasferite dall' utente ad un sistema di ricerca informatico, quale ad esempio il motore di ricerca *Google* [274]. Questa forma di dialogo tra un soggetto ed un *server* è assoggettata alle garanzie espresse dall' art. 10 della Legge fondamentale per la Repubblica Federale di Germania che tutela la segretezza delle comunicazioni e, inoltre, alla captazione di questa "relazione informatica" è applicabile, secondo i giudici tedeschi, la disciplina codicistica in materia d'intercettazione di comunicazioni[275]. Non appare possibile pervenire ad analoghe conclusioni nell' ordinamento italiano attraverso un'esegesi evolutiva dell'art. 15 Cost[276].; quantomeno

---

[272] Cass. sez.un.,24 Settembre 2003, Torcasio, n.36747 in *C.e.d. Cass*., Rv. 225465, sulla della nozione d'intercettazione cfr. Cap.1 § 2.1.

[273] BVerfG, 6 luglo 2016, 2 BvR 1454/13, sul tema si veda *supra* § 4.

[274] E. MANCUSO, *La perquisizione on line*, in *JusOnline*,2017, 3, p.420.

[275] E. MANCUSO, *Ibidem*.

[276] Sul tema della libertà e segretezza delle comunicazioni cfr. Cap. I § 1.

sino a che non si provi ad espandere il catalogo dei diritti oggetto di tutela, non prospettabili al tempo della fondazione costituzionale[277].

4.2.1 La perquisizione on line come mezzo di ricerca della prova atipico

Alla luce delle difficoltà riscontrate nel qualificare le perquisizioni *on line* quali particolari modalità esecutive degli strumenti investigativi disciplinati dal nostro codice di rito, si potrebbe ritenere applicabile a questo mezzo di ricerca della prova l'art.189 c.p.p., disposizione che consente l'ingresso nel processo, a determinate condizioni, di prove non espressamente disciplinate dalla legge.

Il legislatore, in materia di prove atipiche, ha operato, infatti, una scelta intermedia tra il criterio della tassatività e il criterio della libertà delle prove; non optando per una «*aprioristica preclusione*» [278] delle prove non disciplinate dalla legge, ha, quindi, permesso un adeguamento continuo del processo penale allo sviluppo tecnologico.

Pertanto, quando nel processo penale sussiste la necessità di confrontarsi con una prova atipica, non riconducibile allo schema giuridico di uno degli strumenti tipizzati nel codice, spetterà al giudice il compito di valutarla alla stregua di due distinti parametri espressamente indicati dall' art. 189 c.p.p. : l'idoneità della prova a garantire l'accertamento dei fatti e l'assenza di un pregiudizio alla libertà morale della persona. Una volta soddisfatti questi due requisiti richiesti ai fini dell'ammissibilità, il giudice deciderà in concreto le modalità di assunzione della prova, dopo aver sentito le parti, allo scopo, se possibile, di concordare le cadenze procedurali [279].

Nonostante la disciplina della prova atipica sembrerebbe idonea a risolvere la questione di legittimità del captatore informatico, l'applicazione dell'art. 189 c.p.p. all'efficiente strumento delle perquisizioni *on line* è tutt'altro che scontata.

---

[277] E. MANCUSO, *Ibidem*.

[278] G. CONSO-V. GREVI-M. BARGIS, *op.cit,* p.326.

[279]G. CONSO-V. GREVI-M. BARGIS, *Ivi,* p.327.

Una parte della dottrina esclude la configurabilità di mezzi di ricerca della prova atipici, in ragione del fatto che questi strumenti vengono utilizzati dagli organi inquirenti nel corso delle indagini preliminari, senza il previo contradditorio con la difesa[280]. Ne discende l'impossibilità logica di applicare l'art. 189 c.p.p. laddove impone al giudice di sentire le parti sulle modalità di assunzione della prova atipica prima di decidere con ordinanza sulla richiesta di ammissione.

La dottrina maggioritaria [281]e le Sezioni unite della Cassazione sostengono, invece, la possibilità di configurare mezzi atipici di ricerca della prova, come ad esempio le videoriprese d'immagini in luoghi diversi dal domicilio[282]. A tal fine viene fornita un'interpretazione adeguatrice dell'art.189 c.p.p. che posticipa la fase del contraddittorio nel momento in cui viene valutata l'utilizzabilità degli elementi acquisiti.[283].

In altre parole, il contraddittorio non riguarderà l'attività di ricerca della prova ma le modalità di assunzione dell'elemento probatorio precedentemente acquisito e il giudice propenderà per l'ammissione o non ammissione della prova a seconda che siano stati rispettati o meno i requisiti prescritti dall'art.189 c.p.p.

Anche se, per mezzo di questa esegesi adeguatrice dell'art. 189 c.p.p., è possibile risolvere positivamente la questione concernente la configurabilità dei mezzi atipici di ricerca della prova, è necessario sottolineare che definire atipico un atto d'indagine non basta per affermare che quest'ultimo possa essere compiuto liberamente dagli organi inquirenti poiché può incidere su diritti garantiti dalla Costituzione.

La Corte costituzionale, infatti, ha affermato il principio in base al quale «*le attività compiute in dispregio dei diritti fondamentali del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito*»[284] .

---

[280] P. FELICIONI, *Le ispezioni e le perquisizioni, in Trattato di procedura penale,* diretta da G. UBERTIS e G.M VOENA, Milano, 2012, p. 26.

[281] Si veda P.TONINI-C.CONTI, *op.cit.,* p.187; allo stesso modo CONSO-V. GREVI-M. BARGIS, *op.cit.,*327.

[282] Si veda Cass., sez. un., 28 Marzo 2006, n. 26795, Prisco; allo stesso modo Cass. pen, sez. II, 22 maggio 2018, n.22972, in *C.e.d. Cass*., Rv. 273000.

[283] P.TONINI-C.CONTI, *op cit*., p. 188.

[284] Corte cost. 6 aprile 1973, n.34, in www.giustcost.org.

Da ciò ne consegue che per poter ammettere nel processo l'ingresso delle perquisizioni *on line* come mezzo atipico di ricerca della prova sarà, quindi, necessario verificare, in primo luogo, se le stesse soddisfino i requisiti della prova atipica di cui l'art. 189 c.p.p. e, in secondo luogo, se possano determinare una violazione dei diritti fondamentali.

Riguardo l'opportunità di far rientrare le perquisizioni *on line* nell'ambito di applicazione dell'art. 189 c.p.p. si può affermare che la perquisizione *eseguita* mediante l'inoculazione nel dispositivo bersaglio del virus *trojan horse,* soddisfa sicuramente i requisiti disposti nell'articolo 189 del c.p.p. Il captatore informatico, infatti, permette di raccogliere una pluralità di elementi probatori la cui utilità, per l'accertamento dei fatti, è indubbia e, inoltre, per quanto riguarda la tutela dell'integrità morale della persona prevista espressamente dall'art. 189 c.p.p., proprio la natura ingannevole del virus *trojan* garantisce che il processo volitivo dell'indagato si formi in assenza di alcun condizionamento esterno[285].

Per quanto concerne, invece, il problema dell'indebita compressione dei diritti fondamentali determinata dal ricorso al virus *trojan*, sarà necessario individuare i diritti inviolabili coinvolti nella perquisizione *on line*. A tal fine è possibile determinare un sistema di garanzie dell'individuo rispetto agli atti d'indagine compiuti dagli organi inquirenti articolato su tre livelli, a seconda dei diritti che subiscono una compressione dall'esecuzione di una perquisizione *on line.* Il primo livello rileva nel caso in cui la perquisizione determini una compressione di un diritto inviolabile coperto da riserva di legge e di giurisdizione come previsto dagli artt.13, 14, 15 Cost. In questo caso l'elemento probatorio raccolto sarà inutilizzabile in assenza di una previsione normativa che determini le modalità con le quali questi diritti possono subire una limitazione. Per contro, se a subire un pregiudizio è un bene giuridico non coperto da riserva di legge rinforzata, l'elemento probatorio raccolto per mezzo della perquisizione *on line* potrà avere ingresso se l'acquisizione risulta assistita da un provvedimento motivato dell'autorità giudiziaria nel rispetto dei requisiti dell'art.189 del c.p.p[286]. Ciò premesso emerge che mentre per i diritti assistiti dalla riserva di legge il bilanciamento tra l'esigenza di accertamento del reato e la tutela dell'individuo viene effettuato direttamente dal legislatore, per i diritti

[285] M. TORRE, *op cit*., p.69.

[286]Si veda, M. TORRE, *op cit*., p.72 e ss.; allo stesso modo S. MARCOLINI-F. RUGGERI-L. PICOTTI, *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, pp.190 ss.

non coperti dalla riserva di legge rinforzata questo compito sarà una prerogativa del giudice. Infine, quando l'attività investigativa messa in atto con la perquisizione *on line* non determina un'indebita compressione di alcun diritto con rilevanza costituzionale, non sarà necessario alcun provvedimento giurisdizionale e l'utilizzabilità dei risultati ottenuti sarà determinata dal rispetto dei requisiti previsti dall'art.189 c.p.p.[287].

Tra i diritti inviolabili dell'uomo quello che subisce un profondo pregiudizio dall'esecuzione di una perquisizione *on line* è sicuramente la privacy che non è oggetto di un'autonoma e specifica tutela a livello costituzionale, salva la possibilità di ritrovare un fondamento nell'art. 2 della Costituzione.

Non sussiste, pertanto, una riserva di legge rinforzata che obblighi il legislatore a determinare i casi e i modi di limitazione di questo diritto e, prendendo in considerazione il sistema di garanzie dell'individuo rispetto agli atti d'indagine precedentemente esposto, la perquisizione *on line* per mezzo del captatore informatico, purché supportata da un provvedimento motivato dell'autorità giudiziaria, sarà legittima e l'elemento probatorio raccolto potrà avere ingresso nel processo. Tuttavia sul tema del pregiudizio arrecato alla privacy dell'indagato dalla perquisizione *on line* non si può non prendere in considerazione quanto statuito dalla CEDU nell'art. 8, il quale vieta ogni indebita ingerenza dell'autorità pubblica nella vita privata, familiare, nel domicilio o nella corrispondenza di un individuo a meno che tale intrusione non sia regolamentata dalla legge e costituisca una misura necessaria in una società democratica.

Conformemente a quanto previsto dall'art. 8 CEDU, quindi, un'attività d'indagine altamente lesiva della privacy dell'indagato sarà ammissibile solo nel caso in cui sia espressamente "prevista dalla legge" e, secondo quanto statuito dalla Corte di Strasburgo, un'attività d'indagine è tale quando le disposizioni normative che la disciplinano rendono l'interessato compiutamente edotto riguardo le conseguenze derivanti dall'esecuzione di quell'attività nei suoi confronti[288].

---

[287] M. TORRE, *Ibidem.*

[288] Per approfondire l'analisi dell'art. 8 CEDU e del canone della "*quality of law*" , che impone al legislatore nazionale di introdurre disposizioni in grado di consentire all'indagato di prevedere le conseguenze dell'attività d'indagine sulla propria posizione giuridica; cfr. Cap. 1 § 1.1.

Tale disposizione, quindi, sollecita un intervento del legislatore italiano per regolare in maniera puntuale i casi nei quali risulti ammissibile l'ingerenza da parte della pubblica autorità nella vita privata di un soggetto, nonostante l'art.2 della Costituzione, al quale viene ricondotto il diritto alla privacy, non preveda una riserva di legge analoga[289] .

L'intervento del legislatore sul diritto alla privacy, inoltre, si rende necessario perché l'art. 8 CEDU è direttamente applicabile nel nostro ordinamento; la Corte Costituzionale, infatti, nelle sentenze c.d. "gemelle"[290] ha riconosciuto alla CEDU il rango di fonte interposta tra la Costituzione e le fonti primarie. La Convenzione, quindi, integra il parametro di Costituzionalità di cui all'art 117 Cost. in base al quale «*la potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali*». Di conseguenza se una legge ordinaria contrasta con una o più disposizioni della CEDU, (nell'interpretazione che di quelle disposizioni viene data dalla Corte Europea dei diritti dell'uomo) e questo contrasto non è risolvibile tramite un'interpretazione "adeguatrice", la legge ordinaria sarà sottoposta allo scrutinio della Corte costituzionale.

Una volta indicate le problematiche connesse al diritto alla privacy sul quale inevitabilmente incidono le *perquisizioni on line,* occorre rilevare che il sistema di garanzie dell'individuo, rispetto ad atti investigativi particolarmente intrusivi articolato su tre livelli, ammette la configurabilità della perquisizione *on line* ,come mezzo atipico di ricerca della prova *ex* art. 189 del c.p.p., semplicemente individuando il bene giuridico sul quale insiste questa attività intrusiva, escludendo *in toto* l'utilizzabilità dell'elemento raccolto solo quando la perquisizione *on line* insiste sui diritti inviolabili di cui gli artt. 13,14,15 Cost. , ammettendola invece nel caso in cui si determini una compressione di diritti non coperti da riserva di legge rinforzata.

Nonostante questa interpretazione persegua il pregevole intento di annoverare tra gli strumenti investigativi a disposizione degli organi inquirenti le perquisizioni *on line* (se pur esclusivamente nelle limitate ipotesi in cui quest'ultime non ledano diritti assistiti da

[289] S. MARCOLINI-F. RUGGERI-L. PICOTTI, *op.cit,* pp.190 ss.

[290] Si veda Corte cost. sent., 24 Ottobre 2007 n. 348 in www.giustcost.org ; allo stesso modo Corte. cost., sent., 31 Ottobre 2007, n. 349, in www.giustcost.org

riserva di legge rinforzata), è da ritenere presente un canone fondamentale del diritto delle prove: il "principio di non sostituibilità" tra i mezzi di prova.

In base a questo postulato il versatile strumento della prova atipica non potrà essere utilizzato per superare un divieto o un'inutilizzabilità speciale stabilita in relazione ad un diverso strumento probatorio[291].

Prescindendo dalle ipotesi specificatamente previste dal codice, come nel caso della testimonianza indiretta *ex* art. 195, comma 4, c.p.p., il principio di non sostituibilità è considerato un postulato cardine per il diritto delle prove «*in applicazione del fondamentale canone di legalità della prova dal quale si evince un generale divieto di aggiramenti surrettizi*» [292].

Per poter comprendere appieno la portata di questo principio sulle potenzialità operative del captatore, occorre considerare le problematiche connesse all'uso del *trojan horse* in funzione perquisente , rappresentate sia dalla difficile verificabilità delle operazioni compiute sia dall'alto rischio di contraffazione dei dati digitali contenuti nell'apparato bersaglio[293].

Il captatore informatico consente, pertanto, agli organi inquirenti di modificare in maniera unilaterale il dispositivo bersaglio, rendendo particolarmente complesso il controllo *ex ante* ed *ex post* delle operazioni compiute, determinando così un contrasto di questo strumento di ricerca della prova con le norme introdotte dalla legge n. 48 del 2008 che impone, nell'ambito delle attività di ricerca della prova, il rispetto di misure tecniche idonee a salvaguardare dati originali e ad impedirne l'alterazione.

Più precisamente, l'ispezione, la perquisizione e il sequestro di dati informatici si realizzano, nella prassi consolidata, con l'ausilio di esperti i quali utilizzando specifici *software*, procedono al *freezing* del sistema informatico in modo da disporre la fotografia e la copia integrale dei dati in esso contenuti, grazie a questi adempimenti il pubblico ministero, le parti e il giudice possono procedere all'estrazione dei dati senza alterare il contenuto del sistema [294].

---

[291] P. FELICIONI, *op.cit.*, p.132.

[292] P.TONINI-C.CONTI, *op cit.*, p.107.

[293] Si veda *supra* § 3.

[294] E. MANCUSO, *op.cit.*, p.430.

In forza del principio di non sostituibilità, considerare utilizzabile l'elemento probatorio raccolto con la perquisizione *on line*, quale mezzo atipico di ricerca della prova, determinerebbe un'indebita elusione dell'art. 247, comma 1 *bis*, c.p.p., che, nel dettare le regole per la perquisizione di un sistema informatico e telematico, dispone l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati digitali e ad impedirne l'alterazione. Ulteriori attriti si potrebbero avere anche rispetto all'art. 254 *bis* c.p.p., laddove dispone che nel caso di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, l'acquisizione avvenga mediante copia su un adeguato supporto che assicuri la corrispondenza dei dati acquisiti con quelli originali. Nel caso della perquisizione *on line* da remoto, il dispositivo monitorato non è sottoposto a sequestro, ma rimane in uso al soggetto destinatario del monitoraggio e sarà perciò estremamente complicato garantire la conformità dei dati acquisiti con i dati originali contenuti nel dispositivo[295].

4.2.2 La perquisizione on line e il domicilio informatico

Quando gli organi inquirenti procedono all'inoculazione del *virus trojan* nel sistema informatico bersaglio al fine di eseguire una perquisizione *on line*, si determina inevitabilmente la compressione di un bene giuridico di rilevanza fondamentale: il "domicilio informatico" alla cui protezione è preordinato l'art. 615 *ter* c.p. [296].

Questa disposizione sanziona la condotta di chi s'introduce abusivamente in un sistema informatico protetto da misure volte ad impedire l'accesso a soggetti non autorizzati o vi si trattiene contro la volontà di chi ha diritto di escluderlo.

[295] M. TORRE, *op cit*., p.95.

[296] Cass.pen., sez. V, 26 ottobre 2012, n.42021, in *Foro.it*, 2012, 12, 2, 709: «Con la previsione dell'art. 615 ter cod. pen., introdotto a seguito della L. 23 dicembre 1993, n. 547, il legislatore ha assicurato la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Tuttavia, l'art. 615 ter cod. pen. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "jus excludendi alios", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello "jus excludendi" sia persona fisica, persona giuridica, privata o pubblica, o altro ente».

In quanto secondo l'art. 615 *ter* c.p. il domicilio informatico deve essere inteso come «*spazio ideale ma anche fisico in cui sono contenuti i dati informatici di pertinenza della persona* »[297], una trasposizione sul piano digitale del domicilio fisico. Al soggetto che fruisce del domicilio informatico viene riconosciuto, quindi, un legittimo *ius includendi et excludendi alios* rispetto a tutti coloro che non vantano un analogo diritto sul medesimo sistema informatico o telematico e un *ius includendi se* inteso come il diritto ad accedere, permanere ed uscire da un determinato luogo digitale[298] .

Al domicilio informatico, quindi, viene garantito il medesimo grado di dignità del domicilio fisico tutelato dall'art. 14 Cost.il quale è considerato la proiezione spaziale della persona, vale a dire il luogo nel quale essa svolge la propria vita senza possibilità di interferenza ad opera di altri soggetti[299].

Allo stesso modo il domicilio informatico inteso come luogo virtuale dove sono contenuti i dati attinenti la persona è meritevole di una protezione costituzionale e « *ciò deve avvenire per presidiare quello che appare essere divenuto un unico oggetto di tutela: la persona nelle sue diverse considerazioni, via via determinate dal suo rapporto con le tecnologie*»[300]

Da ciò ne deriva che se si considerano le perquisizioni *on line* un mezzo atipico di ricerca della prova *ex* art. 189 c.p.p. [301], tutte le volte in cui vengono disposte su un sistema informatico, sussumibile nel concetto di domicilio informatico, l'elemento probatorio così raccolto non potrebbe avere ingresso nel processo in quanto formato in violazione dell'art.14 Cost. che tutela l'inviolabilità del domicilio [302].

Per contro la Corte di Cassazione nella sentenza Virruso[303], ha escluso che l'utilizzo del virus *trojan horse* per l'esecuzione di una perquisizione *on line* diretta a captare e clonare

---

[297] *Ibidem*

[298] G. GIOSTRA-R. ORLANDI, *op cit*., p.265

[299] S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2013, p.317.

[300] S. RODOTÀ, *Ibidem*.

[301] Si veda *supra* § 4.1.1.

[302] L.BATTINIERI, *Le perquisizioni on line tra esigenze investigative e ricerca atipica della prova*, in *Sicurezza e Giustizia*,2013, 4, p.44.

[303] Cass.pen., sez. V, 29 aprile 2010, n.16556, Virruso, in *C.e.d. Cass*., Rv.246954.

il flusso di dati presenti e futuri su un personal computer ubicato nei locali sede di un ufficio pubblico, potesse ritenersi in conflitto con l'art. 14 della Cost.

In questo modo la Corte, sempre inquadrando le perquisizioni *on line* nell'ambito dell'art. 189 c.p.p., ha ritenuto ammissibile l'ingresso nel processo della prova così formata.

Il caso oggetto della sentenza riguardava l'utilizzo da parte della polizia giudiziaria del virus *trojan horse* per acquisire tutti i dati contenuti all'interno di un computer usato dall'indagato e collocato sul luogo del lavoro di quest'ultimo.

Gli inquirenti hanno usato un tipo di captatore informatico che ha permesso di copiare tutti i file contenuti nel computer in uso al soggetto indagato, operando così un monitoraggio occulto e continuativo di tutti i dati elaborati di volta in volta sul computer infetto.

Proprio il fatto che oggetto di captazione fossero i flussi di dati caricati dall' indagato sull'apparato monitorato, ha indotto la difesa a sostenere che l'attività investigativa doveva essere qualificata come intercettazione telematica *ex* art. 266 *bis* c.p.p.

Il pubblico ministero aveva, invece, autorizzato questa attività di captazione con "decreto di acquisizione di atti" *ex* art. 234 c.p.p. il quale disponeva non solo l'acquisizione dei dati esistenti ma anche di tutti quei dati che sarebbero stati inseriti in futuro nella memoria del computer.

La Corte ha ritenuto legittimo il decreto del pubblico ministero di acquisizione in copia della documentazione informatica memorizzata sul personal computer dell'indagato poiché « *l'attività autorizzata dal pubblico ministero, consistente nel prelevare e copiare documenti memorizzati nell'hard disk dell' apparecchio in uso, aveva avuto ad oggetto non un "flusso di comunicazioni" richiedente un dialogo con altri soggetti, ma " una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del computer*»[304].

Quest'ultima considerazione ha indotto i giudici a ritenere corretta la riconducibilità di tale attività di apprensione di dati informatici al concetto di prova atipica *ex* art. 189 c.p.p. escludendo così l'applicazione della disciplina degli artt. 266 ss. c.p.p.

La Corte perviene a questa conclusione perché sostiene che l'utilizzo del captatore, nel caso di specie, non si sostanzi in una violazione del diritto all'inviolabilità del domicilio, in quanto l'apparecchio monitorato non era collocato in un luogo di privata dimora e

[304] Cass.pen., sez. V, 29 aprile 2010, n.16556, Virruso.

l'imputato non godeva certo dello *ius excludendi alios* , bensì il computer era ubicato nei locali di un ufficio pubblico comunale al quale potevano accedere tutti gli impiegati per poter svolgere le proprie mansioni, il pubblico degli utenti e il personale delle pulizie.
Secondo alcuni autori la pronuncia della Corte nel caso Virruso presenta dei profili di contrasto con il concetto stesso di domicilio informatico perché, per poter affermare se le perquisizioni *on line* si pongano in conflitto con il diritto costituzionale dell'inviolabilità del domicilio, non bisogna prendere in considerazione esclusivamente la collocazione spazio temporale dell'apparato bersaglio ma bisogna valutare se il sistema informatico costituisca o meno una proiezione del domicilio fisico privato[305].
Di conseguenza in tutti quei casi in cui il *personal computer* oggetto della perquisizione rientra nell'ambito di applicazione della nozione di domicilio informatico, inteso come spazio ideale ma anche fisico in cui sono contenuti i dati informatici attinenti alla persona, la captazione unidirezionale dei dati *ivi* contenuti dovrebbe ritenersi illecita poiché effettuata in violazione dell'art.14 della Costituzione, quindi l'elemento probatorio eventualmente raccolto per mezzo della perquisizione *on line* non potrebbe avere ingresso nel processo[306].
Occorre evidenziare, inoltre, che un sistema informatico non integrerà gli estremi del domicilio informatico nei soli casi in cui, ad esempio, si tratti di un *computer* messo a disposizione di una platea indifferenziata di utenti e utilizzato per effettuare una pluralità di operazioni non attinenti alla sfera personale di chi ne fruisce[307].
Prima di ammettere che, nel caso esaminato, l'attività investigativa di perquisizione *on line* realizzata per mezzo del *trojan horse*, configuri una prova atipica *ex* art. 189 c.p.p., la Corte di cassazione ha escluso l'applicabilità della disciplina delle intercettazioni telematiche ed ha statuito che l'utilizzo del captatore informatico per clonare in tempo reale tutti i dati presenti e futuri contenuti del computer, non può ritenersi confliggente con l' art. 15 della Costituzione, relativo alla libertà e segretezza delle comunicazioni, poiché l'attività di indagine si è risolta sì nella captazione di tutti i *file* contenuti nel dispositivo bersaglio, ma relativa a flussi di dati non aventi carattere comunicativo.

---

[305] Si veda L. BATTINIERI, *op.cit.* p.44 e ss.; allo stesso modo E. MANCUSO, *op.cit.*, p. 427 e P. FELICIONI, *op.cit.*, p. 132

[306] L. BATTINIERI, *op.cit.*, p.45

[307] L. BATTINIERI, *Ibidem*.

L'oggetto della perquisizione, infatti, non era un testo inoltrato e trasmesso con il sistema informatico ma un documento predisposto per essere stampato su un supporto cartaceo e solo successivamente consegnato al suo destinatario.

I giudici di legittimità hanno precisato come per flusso di comunicazioni deve essere inteso la trasmissione di presenza o a distanza di informazioni da una fonte emittente ad una ricevente, non può ritenersi intercettazione di flusso di comunicazioni la captazione di un'elaborazione del pensiero esternata in scrittura su un personal computer[308].

Per quanto concerne l'applicabilità al caso di specie della disciplina prescritta dagli artt.359 e 360 c.p.p. per gli accertamenti tecnici irripetibili, la Corte ha evidenziato come l'attività realizzata dalla polizia giudiziaria di riproduzione dei *files* memorizzati non aveva comportato né la distruzione né l'alterazione dell'archivio informatico. Quindi si era trattato di un'attività sempre reiterabile alla cui esecuzione non era necessaria la partecipazione del difensore.

Questa argomentazione non sembra, però, tenere conto della circostanza che un sistema informatico nel quale viene inoculato un captatore subisce un'alterazione a livello strutturale[309], mutano infatti alcune funzioni del dispositivo in quanto il *trojan horse* permette ad un operatore da remoto di prendere possesso del sistema bersaglio, di effettuare una serie di operazioni che esulano dalla sfera volitiva dell'utente autorizzato ed infine di poter anche accidentalmente alterare il contenuto del sistema stesso non permettendo così alla difesa di ripetere le operazioni captative[310].

[308] L. BATTINIERI, *Ibidem*.

[309] Si veda *supra* § 2.

[310] S. ATERNO, *Il captatore informatico tra esigenze investigative e limitazione della privacy: un bilanciamento necessario e urgente (I parte*) , in *Sicurezza e Giustizia*, 2017, 3, p.20.

4.2.3 Considerazioni conclusive sul tema delle perquisizioni on line

Considerando le difficoltà riscontrate per cercare di inquadrare le perquisizioni *on line*, sia nella disciplina degli strumenti tipizzati dal codice, sia nell'ambito dell'art.189 c.p.p., potrebbe reputarsi opportuno un intervento normativo volto a disciplinare le modalità d'intromissione in un sistema informatico, i reati presupposto che giustificano tale attività d'indagine e il contenuto del provvedimento motivato dell'autorità giudiziaria.

Il legislatore, vista la quantità di dati con i quali gli inquirenti entrano in contatto nell'espletamento della perquisizione *on line* dovrebbe, inoltre, preoccuparsi di disporre idonee cautele per tutelare l'indagato introducendo espressamente la sanzione dell'inutilizzabilità del materiale probatorio acquisito illegittimamente o irrilevante[311] .

La recente delega conferita al Governo con la Legge n. 103 del 2017 per l'attuazione di dettaglio della riforma del regime delle intercettazioni si è occupata di regolamentare il captatore informatico riferendosi, però, alle sole intercettazioni "ambientali" e disciplinando esclusivamente l'ipotesi in cui l'installazione del *trojan horse* si realizzi in dispositivi elettronici portatili; e non viene preso in considerazione l'utilizzo di questo strumento di ricerca della prova in relazione ai dispositivi fissi.

Da questo punto di vista l'intervento riformatore è stato criticato in quando non prende in considerazione tutte le operazioni investigative eseguibili per mezzo del *trojan horse*[312], appare, infatti, riduttivo considerare il captatore informatico esclusivamente come strumento tecnico d'intercettazione e quindi solo come componente eventuale di questo mezzo di ricerca della prova[313].

Il legislatore, in questa riforma, non si è occupato delle perquisizioni *on line,* la cui indiscussa utilità investigativa si accompagna ad una inevitabile compressione di beni costituzionalmente tutelati, senza che di questa ingerenza siano stabiliti dal legislatore i casi e i modi.

---

[311] F. IOVENE, *op.cit.,* p.342.

[312] G. GIOSTRA-R. ORLANDI, *op cit*., p.290.

[313] M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 20 Dicembre 2018, p. 2.

Fintanto che questo mezzo di ricerca della prova non venga puntualmente regolamentato non si possono ritenere *tout court* legittime le perquisizioni e i relativi risultati utilizzabili, l'interprete dovrà verificare, quindi, di volta in volta e sulla base del caso la concreta possibilità di applicare la disciplina degli strumenti di ricerca della prova tipizzati dal codice come le perquisizioni tradizionali e le intercettazioni oppure le disposizioni concernenti le prove atipiche [314].

5. Il trojan horse nell'esperienza europea.

L'utilizzo del captatore informatico da parte degli organi inquirenti è stato oggetto di attenzione anche da parte degli altri Stati europei che, in considerazione della poliedricità di questo strumento investigativo, hanno adottato soluzioni differenziate.

Alcuni Stati come la Francia hanno tentato di tipizzare il captatore informatico attraverso una disciplina ad hoc, altri, invece, come l'Italia, sono pervenuti ad un'applicazione analogica di norme che regolamentano altri mezzi della ricerca della prova o sono ricorsi alla categoria della prova atipica[315].

In Francia, l'impiego del captatore informatico per l'acquisizione a distanza di dati e informazioni di natura digitale è possibile esclusivamente quando si procede per uno dei reati di cui al titolo 25 del codice di procedura penale francese, vale a dire delitti di criminalità e di delinquenza organizzata.

In relazione alla disciplina derogatoria in materia di criminalità organizzata il legislatore ha introdotto con l art. 706-102-1 c.p.p. la c.d. "*captation des données informatiques*" , applicabile ai delitti costituenti atti di terrorismo previsti dagli artt. 706-73 e 706-73-1 c.p.p. [316].

L''art. 706-102-1 c.p.p. disciplina l'utilizzo del captatore informatico che permette agli inquirenti di apprendere i dati memorizzati su un sistema informatico al fine di salvarli,

[314]G. GIOSTRA-R. ORLANDI, *op cit.,* p. 323.

[315] Sul tema delle perquisizioni *on line* come mezzo di ricerca della prova atipico cfr. Cap.II § 4.2.1.

[316] C.PELOSO, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo,* in *Dir. pen. cont.*, 2017,1, p. 159.

conservarli o trasmetterli così come sono ricevuti o trasmessi da dispositivi audiovisivi[317]. Il che si significa procedere a una perquisizione e a un sequestro a distanza con la conseguente omissione di tutte quelle garanzie previste in materia di perquisizioni e di sequestri tradizionali[318].

Il Codice di procedura penale francese, tuttavia, prevede una serie di cautele procedurali sulle modalità con cui tali operazioni devono essere effettuate, quali ad esempio l'obbligo per il giudice, a pena di nullità, di precisare il reato che giustifica il ricorso a tale mezzo informatico, la localizzazione esatta o la descrizione del sistema informatico e la durata delle operazioni (art. 706-102-3 c.p.p.). Il secondo comma dell'art. 706-102-1 c.p.p. dispone, inoltre, la creazione di liste di tecnici presso la *Cour de Cassation* e le *Cours d'appel* a cui affidare il compito di compiere le operazioni con il captatore informatico[319].

La legge francese introduce anche una serie di limiti all'utilizzo del captatore informatico. L'art. 706-102-4 comma 4 c.p.p., infatti, vieta la collocazione del *software s*pia negli uffici di avvocati e medici, negli studi di notai e ufficiali giudiziari, negli uffici di giornalisti giudici e parlamentari; mentre l'art. 706-102-8 c.p.p. dispone espressamente che ogni elemento relativo alla vita privata estraneo ai reati indicati nella decisione del provvedimento che autorizza la misura non può essere mantenuto nel fascicolo del processo[320].

Si segnala, infine, sempre in relazione all'esperienza francese in materia di sistemi di controllo da remoto, la legge n.731 del 3 giugno 2016 che ha introdotto gli artt. 706-95-4 e ss c.p.p. i quali disciplinano l*'IMSI catcher,* uno strumento tecnologico, simile ad un'antenna, che permette di captare e localizzare il numero di telefono e che, nelle versioni più aggiornate, può anche permettere di intercettare dati[321].

In Spagna con la *Ley Organica* n.13 del 2015 di modifica del Titolo VIII del libro II della *Ley de Enjuiciamento Criminal*, viene disciplinato compiutamente l'utilizzo del captatore informatico al fine di eseguire intercettazioni telefoniche e telematiche per il

---

[317] P. LE FÈVRE, *Il regime della captazione dei dati informatici nei diritto francese*, in *Parola alla Difesa*, 2016, 1, p. 181.

[318] P. LE FÈVRE, *Ibidem*.

[319] C.PELOSO, *op. cit.*, p. 160.

[320] P. LE FÈVRE, *op. cit.* p. 182.

[321] C.PELOSO, *op. cit.*, p. 161.

monitoraggio delle immagini e per la raccolta di registrazioni contenute in dispositivi di archiviazione di massa e in *computer* remoti. Il *trojan horse*, secondo quanto disposto dalla legge 13 del 2015, può essere utilizzato limitatamente alle indagini nelle quali questo strumento risulti necessario e sussidiario agli altri mezzi di ricerca della prova. La norma prevede inoltre che il decreto con cui il giudice autorizza l'utilizzo del captatore specifichi espressamente le generalità degli individui nei cui confronti vengono eseguite le intercettazioni, i luoghi e il *software* con il quale si procederà alla captazione[322].

Comparando le soluzioni adottate dai diversi Paesi europei riguardo l'utilizzo del *trojan horse* nell'ambito degli strumenti d'indagine a disposizione degli organi inquirenti, è opportuno segnalare che l'ordinamento giuridico portoghese ha ritenuto inammissibile il ricorso al captatore informatico in quanto lesivo di una pluralità di diritti costituzionalmente garantiti.

L'art. 125 del Codice di procedura penale portoghese dispone che ogni prova ottenuta attraverso la tortura, la coercizione o la violenza all'integrità personale fisica e morale, l'intromissione nella sfera privata di un soggetto, nel domicilio, nella corrispondenza o nelle comunicazioni telefoniche, va considerata nulla ed inutilizzabile conformemente a quanto disposto dalla stessa Costituzione[323].

La Costituzione portoghese, infatti, prevede espressamente all' art. 26, n.1 e 2 che ad ogni cittadino è garantito il diritto all'identità personale, allo sviluppo della personalità, alle capacità civili, alla cittadinanza, al nome e alla protezione della riservatezza della vita propria e della propria famiglia.

[322] M. TORRE, *op. cit.* p. 134.

[323] P. DE SÁ E CUNHA LEONOR CHASTRE, *L' utilizzo del captatore informatico trojan horse nella procedura penale portoghese*, in *Parola alla difesa*, 2016, 1, p. 183.

La legge deve, quindi, stabilire effettive garanzie riguardo l'acquisizione e l'utilizzo di informazioni attinenti alle persone e famiglie, nonché evitare la loro acquisizione o il loro utilizzo contrario alla dignità umana. Il ricorso al *virus trojan*, pertanto, è stato ritenuto dall'ordinamento inammissibile, in quanto non corrisponde ad alcuno strumento di acquisizione della prova previsto dal Codice di Procedura Penale portoghese (ad esempio, registrazioni telefoniche, intercettazioni ambientali o sequestro della corrispondenza) e può determinare un'indebita intromissione nella vita privata, nella corrispondenza o nelle comunicazioni telefoniche dell'individuo[324].

[324] P. DE SÁ E CUNHA LEONOR CHASTRE, *ivi*, p. 184.

Capitolo III

LE INTERCETTAZIONI DI COMUNICAZIONI TRA PRESENTI CON IL CAPTATORE INFORMATICO

SOMMARIO: 1. Inquadramento della captazione mediante *virus trojan horse* nell'ambito degli artt. 266 e ss. c.p.p. – 2. L'uso del captatore informatico nei soli procedimenti per i delitti di criminalità organizzata: gli approdi della Sezioni Unite nella sentenza "Scurato". – 2.1 Disciplina derogatoria all'art. 266 comma 2 per i reati di criminalità organizzata di cui all'art 13 d.l. 152/1991. – 2.2 Definizione di criminalità organizzata. – 3. Il regime di utilizzabilità del captatore informatico: gli approdi della delega "Orlando". – 3.1 Il decreto attuativo della delega "Orlando". – 3.2. L'art. 6 d.lgs. n. 216/2017 e la legge n.3/2019 (c.d. legge "spazza-corrotti" o "anticorruzione"): il regime speciale che accomuna reati di criminalità organizzata e delitti contro la pubblica amministrazione. – 3.2.1 Estensione della portata applicativa del captatore informatico. – 3.3 Il decreto autorizzativo "rafforzato". – 3.4 Modalità procedimentali di esecuzione dell'attività captativa. – 3.5. Divieto di utilizzazione per la prova di reati diversi.

1. Inquadramento della captazione di comunicazioni mediante virus trojan horse nell'ambito degli artt. 266 e ss. c.p.p.

Il captatore informatico assume particolare rilievo come strumento per la realizzazione d'intercettazioni di comunicazioni tra presenti poiché, una volta inoculato nel dispositivo portatile del soggetto sottoposto a indagine, consente agli inquirenti di attivare da remoto il microfono del dispositivo bersaglio per registrare le conversazioni e trasmetterle al centro di controllo.

Le intercettazioni di comunicazioni tra presenti mediante captatore sono meno legate all'ambiente da monitorare, quanto piuttosto al soggetto indagato e, per questa ragione, vengono definite "itineranti" perché, prescindendo dal riferimento del luogo, si spostano insieme al dispositivo infettato, permettendo all'apparato informatico nel quale viene immesso il virus di acquisire qualsiasi tipologia di comunicazione ovunque esso si trovi[325].

Sono chiari i vantaggi investigativi conseguenti all'uso del *software* spia rispetto all'impiego delle tecnologie tradizionali che si avvalgono essenzialmente di microspie fisse, installate segretamente ad opera della polizia giudiziaria nell'ambiente da monitorare.

Nonostante sotto il profilo tecnico-operativo sia evidente l'efficacia di questo strumento investigativo per l'accertamento dei reati, è doveroso interrogarsi sulla compatibilità delle intercettazioni di comunicazioni realizzate per mezzo del captatore informatico con la disciplina degli artt. 266 e ss, c.p.p.

Pertanto, al fine di applicare le disposizioni codicistiche in materia d'intercettazioni alla captazione tramite *virus trojan,* è necessario che oggetto della captazione siano effettivamente dati di natura comunicativa, vale a dire una comunicazione o conversazione tra più soggetti e non, invece, dati già memorizzati all'interno del dispositivo bersaglio (cd. dati non comunicativi)[326]. Lo scopo precipuo delle intercettazioni di cui gli artt. 266 e ss. c.p.p. è, infatti, rappresentato dall'apprensione contestuale ed occulta del contenuto di una conversazione o comunicazione tra soggetti anche nella forma di flusso informatico o telematico come previsto dall'art. 266-*bis* c.p.p.[327].

Da ciò consegue che quando oggetto della captazione è una comunicazione, sia che venga intercettata mediante le tecniche tradizionali sia che venga appresa con il captatore informatico, l'applicabilità della vigente disciplina giuridica in materia d'intercettazioni non dovrebbe essere messa in discussione[328].

---

[325] G. LA CORTE, *Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata*, in *Giurisprudenza Penale*, 2017, 6, p.7.

[326] M. TORRE, *op.cit*., p.25.

[327] C.MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p. 4.

[328] M. TORRE, *op.cit*., p. 26.

Tuttavia un profilo di criticità che si riflette sul tema dei reati intercettabili concernente il corretto inquadramento normativo delle intercettazioni di comunicazioni effettuate mediante il captatore informatico, riguarda l'applicazione dell'art. 266 c.p.p. piuttosto che l'art. 266-*bis* c.p.p[329].

Secondo un orientamento restrittivo le intercettazioni di comunicazioni vocali realizzate per mezzo del captatore informatico, riguardando pur sempre la captazione della voce umana, dovrebbero essere ricondotte agli stringenti limiti di ammissibilità[330] dell'art. 266 c.p.p.[331].

Per contro sussiste una tesi estensiva che ritiene applicabile alle intercettazioni realizzate con l'ausilio del *virus trojan horse* l'art. 266 *bis* c.p.p., consentendo in questo modo, il ricorso al captatore informatico non solo nei procedimenti relativi ai reati indicati nell'art. 266 c.p.p. ma anche a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche[332].

A sostegno della tesi estensiva è necessario segnalare un'argomentazione di natura sistematica: proprio il fatto che la legge n. 547/1993, introducendo nel codice di rito l'art. 266-*bis* c.p.p., abbia previsto una norma *ad hoc* concernente le intercettazioni informatiche e telematiche, esclude implicitamente che le "altre forme di comunicazione" a cui fa riferimento l'art. 266 c.p.p. includano quelle di natura informatica[333].

L'adesione alla tesi estensiva, svincolando il ricorso alle intercettazioni dagli stringenti limiti di ammissibilità dell'art. 266 c.p.p., presenta come indubbio vantaggio quello di riconoscere agli organi preposti all'accertamento ed alla repressione dei reati la possibilità di far fronte ad "armi pari" a qualsiasi forma di attività criminale che si realizza per mezzo di strumenti informatici[334].

A prescindere dai diversi orientamenti riguardanti l'applicabilità dell'art. 266 c.p.p. o dell'art. 266 *bis* c.p.p. alla captazione di comunicazioni con il virus *trojan horse*, la

---

[329] Sul tema delle intercettazioni telematiche cfr. *supra*, Cap. I, § 3.

[330] Sui limiti di ammissibilità delle intercettazioni cfr., *supra*, Cap. I, § 2.2.

[331] M. TORRE, *op.cit.*, p.27.

[332] M. TORRE, *ibidem.*

[333] M. TORRE *ibidem.*

[334] M. TORRE, *op.cit.*, p.28.

vigente disciplina giuridica in materia d'intercettazioni, rimanendo al passo dell'evoluzione tecnologica, appare idonea ad essere applicata anche nel caso in cui la captazione di comunicazioni consegua all'inoculazione, in un dispositivo bersaglio, di virus informatici.

In tal senso le Sezioni unite nella sentenza Scurato[335], dopo aver ricostruito compiutamente i presupposti delle intercettazioni tra presenti previste dall'art. 266, comma 2, c.p.p., sembrano condividere il principio di "neutralità tecnica" già affermato a livello europeo in materia di protezione dei dati personali. Secondo questo principio la normativa in materia d'intercettazioni dovrà trovare applicazione a prescindere dalla tecnologia utilizzata per l'esecuzione dell'attività di captazione[336].

Il canone della "neutralità tecnica" è definito compiutamente dalla Direttiva 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti. Il legislatore europeo in questo provvedimento prende in considerazione sia le sfide poste dall'evoluzione tecnologica sia le potenzialità intrusive di quest'ultime nei confronti della tutela delle informazioni più sensibili dell'individuo, ed evidenzia come nell'ambito dell'attività di prevenzione, indagine, accertamento e perseguimento di reati «*la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate*»[337].

[335] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato, in *C.e.d. Cass*., Rv. 266905.

[336] G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "tra presenti"*, nota a Cass., sez. un., 28 aprile 2016, n. 26889, Scurato, in *Dir. pen. cont.*, 7 Ottobre 2016, p. 11.

[337] Cfr. considerando (18) direttiva 2016/680/UE.

2. L'uso del captatore informatico nei soli procedimenti per i delitti di criminalità organizzata: gli approdi delle Sezioni unite nella sentenza "Scurato".

Nell'ambito delle intercettazioni ambientali gli organi inquirenti sempre più frequentemente ricorrono al *virus trojan*. Quest'ultimo opera come una microspia "telematica" e, rappresentando un'evoluzione tecnologia della microspia fissa collocata fisicamente nei luoghi di pertinenza dell'indagato, si installa furtivamente nel dispositivo bersaglio consentendo di controllare da remoto il microfono dello stesso. Il perimetro dell'intercettazione ambientale, quindi, grazie al captatore informatico conosce oggi una dirompente *vis* espansiva, non risultando più circoscritto al luogo in cui è collocato l'apparato microspia[338].

Se dal punto di vista investigativo, quindi, i vantaggi di questo mezzo di ricerca della prova sono evidenti, dal punto di vista giuridico l'installazione surrettizia di un *software* spia in un dispositivo elettronico portatile sembra determinare una potenziale compressione di valori fondamentali protetti dalla Costituzione, quali l'inviolabilità del domicilio (art. 14 Cost.) e la libertà e segretezza delle comunicazioni (art. 15 Cost.) [339].

Al fine di risolvere il contrasto con queste disposizioni costituzionali, sul tema delle intercettazioni di comunicazioni tra presenti realizzate con il captatore informatico, si sono avvicendate alcune significative pronunce da parte dei giudici di legittimità.

Una delle prime pronunce in materia è quella relativa al c.d. caso Bisignani[340] .

Si tratta di un'indagine su una presunta associazione di stampo P4, avviata dalla procura della Repubblica presso il Tribunale di Napoli. Nel caso di specie il ricorso al *software* spia non solo aveva permesso di avere accesso ai dati memorizzati nell'*hardware* del sistema informatico bersaglio, ma anche di effettuare intercettazioni ambientali attraverso il controllo della videocamera e del microfono del dispositivo. Per quest'ultimo caso, il giudice per le indagini preliminari disponeva l'autorizzazione *ex* art. 267 c.p.p. facendo rientrare tale attività, seppur effettuata per mezzo dello strumento atipico del captatore

---

[338] A. TESTAGUZZA, *I Sistemi di Controllo Remoto: fra normativa e prassi*, in *Dir. pen. proc*., 2014, p. 759.

[339] M. TORRE, *op.cit.*, p. 37.

[340] Cass., Sez. VI, 27 novembre 2012, n. 15009, Bisignani, in *C.e.d. Cass.*, Rv. 2548865.

informatico, all'interno delle intercettazioni ambientali. Per quanto riguarda, invece, l'attività investigativa consistente nell'estrapolazione di documenti e dati informatici già formati contenuti nella memoria del *personal computer*, i giudici di legittimità, non discostandosi dal *decisum* della Cassazione nella sentenza "Virruso"[341], ritenevano che questa attività non rientrasse dalla nozione d'intercettazione di comunicazioni o conversazioni e che non si ponesse in contrasto con l'art. 14 Cost[342]. Conseguentemente la Corte, nella decisione in esame, ricondusse al concetto di prova atipica di cui l'art. 189 c.p.p. la captazione, per mezzo dell'inoculazione del *trojan horse* in un dispositivo bersaglio, di dati non aventi ad oggetto «*un flusso bidirezionale o pluridirezionale di comunicazioni*»[343].

La Corte di cassazione nel 2015 con la sentenza "Musumeci"[344] torna, nuovamente, sulla questione delle intercettazioni realizzate per mezzo del captatore informatico, e ritiene non giuridicamente ammissibile la captazione tramite *virus trojan horse* delle conversazioni tra presenti mediante l'attivazione del microfono dell'apparecchio telefonico *smartphone*.

I giudici di legittimità sottolineano come la captazione di comunicazioni realizzata con questa metodica, consentendo l'intercettazione delle conversazioni in qualsiasi luogo in cui si rechi il soggetto con l'apparecchio infettato, contrasti, prima ancora che con la normativa codicistica, con l'art. 15 Cost. Infatti, l'unica interpretazione compatibile con il richiamato dettato costituzionale è quella secondo cui l'intercettazione tra presenti debba avvenire in luoghi ben circoscritti e individuati *ab origine* e non in qualunque luogo si trovi il soggetto[345].

Le Sezioni unite della Corte di cassazione con la sentenza Scurato[346], discostandosi dalla sentenza Musumeci, si pronunciano sul tema delle intercettazioni di conversazioni tra

---

[341] Cass., sez.V, 29 aprile 2010, n. 16556, Virruso, in *C.e.d. Cass*., Rv.246954.

[342] Sul rapporto tra perquisizioni *on line* e inviolabilità del domicilio (art. 14 Cost.) cfr., *supra*, Cap. II, § 4.1.2.

[343] Cass., sez. VI, 27 novembre 2012, n. 15009, Bisignani.

[344] Cass., sez. VI, 26 maggio 2015, n.27100, Musumeci, in *C.e.d. Cass*., Rv. 265655.

[345] *Ibidem.*

[346] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

presenti realizzate attraverso l'attivazione da remoto del microfono di un dispositivo mobile.

La decisione della Corte trae origine dal ricorso per Cassazione contro l'ordinanza, emessa dal Tribunale del riesame di Palermo, di conferma di una misura di custodia cautelare disposta sulla base degli indizi emersi da una serie d'intercettazioni "ambientali" svolte tramite *trojan horse*.

L'ordinanza veniva impugnata per due ordini di ragioni: da un lato il decreto, emanato dal pubblico ministero, aveva disposto l'intercettazione anche nei luoghi di privata dimora senza che fosse soddisfatto il requisito dell'attualità dell'azione criminosa previsto dall'art. 266, comma 2, c.p.p., dall'altro, la difesa contestava il fatto che la captazione fosse stata disposta senza che nel decreto di autorizzazione fossero indicati precisamente i luoghi dove avrebbe dovuto essere effettuata[347], richiamando a sostegno delle proprie argomentazioni la sentenza "Musumeci"[348]. Infatti, il già menzionato orientamento[349], basandosi sul dettato costituzionale dell'art. 15 Cost. secondo il quale la libertà e la segretezza delle comunicazioni sono inviolabili, sostiene che le norme che disciplinano le intercettazioni tra presenti sono di stretta interpretazione, ragion per cui non può considerarsi giuridicamente corretto attribuire alla norma codicistica una portata applicativa talmente ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si trovi[350].

Sul ricorso dell'indagato la sezione VI decideva di rimettere la questione alle sezioni unite in ragione della particolare delicatezza della materia considerando che il ricorso a strumenti investigativi, come il captatore informatico, determina una forte invadenza nella privacy dell'indagato e dei suoi conviventi intercettati, compromettendo di fatto valori tutelati dalla Costituzione e dalle Convenzioni internazionali al cui rispetto l'Italia è vincolata *ex* art. 117 Cost.[351].

---

[347] G. LASAGNI, *op.cit.* p.6.

[348] Cass., sez. VI, 26 maggio 2015, n.27100, Musumeci.

[349] Sulla sent. Musumeci cfr. *supra* § 2

[350] G. LA CORTE, *op.cit.*, p. 8.

[351] G. LA CORTE, *ibidem*.

La Corte, prima di pronunciarsi sull'ammissibilità delle intercettazioni tramite captatore informatico, ricostruisce sistematicamente la disciplina delle intercettazioni di conversazioni tra presenti[352], evidenziando come il termine intercettazione "ambientale" non trovi riscontro in nessun testo normativo, neppure nello stesso art. 266, comma 2, c.p.p.

Le sezioni unite precisano che la locuzione "ambientale" si è affermata in un'epoca nella quale questo genere di captazioni necessitavano della predisposizione di una microspia in un preciso ambiente, infatti lo stesso codice di rito ricorre all'espressione intercettazioni "tra presenti"[353].

I giudici di legittimità ritengono, inoltre, che il termine "ambientale" non costituisce un parametro normativo ma esclusivamente un termine ampiamente diffuso in dottrina, giurisprudenza e nel linguaggio comune[354].

La Corte procede, quindi, all'analisi di tutti i profili di criticità inerenti alla captazione tramite agente intrusore emersi anche nelle precedenti pronunce giurisprudenziali sul tema.

Innanzitutto, le Sezioni unite disconoscono l'orientamento della sentenza Musumeci[355] secondo il quale l'intercettazione delle conversazioni tra presenti sarebbe da ritenersi legittima solo se il relativo decreto autorizzativo individui con precisione i luoghi in cui eseguire l'attività captativa, considerando che la tecnica investigativa dell'agente intrusore è incompatibile con la pretesa d'indicare nel decreto autorizzativo con precisione e anticipatamente i luoghi interessati, perché l'intercettazione segue tutti gli spostamenti nello spazio del suo utilizzatore[356].

---

[352] M. TORRE, *op.cit.,* p. 38.

[353] M.GRIFFO, *op.cit.,* p. 32.

[354] G. LASAGNI, *op.cit.* p.7.

[355] Cass., sez. VI, 26 maggio 2015, n.27100, Musumeci.

[356] G. LA CORTE, *op.cit.,* p. 9.

I giudici di legittimità, pertanto, evidenziano come l'art. 266, comma 2, c.p.p. non imporrebbe come condizione di legittimità di un provvedimento d'intercettazione "tra presenti" la precisazione dello specifico luogo in cui deve essere svolta l'attività investigativa[357].

È stata la sola giurisprudenza a ritenere l'indicazione della *sedes intercettandi* un presupposto funzionale alla tutela dei diritti costituzionalmente garantiti.

Le Sezioni unite rilevano come neppure nella giurisprudenza della Corte europea dei diritti dell'uomo si possono trovare riscontri sulla necessità di predeterminare l'ambiente di svolgimento delle operazioni di captazione.

La Corte di Strasburgo tra le garanzie minime che il legislatore deve apprestare in materia d'intercettazioni richiede, infatti, la predeterminazione della tipologia delle comunicazioni oggetto d'intercettazione, l'attribuzione della competenza a disporre l'autorizzazione ad un organo indipendente, la ricognizione dei reati per cui tali mezzi invasivi sono applicabili, la determinazione dei limiti di durata e delle procedure da osservare[358]. È evidente come l'indicazione del luogo non figuri fra gli elementi necessari richiesti dalla Corte europea dei diritti dell'uomo[359].

La specificazione del "dove" nel provvedimento autorizzativo, secondo la Corte, invece, sarebbe necessaria soltanto quando la captazione intervenga nei luoghi indicati nell'art. 614 c.p. Infatti, l'art. 266, comma 2, c.p.p. dispone che, qualora l'attività di captazione si svolga all'interno di un luogo domiciliare, l'intercettazione sarà consentita solo se sussiste fondato motivo di ritenere che *ivi* si stia svolgendo l'attività criminosa.

Una volta precisato che, nel decreto di autorizzazione, l'indicazione del luogo di svolgimento delle intercettazioni tra presenti non è richiesta né dalla legge, né dalla giurisprudenza sovranazionale, salvo quando esse debbano realizzarsi in un luogo di privata dimora[360], le Sezioni unite procedono a risolvere le problematiche concernenti l'ammissibilità delle intercettazioni di comunicazioni tra presenti per mezzo del *virus trojan horse*.

---

[357] M.GRIFFO, *op. cit.*, p.36.

[358]Sul tema si veda Corte Edu, sent. del 4 Dicembre del 2015, Zakharov c.Russia ; allo stesso modo Corte Edu, sent. del 6 Giugno 2019, Bosak e altri c. Croazia.

[359] Corte Edu, sent. del 23 Febbraio del 2016, Capriotti c.Italia.

[360] G. LASAGNI, *op.cit.*, p. 7.

La decisione riguarda l'ammissibilità dell'intercettazione di conversazioni o comunicazioni tra presenti mediante l'installazione di un captatore informatico in dispositivi elettronici portatili (ad es. *personal computer, tablet, smartphone* ecc.) anche nei luoghi di privata dimora *ex* art. 614 c.p.[361]«*pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa*»[362].

Le Sezioni unite sostengono che l'intercettazione realizzata con il captatore informatico non consente d'individuare *ex ante* i luoghi entro i quali si realizzerà l'attività di captazione; da ciò ne consegue una fisiologica inconciliabilità con la necessità di dimostrare il fondato motivo di ritenere che in un determinato luogo si stia svolgendo l'attività criminosa, al fine di ottenere l'autorizzazione a svolgere intercettazioni ambientali domiciliari.

Tanto è vero che una volta che il *virus trojan horse* è inoculato nel dispositivo bersaglio, il giudice all'atto di autorizzare l'intercettazione tramite captatore non può prevedere o predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico (*smartphone, tablet* e *computer*) verrà introdotto e logicamente non potrà effettuare un «*adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale*»[363]. Ciò potrebbe dar luogo ad una pluralità d'intercettazioni nei luoghi di privata dimora che comporterebbero la violazione di limiti non soggetti ad alcuna eccezione e per i quali la determinazione dei luoghi è condizione di legittimità dell'autorizzazione. Anche qualora fosse teoricamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico infettato e sospendere la captazione nel caso d'ingresso di un luogo di privata dimora, sarebbe comunque impedito il controllo del giudice al momento dell'autorizzazione che verrebbe comunque disposta al buio[364].

La Corte, tuttavia, ricorrendo alla logica del "doppio binario processuale" rileva che questa modalità d'intercettazione di conversazioni tra presenti, per mezzo del captatore informatico, debba ritenersi inammissibile esclusivamente con riferimento ai reati c.d.

---

[361] Sul tema dei luoghi di privata dimora cfr., *supra*, Cap. I, § 4.1.1.

[362] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato (punto 1 motivazione).

[363] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato (punto 6 motivazione).

[364] *Ibidem*.

ordinari perché soltanto in relazione a questi ultimi, non essendo possibile prevedere i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto, non si può verificare il rispetto della condizione di legittimità richiesta dall'art. 266, comma 2, c.p.p.[365].

Qualora, invece, la captazione interessi i reati di "criminalità organizzata" per i quali l'art. 13 d.l. n. 152 del 1991, derogando al comma 2 dell'art. 266 c.p.p., esclude la necessità di dimostrare il fondato motivo di ritenere che nei luoghi domiciliari si stia svolgendo l'attività criminosa, il ricorso al captatore per la realizzazione delle intercettazioni di conversazioni tra presenti è legittimo e i risultati certamente utilizzabili[366].

In relazione ai procedimenti di criminalità organizzata, una volta venuta meno la limitazione di cui all'art. 266, comma 2, c.p.p., la Corte sostiene che « *l'installazione del captatore informatico in un dispositivo "itinerante" con provvedimento di autorizzazione adeguatamente motivato e nel rispetto delle disposizioni generali in materia di intercettazione, costituisce una delle principali modalità di attuazione delle intercettazioni al pari della collocazione di microspie*»[367].

2.1 Disciplina derogatoria per i reati di criminalità organizzata di cui all'art 13 del decreto legge 13 Maggio 1991 n. 152.

Con l'art. 13 del d.l. n.152/1991 il legislatore ha introdotto una serie di deroghe alla disciplina processuale e al diritto penitenziario, attraverso la predisposizione del c.d. "doppio binario" per l'accertamento dei reati di criminalità organizzata[368].

Le intercettazioni telefoniche e le captazioni ambientali, pertanto, quando si tratta di criminalità organizzata soggiacciono a parametri di ammissibilità parzialmente diversi. La *ratio* dell'introduzione di una disciplina diversificata secondo alcuni Autori va ricercata nella necessità di reagire a interpretazioni distorte della locuzione "gravi indizi

[365] L.GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.*, 2017, 3, p. 177.

[366] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato. (punto 10.1 motivazione)

[367] *Ibidem*

[368] Sulla nozione di criminalità organizzata cfr. *infra* § 2.2.

di reato"[369] di cui l'art. 267 c.p.p., in base alle quali l'ipotesi di reato avrebbe dovuto essere ascritta, al momento dell'autorizzazione, ad un soggetto determinato[370].

Un'altra giustificazione della deviazione dalla normativa generale in materia d'intercettazioni per i delitti di criminalità organizzata veniva individuata nel fatto che il requisito dell'"assoluta indispensabilità" ai fini della prosecuzione delle indagini, impediva di fronteggiare quelle attività criminose nelle quali è l'intercettazione a consentire l'acquisizione del primo indizio[371].

Tuttavia, nessuna delle due ragioni addotte appare pienamente condivisibile. Per quanto riguarda la prima l'art. 267, comma 1, c.p.p. impone che i gravi indizi siano da riferirsi al reato e non alla responsabilità del soggetto da intercettare; relativamente alla seconda, l'intercettazione deve essere disposta sulla base di una «*piattaforma indiziaria, non procedere alla cieca alla ricerca di elementi utili per le indagini*»[372].

Le ragioni di questa deroga alla disciplina ordinaria in materia d'intercettazioni devono essere piuttosto ricercate nel fatto che i delitti di criminalità organizzata vengono perpetrati da associazioni criminose connotate da una pressante forza intimidatrice e dalla piaga del fenomeno omertoso che rendono inattendibili le fonti di prova testimoniali, spingendo gli inquirenti a ricorrere ai mezzi di ricerca della prova "a sorpresa" come le intercettazioni[373].

L'art. 13 del d.l. 152/1991 per l'accertamento dei delitti di criminalità organizzata prevede un affievolimento dei presupposti delle intercettazioni: indizi meno convincenti di quelli richiesti in via ordinaria e uno «*spostamento all'indietro (cioè verso i primi passi delle indagini preliminari) dell'istituto*»[374].

---

[369] Sul tema dei "gravi indizi di reato" e "assoluta indispensabilità per la prosecuzione delle indagini" cfr. supra Cap. 1 § 2.3

[370] P.L. VIGNA, *Il processo accusatorio nell'impatto con le esigenze di lotta alla criminalità organizzata,* in *Giustizia penale*,1991, 3, p. 466.

[371] Sul tema cfr. Delibera del 21 Giugno 1990 del C.S.M., p. 233.

[372] C.DI MARTINO-T.PROCACCIANTINI, *op.cit.*, p. 118.

[373] A.CAMON, *op.cit.*, p.81.

[374] A.CAMON, *ivi*, p.82.

Gli indizi richiesti dall'art. 267 c.p.p. per disporre le intercettazioni per i delitti di criminalità organizzata, infatti, da "gravi" sono stati degradati a "sufficienti"[375].

Dal punto di vista tecnico è quasi impossibile tracciare una linea di demarcazione tra "gravi" e "sufficienti" indizi e, secondo alcuni Autori, l'intervento legislativo esplica i propri effetti principalmente sul piano psicologico, esaurendosi in una sollecitazione nei confronti dei magistrati affinché emettano agevolmente il decreto di autorizzazione, valutando con minor rigore i presupposti delle intercettazioni[376].

Sempre in deroga alla disciplina ordinaria, l'art. 13 del d.l. 152/1991 prevede non che l'intercettazione sia "assolutamente indispensabile" ma che sia "necessaria" e logicamente può anche non costituire l*'extrema ratio*. Inoltre, la necessità va rapportata non alla "prosecuzione", come previsto dall'art. 267 c.p.p., ma allo svolgimento delle indagini con la conseguenza che questo mezzo di ricerca della prova potrà essere utilizzato anche nella fase di avvio delle indagini preliminari.

Un'ulteriore deroga per i reati di criminalità organizzata prevista dall'art. 13 d.l. 152/1991 riguarda il periodo di durata delle intercettazioni che da quindici giorni passa a quaranta giorni. Le proroghe hanno durata più lunga (venti giorni) e in base all'art. 267, comma 2, c.p.p. possono essere stabilite dal pubblico ministero in via d'urgenza e salvo convalida dal giudice per le indagini preliminari entro le quarantotto ore dall'adozione del provvedimento.

Per i reati in argomento, ancora, in deroga al disposto dell'art. 267, comma 4, c.p.p. il pubblico ministero e l'ufficiale di polizia giudiziaria possono farsi coadiuvare da agenti di polizia giudiziaria.

Tuttavia, il termine "coadiuvare" ha suscitato alcune perplessità perché può ragionevolmente attendersi che, nella prassi, i rapporti tra l'agente incaricato ad ascoltare i colloqui e il suo superiore finiscano con il ridursi a qualche istruzione sul modo in cui usare le apparecchiature lasciando per il resto incontrollati gli esecutori materiali dell'ascolto[377].

---

[375] C.DI MARTINO-T.PROCACCIANTINI, *op.cit*., p. 119

[376] F.CORDERO, *sub artt. 266-267, in Codice di procedura penale commentato*, Torino, 1992, p.310.

[377] A.CAMON, *op.cit*., p.150.

Infine, l'art. 13 d.l. 152/1991, come norma speciale rispetto all'art. 266, comma 2, c.p.p., dispone testualmente che «*quando si tratta d'intercettazione di comunicazioni tra presenti disposta in un procedimento relativo ad un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'art. 614 del codice penale, l'intercettazione è consentita anche se non vi è fondato motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa*».

Quest'ultima risulta essere la deroga alla disciplina ordinaria delle intercettazioni che più interessa alla luce delle determinazioni delle Sezioni unite nella sentenza Scurato[378] in relazione alle intercettazioni di comunicazioni tra presenti realizzate per mezzo del captatore informatico.

2.2 Definizione di criminalità organizzata.

Nella sentenza Scurato[379] le Sezioni unite, in riferimento alle intercettazioni di comunicazioni tra presenti realizzabili per mezzo dell'inoculazione nel dispositivo bersaglio del virus trojan *horse*, enunciano il seguente principio di diritto: «*limitatamente ai procedimenti per i delitti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad. es., personal computer, tablet, smartphone, ecc.) - anche nei luoghi di privata dimora ex articolo 614 codice penale, pur non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa*»[380].

Dalla decisione in commento discende la necessità di individuare con chiarezza la categoria dei delitti di criminalità organizzata.

Nell'ordinamento italiano non sussiste una compiuta definizione di criminalità organizzata; questa nozione può essere ricavata da elementi criminologici, sociologici o dalle convenzioni internazionali che si sono occupate della materia come la Convenzione ONU "*Transnational Organized Crime*" ratificata con la legge 146/2006.

---

[378] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

[379] *Ibidem.*

[380] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato (punto 11 motivazione).

Anche in assenza di una definizione puntuale il sistema italiano conosce cinque varianti di criminalità organizzata: quella comune, riconducibile allo schema dell'associazione per delinquere *ex* art. 416 c.p che si riscontra tutte le volte in cui un gruppo di soggetti si associa al fine di commettere delitti comuni; l'associazione di tipo mafioso *ex* art. 416 *bis* c.p. finalizzata alla commissione di delitti e alla realizzazione di attività lecite per mezzo del metodo mafioso (ad esempio l'acquisizione di concessione o appalti, il controllo di attività economiche e il condizionamento di voti favorevoli durante le competizioni elettorali); le associazioni monotematiche costituite per la gestione di singole attività delittuose (ad esempio un'associazione finalizzata alla tratta degli esseri umani *ex* art. 416 c.p.) ed infine le associazioni con finalità di terrorismo o di eversione dell'ordine democratico *ex* art. 270 e ss. c.p[381].

Una volta individuati i fenomeni criminosi riconducibili nell'alveo della criminalità organizzata, è necessario ricostruire il significato specifico da attribuire a questa espressione.

Sul tema sussistono due filoni interpretativi. Un primo orientamento ricostruisce la nozione di criminalità organizzata secondo un parametro socio-criminologico non individuando con precisione i delitti compresi in questa categoria[382].

Tanto è vero che viene ricondotto nell'ambito della criminalità organizzata non solo il delitto dell'associazione per delinquere di cui all'art. 416 c.p. nel quale la struttura organizzativa, anche minima, purché idonea a realizzare gli obiettivi criminosi è un elemento strutturale della fattispecie incriminatrice, ma anche le ipotesi di concorso di persone nel reato quando sono connotate da una suddivisione dei compiti tra gli autori del reato che collaborano per raggiungere un obiettivo antigiuridico[383]. In questo senso rientrano nella nozione di criminalità organizzata i reati che a qualsiasi titolo sono connessi ad associazioni criminali o alle attività di tali associazioni[384] .

---

[381] M. GRIFFO, *op. cit*., p.36.

[382] A.CAMON, *op.cit*., p.83.

[383] D.MANZIONE, *Una normativa «d'emergenza» per la lotta alla criminalità organizzata e la trasparenza e il buon andamento dell'attività amministrativa (D.l. 152/91 e L.203/91): uno sguardo d'insieme*, in *Legislazione pen*ale, 1992, p.851.

[384] M. MADDALENA, *I problemi pratici delle inchieste di criminalità organizzata nel nuovo processo penale*, in *Processo penale e criminalità organizzata* a cura di V. GREVI, Roma-Bari, 1993, p.83.

La stessa Corte di cassazione ha evidenziato che nel concetto di criminalità organizzata rientrano le più diverse attività criminose purché realizzate da una pluralità di soggetti che per la commissione di più reati abbiano costituito una struttura organizzativa che assume un ruolo preminente rispetto ai singoli partecipanti della stessa[385].

Secondo questa prima esegesi, quindi, il concetto di criminalità organizzata ricomprende sia il delitto di associazione per delinquere di cui l'art. 416 c.p che il concorso di persone nel reato di cui l'art. 110 c.p. nonostante la fattispecie associativa e quella concorsuale descrivano fenomeni delittuosi distinti. Nell'associazione per delinquere il vincolo associativo ha natura tendenzialmente permanente o quantomeno stabile poiché è destinato a perdurare oltre il compimento dei delitti che siano stati eventualmente programmati. Nel concorso di persone, invece, l'accordo assume un carattere meramente occasionale, essendo legato in modo diretto alla realizzazione di uno o più reati individuati che una volta commessi esauriscono l'accordo tra i correi[386]. L'accordo tra più soggetti per realizzare uno o più reati, quindi, è un elemento comune alla fattispecie associativa ed a quella concorsuale, in quest'ultima ipotesi il reato sotteso deve essere realizzato, quantomeno nella forma del tentativo, altrimenti i partecipanti all'accordo non sono punibili in forza dell'art. 115, comma, c.p. Diversamente, nell'associazione per delinquere il vincolo associativo, idoneo a commettere una indefinita serie di reati ,costituisce di per sé un pericolo per l'ordine pubblico, divenendo irrilevante la mancata consumazione dei delitti programmati[387].

Il secondo filone interpretativo sul tema del significato da attribuire alla locuzione "criminalità organizzata" è caratterizzato da tesi che indicano specificamente i delitti ricompresi in questa categoria.

Precisamente, alcuni Autori fanno riferimento esclusivamente ai reati previsti dall'art. 51, comma 3-*bis,* c.p.p[388]; Altri, invece, si riferiscono a questi stessi reati e a quelli di cui l'art. 372, comma 1-*bis*, c.p.p. ascrivendo ai primi la denominazione di "reati di

---

[385] Cass. pen., sez.VI, 20 novembre 1997, n.1972, Pacini Battipaglia, in *C.e.d. Cass*., Rv. 210045.

[386] Cass. pen., sez. VI, 8 Maggio 2013, n. 19783, in *C.e.d. Cass*., Rv. 255472.

[387] *Ibidem*.

[388] R. ORLANDI, *Il procedimento penale per fatti di criminalità organizzata: dal maxi-processo al grande processo*, in *Atti dell'incontro di studio su "Lotta alla criminalità organizzata: gli strumenti normativi"*, a cura di G.GIOSTRA e G. INSOLERA, Milano 1995, p.88.

criminalità organizzata in senso stretto" e ai secondi "reati di criminalità organizzata in senso ampio"[389].

Le sezioni unite nella sentenza Scurato[390] evidenziano come la corretta individuazione della nozione di criminalità organizzata non deve essere considerata un mero esercizio teorico perché da essa dipende l'applicazione delle norme processuali che si riferiscono specificamente a questa categoria di reati, tra le quali proprio l'art. 13 d.l. n.152/1991.

La Corte attribuisce validità all'approccio teleologico secondo il quale il significato dell'espressione "criminalità organizzata" deve essere definito facendo riferimento alle finalità specifiche della singola disciplina che deroga alle regole processuali generali[391].

In questo modo si avalla una nozione ampia e comprensiva di una pluralità di attività criminose eterogenee, realizzate da una pluralità di soggetti che per la commissione del reato abbiano costituito un apposito apparato organizzativo con esclusione del mero concorso di persone[392].

Le Sezioni unite hanno, quindi, ritenuto sufficiente ai fini dell'integrazione di una fattispecie di criminalità organizzata la sussistenza del requisito della stabile organizzazione programmaticamente ispirata alla commissione di più reati e ciò in considerazione del particolare allarme sociale che qualsiasi struttura associativa criminale suscita nell'opinione pubblica[393].

La sentenza in esame, pertanto, ricorre ad un parametro socio-criminologico che permette di cogliere l'essenza dei delitti di criminalità organizzata e nello stesso tempo di «*ricomprendere tutti i suoi molteplici aspetti, nell'ottica riconducibile alla ratio che ha ispirato gli interventi del legislatore in materia, tesi a contrastare nel modo più efficace*

---

[389] G. CONSO, *La criminalità organizzata nel linguaggio comune*, in *Giustizia Penale*,1992, 3, pp. 385-392.

[390] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

[391] L.GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo, op.cit.*, p. 185.

[392] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato (punto 16 motivazione): « *Per reati di criminalità organizzata devono intendersi non solo quelli elencati nell'articolo 51, commi 3-bis e 3-quater, codice di procedura penale, ma anche quelli comunque facenti capo a un'associazione per delinquere, ex articolo 416 codice penale, correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato*».

[393] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato (punto 13 motivazione).

quei reati che per la struttura organizzativa che presuppongono e per le finalità perseguite costituiscono fenomeni di elevata pericolosità sociale»[394].

Un profilo critico conseguente alla presa di posizione delle Sezioni unite nella sentenza Scurato sulla nozione di criminalità organizzata è la difficoltà di tracciare un confine sufficientemente delineato, nella fase delle indagini preliminari, tra la fattispecie associativa ed il mero concorso di persone[395].

Ne potrebbe conseguire, quindi, un pericolo di strumentalizzazione della struttura associativa in quanto potrebbero realizzarsi intercettazioni tramite captatore informatico fondate su ipotesi di reati associativi, configurati come una sorta di illecito "contenitore", magari senza una specifica individuazione dei delitti scopo dell'associazione ipotizzata[396].

In altre parole, attraverso la qualificazione giuridica come reato associativo di un fatto sarebbe possibile ottenere l'autorizzazione ad eseguire le intercettazioni di comunicazioni per mezzo del captatore informatico per l'accertamento di reati rispetto ai quali non è esperibile l'impiego di questo strumento investigativo.

Questa pratica, inoltre, è incentivata da quel consolidato orientamento giurisprudenziale[397] secondo il quale la legittimità dell'intercettazione deve essere valutata al momento della richiesta e della concessione dell'autorizzazione «*non potendosi procedere ad una sorta di controllo diacronico della sua ritualità sulla base delle risultanze derivanti dal prosieguo delle captazioni e dalle altre acquisizioni*»[398].

---

[394] *Ibidem.*

[395] M. GRIFFO, *op. cit.*, p.37.

[396] L.GIORDANO, *op.cit.*, p. 181.

[397] Cass., sez. VI, sent. 13 giugno 2017, n.36874, Romeo, in *C.e.d. Cass.*, Rv.270812.

[398] *Ibidem.*

Di conseguenza, le intercettazioni di comunicazioni giustificate dall'originaria prospettazione circa la sussistenza di un reato di criminalità organizzata sono utilizzabili anche se nel corso del procedimento si determina un mutamento nella qualificazione giuridica del fatto[399].

Per scongiurare il pericolo di strumentalizzazione del reato associativo è necessario fare affidamento sulla funzione di garanzia del decreto autorizzativo[400]. Nella sentenza "Romeo"[401] la Corte di cassazione ha ritenuto che, in considerazione del mezzo tecnologico utilizzato per la captazione delle conversazioni (ossia il virus *trojan horse*), è necessario rispettare un onere motivazionale particolarmente intenso al fine di emettere il provvedimento autorizzativo[402].

Pertanto, la forza intrusiva del captatore informatico e il potenziale *vulnus* all'esercizio di libertà costituzionalmente garantite devono essere bilanciati con il rispetto dei canoni di proporzione e ragionevolezza, in modo che la qualificazione del fatto come delitto di criminalità organizzata sia suffragata da sufficienti, sicuri ed obiettivi elementi indiziari[403].

Secondo la Corte dalla preminente funzione di garanzia riconosciuta al decreto di autorizzazione ne discende che il bilanciamento tra i diritti costituzionalmente garantiti deve essere effettuato proprio nella motivazione del provvedimento autorizzativo che dovrà spiegare compiutamente con precisione quale sia «*il criterio di collegamento tra l'indagine in corso e la persona da intercettare*»[404].

---

[399] Sul tema, a fronte dell'indirizzo giurisprudenziale prevalente che elimina le conseguenze della diversa qualificazione del fatto per il quale sono state disposte le intercettazioni, sussiste un orientamento che è contrario all'utilizzo dei risultati delle intercettazioni per reati per i quali non sussistono i presupposti di ammissibilità dell'istituto. In tal senso si veda Cass., Sez.II, 18 dicembre 2015, n.1924 in *C.e.d. Cass*., Rv.265989; Cass., Sez.III, 25 Febbraio 2010, n.12562, in *C.e.d. Cass*., Rv.246594.

[400] M. GRIFFO, *op. cit*., p.37.

[401] Cass., sez. VI, sent. 13 giugno 2017, n.36874, Romeo.

[402] L.GIORDANO, *La prima applicazione della sentenza "Scurato" nella giurisprudenza di legittimità*, *Dir. pen. cont.*,2017, 9, p.186.

[403] Cass., sez. VI, sent. 13 giugno 2017, n.36874, Romeo.

[404] *Ibidem*.

Secondo questa impostazione il giudice è tenuto a dare conto della ragione dell'intrusione nella sfera della libertà di comunicazione altrui evidenziando quale sia il rapporto tra il soggetto intercettato e le investigazioni in corso[405].

Al fine di garantire il corretto impiego del virus *trojan horse* per l'esecuzione delle intercettazioni, oltre che far affidamento sulla funzione di garanzia del decreto autorizzativo, bisogna contare sulla professionalità del giudice per le indagini preliminari e del pubblico ministero[406].

Il primo deve, conformemente a quanto disposto dalla Corte di cassazione nella sentenza "Romeo"[407], verificare con puntualità i presupposti per l'adozione del provvedimento di autorizzazione. Invece il pubblico ministero è tenuto a descrivere, nella richiesta d'intercettazione al giudice per le indagini preliminari, l'operatività del *software* e le funzioni che si intendono attivare; nella fase esecutiva deve disporre la precisa verbalizzazione delle operazioni con le quali è avvenuta l'installazione del virus nel dispositivo bersaglio ed infine procedere al sequestro del dispositivo per garantire in dibattimento il contraddittorio sulle modalità di raccolta delle prove[408].

[405] L.GIORDANO, *La prima applicazione della sentenza "Scurato" nella giurisprudenza di legittimità*, *op.cit.*, p. 181.

[406] L.GIORDANO, *Ibidem*.

[407] Cass., sez. VI, sent. 13 giugno 2017, n.36874, Romeo

[408] F. CAJANI, *Odissea del captatore informatico*, in *Cassazione Penale*,2016, 11, p. 4151.

3. Il regime di utilizzabilità del captatore informatico: gli approdi della delega "Orlando".

Il dibattito che si è sviluppato in merito all'uso del virus *trojan horse* per la realizzazione di intercettazioni di comunicazioni tra presenti, ha indotto il legislatore ad introdurre nel corso dei lavori preparatori della riforma Orlando un principio direttivo contenuto nell'art. 1 comma 84, lett. *e),* della legge 103/2017 con cui ha conferito una delega al governo per disciplinare compiutamente le intercettazioni di comunicazioni o conversazioni tra presenti realizzate per mezzo dell'inoculazione di captatori informatici in dispositivi elettronici portatili[409].

Bisogna accogliere con favore l'attenzione riposta dal legislatore su un tema controverso come quello del captatore informatico che è diventato, nel giro di pochi anni, elemento centrale del panorama giurisprudenziale in quanto sull'argomento si sono avvicendate una pluralità di pronunce[410] dei giudici di legittimità.

Il legislatore, nonostante fosse consapevole dei rischi connessi all'utilizzo di questo strumento d'indagine, appariva animato da uno "spirito progressista" poiché, discostandosi dai più recenti orientamenti europei che conferiscono al captatore una finalità preventiva, attribuiva al *software* spia una funzione repressiva[411].

È apprezzabile, inoltre, l'interesse della riforma a regolamentare gli aspetti tecnici del *trojan horse* se pur limitatamente alla funzione inerente all'attivazione del microfono del dispositivo nel quale viene inoculato il virus informatico[412].

Le indicazioni della delega sul tema delle intercettazioni di comunicazioni realizzate per mezzo del captatore informatico hanno determinato una parziale rilettura circa gli approdi raggiunti sul tema dalla giurisprudenza nella sentenza Scurato[413].

---

[409] M. GRIFFO, *op. cit*., p.38.

[410]Si veda in tal senso Cass., sez.V, 29 aprile 2010, n. 16556, Virruso.; allo stesso modo Cass., sez. VI, 26 maggio 2015, n.27100, Musumeci; Cass., sez. VI, 27 novembre 2012, n. 15009, Bisignani; Cass., sez. un., 28 aprile 2016, n. 26889, Scurato e Cass., sez. VI, sent. 13 giugno 2017, n.36874, Romeo.

[411] D.CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *Jiusonline*,2017, 3, p. 391.

[412] D.CURTOTTI, *Ibidem*.

[413] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

In primo luogo, il comma 84 lett. *e)* della legge 103/2017 prevede che l'attivazione del microfono del dispositivo bersaglio possa realizzarsi esclusivamente per mezzo di un apposito comando inviato da remoto e non nel momento dell'immissione del virus *trojan horse*. Inoltre, ciò deve avvenire nei limiti stabiliti da un decreto autorizzativo emanato da un giudice.

La previsione concernente l'attivazione del microfono da remoto permette di introdurre attraverso il captatore informatico una forma di «*monitoraggio monitorante*»[414] vale a dire la possibilità di attivare o disattivare il microfono all'occorrenza.

In questo modo si potrebbero superare le criticità avanzate dalla giurisprudenza[415] in relazione all'impossibilità di predeterminare i luoghi oggetto della captazione tramite il virus *trojan horse* e, come nelle intercettazioni realizzate con le tecniche tradizionali, sarebbe possibile indicare nel decreto autorizzativo i luoghi nei quali il dispositivo potrà essere attivato da remoto[416].

Tuttavia, si deve sottolineare come l'attivazione e disattivazione continua del dispositivo bersaglio da remoto potrebbero determinare un esaurimento della batteria dello stesso con il rischio che il soggetto intercettato percepisca la presenza del virus[417].

Un altro profilo di criticità è ravvisabile nel fatto che un controllo costante del captatore con il fine di disattivarlo nel rispetto dei limiti del decreto autorizzativo determinerebbe un ingente dispendio di personale[418].

Ciò nondimeno la maggior distanza tra la legge delega 103/2017 e gli approdi della sentenza Scurato è ravvisabile nella delimitazione dell'ambito applicativo del *software* spia.

Tanto è vero che il comma 84 lett. *e)* prevede che le intercettazioni tramite captatori informatici siano sempre ammissibili nel caso in cui si proceda per i delitti di cui l'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., invece, per l'accertamento dei delitti diversi da quelli menzionati è sempre possibile ricorrere alla captazione con il *trojan horse* nei luoghi

---

[414] D.CURTOTTI, *op. cit.,* p. 399.

[415] Si veda in tal senso Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

[416] D.CURTOTTI, *op. cit.*,p.400.

[417] D.CURTOTTI, *Ibidem.*

[418] C.PARODI, *La riforma "Orlando": la delega in tema di "captatori informatici",* 4 Aprile 2017, in www.magistraturaindipendente.it, p. 3.

diversi da quelli di privata dimora di cui l'art. 614 c.p., dove l'intercettazione è autorizzabile dal giudice soltanto qualora sussista il fondato motivo di ritenere che *ivi* si stia svolgendo l'attività criminosa. In ogni caso il decreto autorizzativo del giudice dovrà indicare le ragioni per le quali tale modalità d'intercettazione particolarmente invasiva sia necessaria per lo svolgimento delle investigazioni[419].

La scelta del legislatore è ben diversa dalla soluzione adottata dalla Corte di cassazione nella sentenza Scurato che aveva «*circoscritto diffusamente*»[420] l'ambito di applicazione delle intercettazioni con il captatore informatico: "circoscritto" nel senso che aveva ritenuto legittimo il ricorso a questo mezzo di ricerca della prova per i soli delitti di criminalità organizzata per i quali, ai sensi dell'art. 13 d.l. 152/1991, le intercettazioni nei luoghi di privata dimora sono ammesse senza limiti, "diffusamente" in quanto la nozione di criminalità organizzata era tale da ricomprendere ogni delitto sussumibile nel modulo d'incriminazione di cui l'art. 416 c.p con esclusione del mero concorso di persone nel reato[421].

È evidente, quindi, l'asimmetria tra gli ambiti di ammissibilità che appaiono «*come cerchi intersecantisi*»[422] poiché da un lato la scelta legislativa restringe il numero dei reati per l'accertamento dei quali è consentito il ricorso al captatore informatico, che passa dall'ampio perimetro dei delitti di criminalità organizzata al più ristretto cerchio dei delitti di mafia e di terrorismo (art. 51, comma 3-*bis* e 3-*quater* c.p.p.), dall'altro «*il legislatore delegante fa rientrare dalla finestra ciò che le sezioni unite sembravano aver fatto uscire dalla porta principale, ossia la possibilità d'impiegare il captatore informatico per i reati comuni*»[423].

Il comma 84 lett. *e)* della l. 103/2017 specifica che le intercettazioni ottenute tramite *trojan horse* potranno essere utilizzate ai fini probatori soltanto per i reati oggetto del provvedimento autorizzativo e introduce una serie di previsioni di carattere tecnico che riguardano le modalità procedimentali d'intercettazione tramite captatore informatico.

---

[419] M. GRIFFO, *op. cit.*, p38.

[420] O.CALAVITA, *L'odissea del trojan horse*, in *Dir. pen. cont.*,2018, 11, p.57.

[421] O.CALAVITA, *Ibidem*.

[422] M. TORRE, *il Captatore informatico nella legge delega 23 Giugno 2017, n.103*, in *Jusonline*, 2017, 3, p.438.

[423] M. TORRE, *ibidem*.

Il legislatore delegante, pertanto, prevede che la registrazione audio, mediante attivazione da remoto del dispositivo infettato, dovrà essere avviata dalla polizia giudiziaria o dal personale incaricato su indicazione della polizia operante, la quale sarà tenuta ad indicare necessariamente l'ora d'inizio e fine della registrazione, secondo circostanze da indicare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui l'art. 268 c.p.p.

Il trasferimento dei *file* registrati, inoltre, dovrà essere effettuato soltanto verso il *server* della procura e, una volta terminata la captazione, il *trojan* dovrà essere reso inutilizzabile.

Conclusivamente la legge delega dispone che nei casi d'urgenza il pubblico ministero potrà disporre questa tipologia d'intercettazioni, limitatamente al fatto che si proceda per i delitti di cui l'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. con successiva convalida da parte del giudice entro quarantotto ore. Il decreto d'urgenza dovrà dare conto delle specifiche situazioni di fatto che rendono impossibile la richiesta al giudice.

3.1 Il decreto attuativo della delega "Orlando".

Con il d.lgs. n.216/2017 il Governo ha dato seguito alla delega legislativa attribuitagli dall'art. 1, comma 84, della l.103/2017 i cui criteri direttivi sono così dettagliati da *«far pensare ad una veste normativa pressoché definitiva»*[424].

Questa riforma è considerata da alcuni Autori anacronistica *ab origine* perché il parlamento ha conferito la delega al governo in materia di intercettazioni tramite captatore informatico assumendo come punto di riferimento i principi enunciati dalle Sezioni unite nella sentenza Scurato e da ciò ne discende che il decreto delegato disciplina esclusivamente l'uso del captatore per l'esecuzione di intercettazioni tra presenti attraverso l'attivazione del microfono[425]. In questo modo il legislatore ha dimostrato di non tener conto della poliedricità del captatore informatico[426].

[424] D.CURTOTTI, *op. cit*, p. 383.

[425] Si veda D.CURTOTTI, *op. cit,* p.389; allo stesso modo O.CALAVITA, *op.cit.,* p.57.

[426] M. TORRE, *Il Captatore informatico nella legge delega 23 Giugno 2017, n.103, op.cit.,* p.437.

Il Governo, nel regolamentare l'uso del captatore informatico, con l'art. 4 d.lgs. 216/2017, rubricato «*modifiche al codice di procedura penale in materia d'intercettazioni mediante inserimento di captatore informatico*», ha introdotto un nuovo periodo nell'art. 266, comma 2, c.p.p. in forza del quale è consentita l'intercettazione di comunicazioni tra presenti «*anche mediante l'inserimento del captatore informatico su un dispositivo elettronico portatile*»[427] . Inoltre, dando attuazione ai principi direttivi contenuti nella legge delega, il d.lgs. 216/2017 introduce il comma 2-*bis* dell'art. 266 c.p.p. in base al quale: «*L'intercettazione di comunicazioni tra presenti mediante inserimento del captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui l'art. 51, commi 3 bis e 3 quater, c.p.p.*».

In primo luogo, è necessario sottolineare come conformemente a quanto previsto dalla legge delega, il d.lgs. 216/2017 stabilisce che le intercettazioni realizzate con la "cimice informatica" possano realizzarsi esclusivamente per mezzo dell'immissione del virus *trojan horse* in un dispositivo elettronico caratterizzato da "portabilità"[428].

In secondo luogo il Governo, per mezzo della modifica dell'art. 266 c.p.p., conferma la scelta compiuta dal legislatore delegante di non seguire la soluzione proposta dalle Sezioni unite nella sentenza citata e, abbandonando la logica del doppio binario processuale, ammette l'uso del *trojan horse* come cimice elettronica senza alcuna limitazione riguardante il tipo di reato oggetto d'indagine[429].

Conseguentemente, secondo quanto disposto dall'art. 266, comma 2, c.p.p. questa peculiare forma d'intercettazione tra presenti è sempre consentita per i reati diversi da quelli di cui l'art. 51, commi 3-*bis e* 3-*quater,* c.p.p. nei luoghi diversi da quelli di privata dimora di cui l'art. 614 c.p., dove l'intercettazione è autorizzabile dal giudice soltanto qualora sussista il fondato motivo di ritenere che *ivi* si stia svolgendo l'attività criminosa[430]. Mentre per i delitti di cui l'art. 51, commi 3-*bis* e 3-*quater,* c.p.p. la nuova disposizione consente le intercettazioni ambientali con il *trojan horse* anche in luoghi domiciliari a prescindere dallo svolgimento dell'attività criminosa.

---

[427] In dottrina si era ipotizzato di introdurre *ex* novo un art. 266 ter c.p.p. dedicato all'intercettazione virale di comunicazioni o conversazioni tra presenti. In tal senso si veda D.CURTOTTI, *op. cit,* p. 383.

[428] O.CALAVITA, *op. cit*., p. 67.

[429] G. GIOSTRA-R. ORLANDI, *op.cit*. p. 243.

[430] D.PRETTI, *op.cit.* p. 218.

Pertanto, prima della riforma, le Sezioni unite nella sentenza Scurato avevano precisato che in tutti i procedimenti *latu sensu* di criminalità organizzata, anche comune, era consentito ricorrere al captatore informatico senza la necessità di indicare i luoghi di captazione, invece, con la novella, l'introduzione del citato comma induce a ricondurre l'ambito operativo del *software* spia senza vincoli di luogo ai soli delitti indicati nelle norme di rinvio[431]. In questo modo la disposizione richiama un elenco tassativo di reati[432] che rientrano nella "competenza" delle procure distrettuali, evitando così la vaghezza dell'espressione "criminalità organizzata"[433].

[431] D.PRETTI, *ibidem*.

[432] Si veda art. 51 comma 3 *bis* c.p.p.: «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 taluno dei delitti di cui all'articolo 12, commi 1, 3 e 3-ter, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 600, 601, 602, 416-bis, 416 ter, 452-quaterdecies e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis 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, dall'articolo 291-quater 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».
Art. 51 comma 3 *quater* c.p.p.: «Quando si tratta di procedimenti per i delitti consumati o tentati con finalità di terrorismo 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».

[433] G. GIOSTRA-R. ORLANDI, *op.cit*. p.253

3.2 L'art. 6 d.lgs. n. 216/2017 e la legge n.3/2019 (c.d. legge "spazza-corrotti" o "anticorruzione"): il regime speciale che accomuna reati di criminalità organizzata e delitti contro la pubblica amministrazione.

La riforma attuata con il d.lgs. n. 216/2017 ha introdotto una disciplina peculiare in materia d'intercettazioni di comunicazioni e conversazioni tra presenti per l'accertamento dei reati commessi dai pubblici ufficiali contro la pubblica amministrazione; il legislatore, pertanto, ha inteso equiparare la disciplina delle intercettazioni riguardo questa categoria di reati a quella tipica dei reati di criminalità organizzata e terrorismo. L'art 6 d.lgs. n. 216/2017 dispone, infatti, che nei procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p., si applicano le disposizioni di cui all'art. 13 del decreto legge 13 maggio 1991, n.152, convertito con modificazioni dalla legge 12 luglio 1991, n. 203.

L'indistinto rimando allo statuto delle intercettazioni in tema di delitti di criminalità organizzata comporta l'integrale applicabilità della disciplina derogatoria prevista per quest'ultimi ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione[434]. Anche per la suddetta categoria di reati, quindi, operano le regole previste all'art. 13 del d.l. n. 152/1991 ed in particolare quelle relative ai requisiti necessari per l'autorizzazione delle operazioni, dovendosi a tal fine valutare, in luogo dei gravi indizi di reato e del requisito di indispensabilità del ricorso alle intercettazioni, i soli sufficienti indizi di reato e la mera necessità del mezzo captativo.

[434] D.PRETTI, *op.cit.* p.227.

Sul fronte della durata delle operazioni, inoltre, essa non può superare i quaranta giorni, ma può essere prorogata dal giudice con decreto motivato per periodi successivi di venti giorni, qualora ne permangano i presupposti applicativi; peraltro, nei casi di urgenza, alla proroga può provvedere direttamente il pubblico ministero, secondo le disposizioni del comma 2 dell'art. 267 c.p.p.[435] .

La riforma, accomunando i reati di criminalità organizzata e i delitti contro la pubblica amministrazione, ha permesso di procedere alla captazione di comunicazioni e conversazioni nei luoghi di cui l'art. 614 c.p. pur quando non vi sia motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa. Il rimando, tuttavia, non è integrale, posto che l'art. 6 del decreto in commento specifica, al secondo comma, che l'intercettazione di comunicazioni tra presenti nei luoghi indicati dall'art. 614 c.p., al fine di accertare i reati dei pubblici ufficiali contro la pubblica amministrazione, non può essere eseguita mediante l'inserimento di un captatore informatico su dispositivo elettronico portatile quando non vi è motivo di ritenere che ivi si stia svolgendo l'attività criminosa. Per quanto concerne, quindi, l'uso del captatore informatico per l'accertamento dei delitti dei pubblici ufficiali contro la pubblica amministrazione, il Legislatore ha ipotizzato una sorta di terzo binario che si aggiunge alla disciplina ordinaria e allo statuto previsto per i delitti di criminalità organizzata[436]. Le intercettazioni tra presenti nei luoghi di privata dimora al fine di accertare i reati dei pubblici ufficiali contro la pubblica amministrazione, pertanto, possono essere liberamente eseguite utilizzando le tradizionali forme captative mediante microspie da collocare fisicamente nei luoghi da monitorare; al contrario, sono limitate alla sussistenza di fondati motivi di ritenere che in quei luoghi si stia svolgendo l'attività criminosa, qualora si intenda operare l'ascolto mediante l'attivazione del microfono di un dispositivo elettrico portatile[437].

[435] Sul tema cfr. *supra* § 2.1.

[436] L.PALMIERI, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza Scurato alla riforma sulle intercettazioni, Dir. pen. cont.*, 2018, 1, p. 64.

[437] D.PRETTI, *op.cit.* p.228.

Il sopra citato comma 2 dell'art. 6 dlgs. 216/2017, tuttavia, è stato espressamente abrogato con l'introduzione dell'art. 1, comma 3 e 4, lett.*a)* e *b)*, l. 3/2019[438] (c.d. legge "spazza-corrotti" o "anticorruzione") che, modificando l'assetto normativo delineato dagli artt. 266, comma 2-*bis*, e 267, comma 1, c.p.p., estende il campo applicativo della disciplina sulle intercettazioni eseguite mediante inserimento del virus *trojan horse* anche ai reati dei pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p. In questo modo si ammette che l'intercettazione ambientale eseguita per mezzo di un *malware* è sempre consentita se si procede sia per delitti di criminalità organizzata, sia per quelli realizzati dai pubblici ufficiali contro la pubblica amministrazione (art. 266, comma 2-*bis*, c.p.p.), con la precisazione che, per entrambe le categorie delittuose, risulta irrilevante l'indicazione spazio-temporale del luogo in cui si trova il dispositivo mobile infettato (art. 267, comma 1, c.p.p.)[439].

È importante evidenziare che la legge "anticorruzione" non ha, però, modificato il disposto dell'art. 267, comma 2-*bis*, c.p.p.[440], introdotto *ex novo* dal dlgs. 216/2017, il quale prevede che, nei casi di urgenza, il *dominus* delle indagini preliminari possa, di propria iniziativa, disporre le intercettazioni tra presenti con il captatore informatico nei delitti di cui l'art. 51, commi 3-*bis* e 3-*quater*, c.p.p.

Da ciò ne consegue che il pubblico ministero può attivarsi nei casi d'urgenza, senza il provvedimento del giudice, disponendo le intercettazioni tramite agente intrusore solo per i delitti di cui l'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., mentre gli è preclusa una simile operazione qualora debba procedere all' accertamento di un reato di corruzione[441].

---

[438] Cfr. L. 9 gennaio 2019 n. 3, recante «*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*», in G.U., 16 gennaio 2019, n.3.

[439] L.CAMALDO, *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico*, in *Dir. pen. cont.*, 24 settembre 2019, p.17.

[440] Sull'art. 267, comma 2-*bis*, c.p.p , cfr. *infra* § 4

[441] L.CAMALDO, *op. cit*, p. 18.

3.2.1 Estensione della portata applicativa del captatore informatico.

Per quanto riguarda il ricorso al captatore informatico ai fini d'intercettazione, dopo l'interpolazione del comma 2-*bis* dell'art. 266 c.p.p. realizzata dalla l. 3/2019[442], il legislatore è intervenuto nuovamente su questa disposizione con il d.l. 161/2019. Il novellato comma 2-*bis* dell'art. 266 c.p.p., pertanto, dispone che lo strumento del *trojan horse* possa essere impiegato senza limiti spazio temporali, oltre che per i reati di cui l'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., anche « *per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4 c.p.p.*»[443].

Rispetto alla formulazione previgente, la novella estende l'impiego del captatore informatico anche per i delitti commessi dagli incaricati di un pubblico servizio non inclusi nella modifica realizzata dalla l. 3/2019.

Il d.l 161/2019, inoltre, modifica il comma 2-*bis* dell'art. 267. c.p.p., sul quale non era intervenuta la legge "anticorruzione", disponendo che il pubblico ministero può attivarsi nei casi d'urgenza e disporre, senza il provvedimento del giudice, le intercettazioni tramite agente intrusore non solo per i delitti di cui l'art. 51, commi 3-*bis* e 3-*quater*, c.p.p. ma anche per l'accertamento dei delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione[444].

---

[442] Sul tema si veda *supra* § 3.2

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

[444] Si veda art. 2, comma 1, lett *d),* punto 2, d.l. 161/2019 : al comma 2-*bis* dopo le parole «*di cui all'articolo 51, commi 3-bis e 3-quater*» sono aggiunte le seguenti: «*e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo* 4».

3.3 Il decreto autorizzativo "rafforzato".

L'art. 267 c.p.p., come modificato dal d.lgs. 216/2017, dispone espressamente che «*Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini: nonché, se si procede per delitti diversi da quelli di cui l'art. 51, commi 3 bis e 3 quater, c.p.p., e per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4 c.p.p.*».

Questa disposizione introduce per la redazione del decreto che autorizza l'intercettazione tramite agente intrusore uno sforzo motivazionale ulteriore da parte del giudice[445] e quindi oltre alla sussistenza di gravi indizi di reato e l'indispensabilità del ricorso a questo strumento captativo, richiede l'indicazione delle ragioni che rendono necessaria tale modalità di esecuzione.

La norma prevede la determinazione delle specifiche necessità operative che ragionevolmente rendano più agevole l'esecuzione delle operazioni di captazione grazie all'inoculazione in un dispositivo elettronico portatile del virus *trojan horse*[446]. Quindi il decreto autorizzativo deve indicare le ragioni inerenti all'infruttuosità delle altre forme di intercettazione ambientale e giustificare il ricorso al *software* spia in ragione alla meno agevole praticabilità e all'alto rischio d'insuccesso delle tecniche tradizionali di captazione[447].

Ad esempio, sarà certamente ammessa l'intercettazione tramite agente intrusore per captare la conversazione tra due soggetti che passeggiano lungo una via pubblica, poiché in questa circostanza non sono facilmente collocabili le microspie tradizionali, oppure l'utilizzo del captatore informatico sarà giustificato nell'ipotesi in cui l'intercettazione di comunicazioni riguardi un incontro che si svolga in un locale pubblico la cui ubicazione non sia nota agli operatori della polizia giudiziaria o che non sia facilmente accessibile

---

[445] S. MENDICINO, *Legittimità delle intercettazioni: il delicato tema della motivazione dei decreti autorizzativi*, in *Diritto e Giustizia*, 2016, 82, p.10.

[446] G. GIOSTRA-R. ORLANDI, *op.cit*. p. 249.

[447] G. GIOSTRA-R. ORLANDI, *ibidem.*

per la collocazione delle microspie[448]. In quest'ultimo esempio è possibile notare come l'intercettazione con metodi tradizionali non sia di per sé irrealizzabile, tuttavia esposta ad un alto rischio di insuccesso e quindi, il ricorso al captatore informatico è indispensabile per la riuscita dell'operazione[449].

In sostanza le intercettazioni di comunicazioni tra presenti mediante agente intrusore rappresentano l'*extrema ratio* a cui ricorrere quando tutti gli altri strumenti cognitivi a disposizione degli organi inquirenti non sono in grado di soddisfare le esigenze investigative[450].

L' art. 267 c.p.p. prevede come ulteriore requisito del decreto autorizzativo, salvo che si proceda per i delitti di criminalità organizzata di tipo mafioso o di terrorismo *ex* art. 51, commi 3-*bis* e 3-*quater*, c.p.p. e per i delitti dei pubblici ufficiali contro la pubblica amministrazione, l'individuazione dei luoghi e del tempo nel cui ambito si procederà all'attivazione del microfono.

L'art. 267, comma 1, c.p.p., inoltre, dispone che, nel decreto autorizzativo, i luoghi possono essere anche "indirettamente determinati"; si ricorre all'indicazione indiretta del luogo, ad esempio, quando, lo *smartphone*, nel quale viene inoculato il virus, sia ceduto a terzi dall'indagato oppure presenti malfunzionamenti tali da ritenere necessaria la sostituzione del dispositivo bersaglio[451]. In tali circostanze è possibile indicare in modo indiretto i luoghi della captazione attraverso formule generiche del tipo "il dispositivo mobile appartenente a Tizio" senza specificare la marca e il numero seriale dello stesso, ammettendo così l'intercettazione itinerante anche nel caso di successione nel tempo di dispositivi mobili[452].

La possibilità di determinare, nel decreto autorizzativo, il luogo in maniera indiretta consente, inoltre, di far fronte a tutte quelle situazioni nelle quali è estremamente difficoltoso prevedere in maniera specifica tutti gli spostamenti dell'apparato infettato[453].

---

[448] D.PRETTI, *op.cit.* p.219.

[449] *Ibidem.*

[450] D.CURTOTTI, *op. cit,* p.403.

[451] O.CALAVITA, *op. cit*., p. 63.

[452] O.CALAVITA, *Ibidem*.

[453] D.PRETTI, *op.cit.* p.220.

Ad esempio, nel caso in cui la Procura venga a conoscenza che Tizio, noto spacciatore contro il quale si procede, debba incontrarsi con Caio per la cessione di un ingente quantitativo di sostanza, ma non si sia a conoscenza dell'ubicazione del luogo, il provvedimento autorizzativo dell'intercettazione itinerante potrebbe rimandare indirettamente al luogo dello scambio, attraverso il ricorso ad una formula ampia quale "nel luogo in cui Tizio incontrerà Caio per cedergli la sostanza stupefacente"[454].

Un altro elemento di novità richiesto dal novellato art. 267 c.p.p. è la necessaria indicazione, nel provvedimento autorizzativo dell'intercettazione itinerante, del tempo di attivazione del microfono. In questo modo si determina una significativa differenza tra le intercettazioni tradizionali che proseguono ininterrottamente per tutto l'arco temporale in cui sono autorizzate e quelle, itineranti, i cui momenti temporali di attivazione necessitano di un apposito comando dell'autorità giudiziaria procedente. Il tempo di attivazione del microfono deve però rimanere confinato nel perimetro di durata massima dell'intercettazione[455].

Il legislatore ha annoverato l'indicazione del luogo, insieme a quella del tempo, tra i presupposti del provvedimento autorizzativo i quali sono garantiti da un'espressa comminatoria d'inutilizzabilità *ex* art. 271, comma 1, c.p.p.[456].

Sempre per quanto attiene al procedimento autorizzativo, il d.lgs. n.216/2017 ha introdotto il comma 2-*bis* dell'art. 267 c.p.p. in virtù del quale il pubblico ministero può disporre l'intercettazione itinerante in casi di urgenza soltanto se si procede per uno dei delitti di cui l'art. 51, commi-3 *bis* e 3-*quater*, c.p.p., con l'onere motivazionale aggiunto di indicare le ragioni d'urgenza per le quali è impossibile attendere il provvedimento giudiziale.

In questa disposizione potrebbe rinvenirsi una violazione dell'art. 76 Cost. per eccesso di delega perché i delitti di cui all'art. 51, co. 3-*bis* e 3-*quater* c.p.p. sono gli unici a poter fruire del mezzo di captazione in discorso secondo la procedura speciale prevista dall'art. 267, comma 2, c.p.p. previa specifica indicazione delle ragioni di urgenza. Sussiste, quindi, una discrasia con la previsione contenuta nell'art. 1, co. 84 lett. *e)* n. 6 della legge di delega, ove prescrive un obbligo motivazionale molto più incisivo, riferito

[454] D.PRETTI, *ivi*, p.221

[455] O.CALAVITA, *op. cit.*, p.64.

[456] *Ibidem.*

all'indicazione di specifiche situazioni "di fatto" pregiudicanti il ricorso alla procedura ordinaria, ed integranti "concreti" casi di urgenza con l'indicazione delle ragioni per le quali il ricorso all'intrusore si manifestasse come necessario[457].

Un ulteriore profilo di illegittimità costituzionale potrebbe rinvenirsi nella violazione dell'art 3 Cost., sia perché non sussiste alcuna ragione per differenziare il trattamento tra i reati ordinari e i reati di criminalità organizzata[458] sia perché, questa limitazione, certamente collegata ai presupposti più rigidi in materia di intercettazione nei luoghi di privata dimora per le indagini su reati "ordinari", appare quantomeno irragionevole atteso che in ogni caso sui presupposti dell'intercettazione d'urgenza opera il controllo successivo del giudice per le indagini preliminari in sede di convalida [459].

3.4 Modalità procedimentali di esecuzione dell'attività captativa

Il d.lgs. 216/2017 nel disciplinare le modalità di esecuzione dell'attività captativa ha perseguito l'obiettivo di garantire la genuinità dei dati captati[460].

A tal fine, l'art. 268, al comma 3 *bis*, c.p.p., stabilisce che quando si procede a intercettazione di comunicazioni informatiche o telematiche, il pubblico ministero può disporre che le operazioni siano compiute con impianti appartenenti a privati [461] e, inoltre, riguardo specificamente al captatore informatico, dispone ulteriormente che per l'avvio e la cessazione delle registrazioni, l'ufficiale di polizia giudiziaria possa avvalersi di persone idonee di cui l'art. 348, comma 4, c.p.p., vale a dire di soggetti che in virtù della loro competenza e professionalità possono cooperare con la polizia giudiziaria per il compimento di atti che richiedono specifiche competenze tecniche[462].

---

[457] L. SURACI, , *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni: qualche rilievo critico*, in www.pluriscedam.utetgiuridica.it, 05 gennaio 2018, p. 5.

[458] Si veda O.CALAVITA, *ivi*, p. 72.; allo stesso modo D.PRETTI, *op. cit.*, p. 223.

[459] C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n.216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria*, in *Dir. pen. cont.*, 13 Aprile 2018, p.25.

[460] G. GIOSTRA-R. ORLANDI, *op.cit*. p. 270.

[461] Sul tema dell'esecuzione delle operazioni d'intercettazioni cfr. Cap. 1 § 2.4.

[462] O. MAZZA, *op. cit*., p. 131.

Il legislatore delegato presta attenzione anche alla stessa fase di inoculazione del virus, in quanto il novellato art. 89, comma 2-*bis*, c.p.p. prevede che possano essere utilizzati esclusivamente programmi informatici con requisiti tecnici stabiliti con Decreto del Ministro della giustizia, in conformità a quanto disposto dall'art. 84 della legge n. 103/2016, secondo il quale il legislatore delegato dovrebbe tenere costantemente conto dell'evoluzione tecnica garantendo la corrispondenza di detti programmi ad elevati standard di affidabilità tecnica, sicurezza ed efficacia.

Per quanto riguarda la fase successiva alla captazione, sempre perseguendo l'obiettivo di garantire l'integrità dei dati, l'art. 89, comma 2-*ter*, disp. att. c.p.p. dispone che le comunicazioni intercettate, dopo l'acquisizione delle necessarie informazioni in merito alla sicurezza e affidabilità della rete di trasmissione, vengano trasferite esclusivamente verso gli impianti della procura della Repubblica e, durante il trasferimento dei dati, siano effettuati controlli per assicurare l'integrale corrispondenza tra quanto trasmesso e intercettato.

Il successivo comma 2-*quater* prevede che nel caso in cui risulti impossibile il contestuale trasferimento dei dati captati al *server* della Procura perché, a titolo esemplificativo, il dispositivo infettato non risulta connesso alla rete Wi-Fi[463], il verbale deve dare atto delle ragioni tecniche impeditive e della successione cronologica degli accadimenti captati e delle conversazioni intercettate. Sempre in relazione al verbale l'art. 89, primo comma, disp. att. c.p.p., prevede che in caso d'intercettazione tramite captatore informatico, lo stesso debba fare riferimento al tipo di programma impiegato ed ai luoghi in cui si svolge la captazione.

Il legislatore, al fine di garantire l'inalterabilità dei dati acquisiti, ha introdotto l'art. 89, comma 2-*quinquies*, disp. att. c.p.p., in base al quale al termine delle operazioni di captazione deve provvedersi, anche con l'ausilio di persone idonee di cui l'art. 348 c.p.p., alla disattivazione del captatore con modalità tali da renderlo inidoneo a successivi impieghi. In questo modo si vuole evitare il rischio che i captatori informatici si trasformino in uno strumento sempre pronto a riattivarsi e ad operare così un monitoraggio continuativo del dispositivo infettato in assenza di ogni legittimazione[464].

---

[463] D.PRETTI, *op.cit.* p.225.

[464] W. NOCERINO, *Le Sezioni unite risolvono l'enigma: utilizzabilità del captatore informatico nel processo penale*, in *Cassazione pen*ale, 2016, p. 3568.

Il legislatore, quindi, occupandosi di aspetti strettamente tecnici riguardanti il "tracciamento" delle operazioni compiute, vuole garantire sia l'originalità che l'integrità delle registrazioni, delineando così il corretto "ciclo di vita" delle intercettazioni realizzate per mezzo dell'inoculazione nel dispositivo bersaglio del virus *trojan horse*[465]. Le disposizioni citate, comunque, non sono prescritte a pena di inutilizzabilità, a differenza di quanto accade per i requisiti indicati dall'art. 268, comma 3, c.p.p., perché la riforma non è intervenuta sul testo dell'art. 271, comma 1, c.p.p., il quale non richiama l'art. 89 disp. att. c.p.p. tra le ipotesi d'inutilizzabilità.

È importante segnalare che sulla disciplina concernente le modalità di realizzazione delle operazioni tramite captatore informatico è intervenuto il d.l. 161 /2019 sostituendo integralmente l'art. 89 disp. att. c.p.p. come previsto dal d.lgs. 216/2017, appena analizzato in questo paragrafo.

L'art. 89 disp.att. c.p.p. riformato dispone che nel procedimento di captazione delle comunicazioni e conversazioni tra presenti mediante l'inserimento del virus *trojan horse* in un dispositivo elettronico portatile, il verbale deve indicare il tipo di programma utilizzato e, ove possibile, i luoghi in cui si svolgono le conversazioni. La disposizione in esame prevede che ai fini dell'intercettazione per mezzo del captatore informatico devono essere utilizzati programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia e durante la trasmissione dei dati deve essere assicurata la corrispondenza integrale tra quanto intercettato, registrato e trasmesso.

[465] D.CURTOTTI, *op. cit.*, p.405.

Al termine delle operazioni si provvede anche mediante persone idonee di cui all'art. 348 c.p.p., alla disattivazione con modalità tali da renderlo inidonei ai successivi impieghi[466].

3.5 Divieto di utilizzazione per la prova di reati diversi

L'art. 4, comma 1, lett. *d)* del d.lgs. n. 216/2017 introduce il comma 1 *bis* dell'art. 270 c.p.p. che, riprendendo in un'accezione "minimalista"[467] la disposizione dell' art. 84, lett. *e)* della legge delega[468], esclude l'utilizzazione dei risultati delle intercettazioni tra presenti effettuate con captatore informatico su dispositivo elettronico portatile "per la prova di reati diversi" da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che si rivelino indispensabili in relazione all'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.

Il legislatore, riguardo l'utilizzabilità dei risultati delle intercettazioni con il captatore informatico, quindi, ha scelto di sostituire la locuzione "in procedimenti diversi", accolta nell'art. 270, comma 1, c.p.p. con l'espressione "per la prova di reati diversi" da quelli per i quali è stato emesso il decreto autorizzativo.

---

[466] Art.2, comma 2, lett.a), d.l. 161/2019: l'articolo 89 è sostituito dal seguente: «*Art. 89. (Verbale e registrazioni delle intercettazioni).*
1. Il verbale delle operazioni previsto dall'articolo 268 comma 1 del codice contiene l'indicazione degli estremi del decreto che ha disposto l'intercettazione, la descrizione delle modalità di registrazione, l'annotazione del giorno e dell'ora di inizio e di cessazione della intercettazione nonché' i nominativi delle persone che hanno preso parte alle operazioni. Quando si procede ad intercettazione delle comunicazioni e conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, il verbale indica il tipo di programma impiegato e, ove possibile, i luoghi in cui si svolgono le comunicazioni o conversazioni.
2. Ai fini dell'installazione e dell'intercettazione attraverso captatore informatico in dispositivi elettronici portatili possono essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia.
3. Nei casi previsti dal comma 2 le comunicazioni intercettate sono trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente nell'archivio digitale di cui all'articolo 269, comma 1, del codice. Durante il trasferimento dei dati sono operati controlli costanti di integrità che assicurino l'integrale corrispondenza tra quanto intercettato, registrato e trasmesso.
4. Quando è impossibile il contestuale trasferimento dei dati intercettati, il verbale di cui all'articolo 268 del codice dà atto delle ragioni impeditive e della successione cronologica degli accadimenti captati e delle conversazioni intercettate.
5. Al termine delle operazioni si provvede, anche mediante persone idonee di cui all'articolo 348 del codice, alla disattivazione del captatore con modalità tali da renderlo inidoneo a successivi impieghi. Dell'operazione si dà atto nel verbale.»

[467] O. MAZZA, *op. cit*., p. 126.

[468] Sul tema cfr. *supra* § 3.

Dalla formulazione letterale della norma è evidente come il legislatore, impedendo la circolazione "esoprocedimentale" degli atti investigativi per la prova di reati diversi, ha previsto espressamente che i dati acquisiti con l'intercettazione itinerante potranno essere utilizzati esclusivamente per la prova del reato per il quale è stata disposta[469].

In sostanza il legislatore è pervenuto ad una soluzione alternativa per le intercettazioni tramite captatore informatico rispetto agli orientamenti giurisprudenziali sull' art. 270, comma 1, c.p.p. considerando l'estensione dei margini di utilizzabilità dei risultati delle intercettazioni tradizionali alla luce delle puntualizzazioni effettuate dalla giurisprudenza sulla nozione di procedimento diverso[470].

La Suprema Corte ha, infatti, chiarito che ai fini del divieto di utilizzazione di cui l'art. 270 comma 1 c.p.p. occorre far riferimento ad una nozione sostanziale di "diverso" procedimento, secondo cui la diversità va ricondotta al dato dell'insussistenza, tra i fatti di reato, di un nesso ai sensi dell'art. 12 c.p.p. ovvero di tipo investigativo e, quindi, all'esistenza di un collegamento meramente fattuale ed occasionale[471]. La Corte ha inoltre evidenziato che la nozione di diverso procedimento[472] va ancorata ad un criterio di valutazione sostanzialistico che prescinde da elementi formali, come il numero d'iscrizione nel registro delle notizie di reato, essendo invece rilevante ai fini della individuazione dell'identità dei procedimenti, l'esistenza di una connessione tra il contenuto dell'originaria notizia di reato, per la quale sono state disposte le intercettazioni ed i reati per i quali si procede sotto il profilo oggettivo, probatorio e finalistico[473].

L'esegesi dell'art. 270, comma 1-*bis*, c.p.p., che limita l'utilizzabilità dell'intercettazione tramite captatore informatico all'accertamento del reato per il quale è stata disposta, è l'unica interpretazione possibile della norma in esame perché diversamente opinando il

---

[469] O.CALAVITA, *op. cit.*, p.75.

[470] L. SURACI, *op. cit.*, p.7.

[471] Cass. pen., Sez. III, 21 gennaio 2016, n. 2608, in *C.e.d. Cass*., Rv.266423

[472] È importante evidenziare che il concetto di diverso procedimento nel quale, ai sensi dell'art. 270, comma 1, c.p.p. è vietata l'utilizzazione dei risultati delle intercettazioni di conversazioni o comunicazioni (salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza), non equivale a quello di "diverso reato" ed in esso, pertanto, non rientrano le indagini strettamente connesse e collegate sotto il profilo probatorio e finalistico al reato in ordine al quale il mezzo di ricerca della prova è stato disposto. Sul tema cfr. Cass.,pen, sez. VI, 16 Ottobre 1995, n.1626, in *C.e.d. Cass*., Rv.203738.

[473] Cass. pen., sez. un., 26 giugno 2014, n. 32697, in *C.e.d. Cass*., Rv. 259777

comma 1-*bis de quo* risulterebbe essere una «*mera superfetazione normativa*»[474] se raffrontato con il comma che lo precede e sarebbe privo di un autonomo significato precettivo[475].

Alla luce dei profili di criticità evidenziati da alcuni Autori[476] nell'interpretazione del comma 1-*bis* dell'art. 270 c.p.p., non sorprende la scelta del legislatore che, con il d.l. 161/2019, ha soppresso il divieto di utilizzazione introdotto dal d.lgs. 216/2017 in ragione della maggior lesività dell'intercettazione tramite agente intrusore dovuta al carattere itinerante della stessa[477].

La nuova normativa, quindi, fermo restando il divieto di impiego dei dati delle captazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte *ex* art. 270, comma 1, c.p.p., prevede che i risultati delle intercettazioni tra presenti realizzate per mezzo dell'inoculazione del virus *trojan horse* in un dispositivo elettronico portatile possono essere utilizzati per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'art. 266, comma 2-*bis*, c.p.p.[478].

Mentre secondo la versione del comma 1-*bis* dell'art. 270 c.p.p. disposta dal d.lgs. 216/2017 il divieto di utilizzo dei dati appresi trovava una deroga solo nel caso in cui essi risultassero indispensabili per l'accertamento di reati per i quali è obbligatorio l'arresto in flagranza, il novellato comma 1-*bis* dell'art. 270 c.p.p. permette di utilizzare i risultati delle intercettazioni tramite captatore informatico per la prova di reati diversi da quelli contemplati dal decreto autorizzativo, purché ricompresi tra i gravi crimini di cui l'art. 51, commi 3-*bis* e 3-*quater* c.p.p. e quelli commessi dai pubblici ufficiali o gli incaricati di pubblico servizio contro la pubblica amministrazione.

---

[474] O.CALAVITA, *op. cit.*, p.75.

[475] O.CALAVITA, *Ibidem*

[476] Si veda O.CALAVITA, *Ibidem*, allo stesso modo L. SURACI, *op. cit.*, p.7 e O. MAZZA, *op. cit.*, p. 126.

[477] W. NOCERINO, *op. cit.*, p.77.

[478] Art. 2, comma 1, lett.g), d.l. 161/2019: all'articolo 270 il comma 1-bis è sostituito dal seguente: «*1-bis. Fermo restando quanto previsto dal comma 1, i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'articolo 266, comma 2-bis*.»; al comma 2, al secondo periodo le parole «*degli articoli 268-bis, 268-ter e 268-quater» sono sostituite dalle seguenti: «dell'articolo 268, commi 6, 7 e 8*».

Conclusioni

Nel presente elaborato sono state trattate una pluralità di questioni inerenti all'utilizzo del virus *trojan horse* in ambito investigativo e, dall'analisi di questo strumento d'indagine, è emerso con chiarezza che il progresso scientifico in campo informatico, in materia di *remote control system*, ha determinato l'inevitabile apertura del sistema delle indagini penali in Italia a forme d'intercettazioni tra presenti effettuate tramite captatore informatico.

Il legislatore, di conseguenza, con il d.lgs. n. 216/2017 è intervenuto a ridisegnare la materia delle intercettazioni, introducendo una nuova ed altrettanto complessa disciplina atta a garantire la tutela della sfera di riservatezza delle persone coinvolte dalle intercettazioni di conversazioni e comunicazioni. Il suddetto decreto ha inciso in particolar modo sull'istituto dell'udienza stralcio sia contemplando un nuovo meccanismo di acquisizione delle captazioni al fascicolo delle indagini sia prevedendo al contempo un apposito archivio riservato per la conservazione dei verbali e delle registrazioni.

Come segnalato nel capitolo I il 31 Dicembre 2019 giorno in cui la riforma "Orlando" sarebbe dovuta entrare in vigore il Consiglio dei Ministri con il d.l. 161/2019 ha innovato la disciplina del d.lgs. 216/2017, attuando quella che potrebbe essere definita "riforma della riforma" [479]. Le novità apportate al d.lgs. 216/2017 hanno determinato in primo luogo l'accentramento nella sfera di competenza del pubblico ministero dell'opera di selezione del materiale raccolto durante le indagini[480].

In secondo luogo, le modifiche introdotte dal d.l. 161/2019 raffinano le modalità di deposito dei verbali redatti, nell'ottica di una maggiore garanzia di trasparenza delle attività condotte, rafforzando, da un lato, il contraddittorio con il difensore

[479] W. NOCERINO, *op. cit.*, p.67.

[480] Si veda in tal senso l'art. 2, comma 1, lett.f), punto 3 del d.l. 161/2019, abroga l'ultimo periodo del comma 4 dell'art, 267 c.p.p., introdotto nel 2017, per cui il pubblico ministero procede alla selezione personalmente ovvero avvalendosi di un ufficiale di polizia giudiziaria. La medesima ratio è sottesa al comma 1, lett. e), punti1-3, prima parte dell'art. 2 d.l. 161/2019 che riformando l'art. 268 c.p.p., attribuiscono al pubblico ministero un ruolo centrale nella fase esecutiva prodromica all'acquisizione.

dell'indagato[481] e, dall'altro, le esigenze di riservatezza delle informazioni apprese durante l'esecuzione delle operazioni[482].

Infine il decreto, intervenendo sulla procedura di acquisizione e di trascrizione, tenta di velocizzare le tempistiche procedimentali, garantendo la speditezza degli adempimenti burocratici[483].

Nonostante le significative modifiche apportate in tema di intercettazioni dal d.l. 161/2019, rimane indubbio che il maggior pregio del d.lgs. 216/2017 sia quello di aver previsto la prima regolamentazione normativa, priva di precedenti nel nostro ordinamento, dell'impiego del captatore informatico da parte degli organi inquirenti, quale modalità specifica di esecuzione delle intercettazioni tra presenti.

Questa disciplina, come analizzato nel capitolo III, è stata introdotta sulla base delle linee guida tracciate dalle Sezioni unite nella sentenza "Scurato" che ha ricondotto alla categoria delle intercettazioni tra presenti la captazione di comunicazioni e conversazioni realizzata mediante l'inoculazione di un virus *trojan horse* in un dispositivo elettronico portatile.

In particolare, il decreto prevede che l'agente intrusore non possa essere mantenuto attivo senza limiti di tempo o di spazio, ma debba essere attivato da remoto secondo quanto previsto dal pubblico ministero nel proprio programma d'indagine. Il captatore informatico, inoltre, deve essere disattivato se l'intercettazione avviene in ambiente domiciliare, a meno che non vi sia prova che in tale ambito si stia svolgendo l'attività criminosa oggetto dell'indagine o che l'indagine stessa non riguardi i delitti più gravi, tra i quali mafia e terrorismo, di cui all'articolo 51, commi 3- *bis* e 3-*quater*, del codice di procedura penale, i delitti dei pubblici ufficiali e i delitti degli incaricati di un pubblico servizio contro la pubblica amministrazione.

---

[481] In tal senso si veda art. 2, comma 1, lett. e) del d.l. 161/2019.

[482] In tal senso si veda l'art.2, comma 1, lett.a) del d.l. 161/2019 che introduce un nuovo comma 2 *bis* all'art. 114 c.p.p., sancendo che «*è sempre vietata la pubblicazione anche parziale del contenuto delle intercettazioni non acquisite ai sensi degli art. 268 c.p.p. e 415 bis c.p.p.*». Allo stesso modo si veda l'art.2, comma 1, lett.f), punto 2 del d.l. 161/2029 per cui attraverso l'abrogazione del comma 1 *bis* dell'art. 269 c.p.p., viene esteso l'onere di segretezza ai verbali delle comunicazioni acquisite al fascicolo delle indagini *ex* art.373, comma 5, c.p.p., nonché il complesso di disposizioni che implementano e regolarizzano il funzionamento dell'archivio segreto *ex* art. 2, comma 1, lett.f), punto 1, del d.l. 161/2019.

[483]In tal senso si veda l'art. 2, comma 1, lett. e), punto 7 del d.l. 161/2019 che consente al giudice di procedere alla trascrizione anche nel corso delle attività di formazione del fascicolo per il dibattimento *ex* art. 431 c.p.p.

Quest'ultime categorie di delitti sono state introdotte, per quanto riguarda i pubblici ufficiali dalla l. n. 3/2019 mentre l'estensione dell'ambito applicativo del captatore informatico ai delitti degli incaricati di un pubblico servizio contro la pubblica amministrazione è stato disposto dal d.l. 161/2019[484].

L'utilità del *trojan horse* è indubbia poiché consente di prescindere dall'installazione fisica dei dispositivi di captazione per realizzare intercettazioni di comunicazioni e conversazioni tra presenti immettendo direttamente nel dispositivo ospite il *software*-spia.

Se, da un lato, quindi, è concesso nutrire preoccupazioni sulle esponenziali capacità acquisitive dei virus informatici, suscettibili di ledere la riservatezza, dignità e libertà della persona, dall'altro «*è del pari legittimo ricordare che solo siffatti strumenti sono oggi in grado di penetrare canali criminali di comunicazione o di scambio di informazione utilizzati per la commissione di gravissimi reati contro persone*»[485].

La normativa prevista dal d.lgs. 216/2017 non è, comunque, rimasta esente da obiezioni. Il Garante per la protezione dei dati personali in una segnalazione al Parlamento e al Governo sulle intercettazioni realizzate con il captatore informatico, ha osservato che, sebbene il legislatore si sia limitato a regolamentare le sole intercettazioni ambientali compiute con l'ausilio del virus *trojan*, gli agenti intrusori sono idonei a concentrare in un unico atto una pluralità di strumenti investigativi (perquisizioni *on line*, *keylogger*, *screenshot*, intercettazioni di ogni tipo, pedinamenti con il sistema satellitare) e possono inoltre eliminare ogni traccia delle operazioni effettuate, alterando i dati acquisiti[486].

Il Garante rileva, inoltre, che nella normativa in esame «*manca, soprattutto, la previsione di garanzie adeguate per impedire che, in ragione delle loro straordinarie potenzialità intrusive, questi strumenti investigativi, da preziosi ausiliari degli organi inquirenti, degenerino invece in mezzi di sorveglianza massiva o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio,*

---

[484] In tal senso si veda l' art. 2, comma 1, lett.c), d), punti 1 e 2 del d.l. 161/2019, che dispone l'impiego del captatore informatico senza limiti spazio temporali anche ai reati commessi dagli incaricati di pubblico servizio (oltre ai pubblici ufficiali) contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni.

[485] A.NELLO ROSSI-A.BALSAMO, *Memoria per la Camera di Consiglio delle Sezioni Unite del 28 Aprile 2016*, in www.questionegiustizia.it/doc/memoria-ssuu-procura-generale-trojan.pdf., p.3.

[486] Si veda in tal senso "*Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico*", 30 aprile 2019, in www.garanteprivacy.it

rendendolo estremamente permeabile se allocato in server non sicuri o, peggio, delocalizzati anche al di fuori dei confini nazionali»[487].

Sarebbe auspicabile, secondo il garante, introdurre in sede legislativa o anche soltanto novellando il d.lgs. 216/2017, un espresso divieto di ricorso a *software*-spia idonei a cancellare le tracce delle operazioni svolte nel dispositivo bersaglio, in modo assicurare la completezza e veridicità del materiale investigativo raccolto[488].

In considerazione delle straordinarie potenzialità acquisitive del captatore e nonostante il fondato timore che il suo utilizzo da parte degli organi inquirenti possa condurre a scenari quasi "orwelliani", non si può rinunciare a questo validissimo strumento d'indagine, « *il mondo del diritto non può rinunciare agli apporti del progresso scientifico*»[489].

Una scelta aprioristica preordinata ad escludere il ricorso ad una simile tecnologia ai fini delle indagini giudiziarie avrebbe come unico effetto un depotenziamento dell'attività investigativa stessa.

L'unica soluzione prospettabile, quindi, è quella di introdurre una regolamentazione del captatore informatico preordinata sì a garantire la fruttuosità delle indagini, ma che non vanifichi la tutela dei fondamentali valori di libertà dell'individuo propri di uno Stato democratico e connaturati alla nostra Costituzione.

È essenziale quindi riuscire a contemperare le esigenze investigative che richiedono l'utilizzo del captatore informatico, le cui potenzialità ancora non sono pienamente esplorate, con le garanzie dei diritti individuali che possono subire un'indebita compressione dal ricorso, da parte degli organi inquirenti, del virus *trojan horse* [490].

Il d.lgs. 161/2019, riformando il d.lgs. 216/2017, sembra in parte aver accolto le istanze del Garante per la protezione dei dati personali sul tema delle intercettazioni di comunicazioni e conversazioni tra presenti. È apprezzabile, pertanto, la scelta del legislatore di introdurre *ex novo* la disciplina della catena di custodia dei dati e delle informazioni acquisite mediante l'impiego dell'agente intrusore. Sul punto, infatti, il novellato art. 89 disp. att. c.p.p. prevede che nelle intercettazioni condotte a mezzo di

---

[487] *Ibidem.*

[488] *Ibidem*.

[489] O.MAZZA, *op.cit*., p.117.

[490] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

captatore informatico i dati appresi, una volta comprovata l'affidabilità della rete di trasmissione, vengano trasferiti esclusivamente dell'archivio digitale di cui l'art. 269, comma 2, c.p.p. Durante il trasferimento sui dati sono operati controlli costanti d'integrità che assicurino la corrispondenza tra quanto intercettato, registrato e trasmesso. Meno condivisibile, in relazione alle potenzialità investigative del virus *trojan horse*, invece, sembra essere la scelta del legislatore di sacrificare le esigenze della riservatezza per un miglioramento dell'attività investigativa. Il decreto in esame, infatti, consente un «*uso bulimico*»[491] dell'agente intrusore, sia estendendo l'impiego del captatore a categorie delittuose ulteriori sia ammettendo l'uso dei risultati da esso scaturenti anche per la prova di reati diversi da quelli per cui è stato emesso il decreto autorizzativo[492].

[491] W. NOCERINO, *op. cit.*, p. 67.

[492] In tal senso si veda art. 2, comma 1, lett.g), punto 1, d.l. 161/2019 che riforma integralmente il comma 1 *bis* dell'art. 270 c.p.p.

Riferimenti Bibliografici

Manuali, monografie e collettanei

APRILE E.-SPEZIA F., *Le intercettazioni telefoniche ed ambientali, innovazioni tecnologiche e questioni giuridiche*, Milano, 2004, p.2.

BALDUCCI P., *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, 2002, p.43.

BARILE P.- CHELI E., voce *Corrispondenza (libertà di)*, in Enc. dir., vol. X, Milano, 1962, p. 745.

BIN R.-PITRUZZELLA G., *Diritto pubblico*, Torino,2011, p. 423.

BUONOMO G., *Profili penali dell'informatica*, Milano, 1994, p. 153.

CAJANI A.-COSTABILE G., *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea, Information Technologies in the criminal investigation: a European perspective*, Forlì, 2011, p.19.

CAMON A., *Le intercettazioni nel processo penale*, Milano, 1996, p.21

CASCINI G., *Il Pubblico Ministero, in GIOSTRA G.-ORLANDI R., Nuove norme in tema di intercettazioni, Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, 188.

CONSO G.-GREVI-M. BARGIS V., *Compendio di procedura penale, VII ed.*, Padova, 2014, p.391.

CORDERO F., *"Procedura Penale*", Milano, 2012, p. 840.

CORDERO F., *sub artt. 266-267, in Codice di procedura penale commentato*, Torino, 1992, p.310.

DI MARTINO C.-PROCACCIANTINI T., *Le intercettazioni telefoniche*, Padova, 2001, p.17.

FELICIONI P., *Le ispezioni e le perquisizioni, in Trattato di procedura penale*, diretta da UBERTIS G. e VOENA G.M., Milano, 2012, p. 26.

FILIPPI L., *L'intercettazione di comunicazioni*, 1997, Milano, p.121.

FUMU G., *"Commento all'art. 266*", in *"Commento al nuovo codice di procedura penale"*, (a cura di) M. CHIAVARIO, vol. II, Torino, 1990, p. 778.

GIGLIO V., *Manuale delle intercettazioni: il nuovo regime normativo, i principi e la giurisprudenza*, Bologna, 2018, p. 9.

GIOSTRA G.-ORLANDI R., *Nuove norme in tema di intercettazioni, Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p.7-8.

ILLUMINATI G., *La disciplina processuale delle intercettazioni*, Milano,1983, p.41.

MADDALENA M., *I problemi pratici delle inchieste di criminalità organizzata nel nuovo processo penale, in Processo penale e criminalità organizzata* a cura di V. GREVI, Roma-Bari, 1993, p.83.

MANCUSO E.M., *L'acquisizione di contenuti e-mail*, in A.SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2014, p.53.

MANGANELLI A.-GABRIELLI F., *Investigare. Manuale pratico delle tecniche d'indagine*, Padova, 2007, p. 150.

MARCOLINI S.-RUGGERI F.-PICOTTI L., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, pp.190 ss.

MARINELLI C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, p. 4.

MARTINES T., *Diritto Costituzionale*, Milano, 2010, p.550.

MAZZA O., *Le nuove intercettazioni*, in A.SCALFATI-M.DEL TUFO (a cura di) *Leggi penali tra regole e prassi, Ius novum*, Torino, 2018, p.16.

MODUGNO F., *Lineamenti di diritto pubblico*, Torino, 2010, p.579.

ORLANDI R., *Il procedimento penale per fatti di criminalità organizzata: dal maxi-processo al grande processo, in Atti dell'incontro di studio su "Lotta alla criminalità organizzata: gli strumenti normativi*", a cura di GIOSTRA G. e INSOLERA G., Milano 1995, p.88.

RODOTÀ S., *Il diritto di avere diritti*, Roma, 2013, p.317.

SCALFATI A., *Le indagini atipiche*, Torino, 2014, p.143.

SCALFATI, A., *La riforma della giustizia penale*, Torino, 2017, p. 279 ss.

SPANGHER, G. *La riforma Orlando. Modifiche al Codice penale, al Codice di procedura penale e all'Ordinamento Penitenziario*, Pisa, 2017, p. 111 ss.

TONINI P., *Manuale di procedura penale*, Milano, 2017, p. 395.

TONINI P.-CONTI C., *Il diritto delle prove penali*, I ed., Milano, 2012, p.395.

TORRE M., *Il Captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, p.11.

VELE A., *Le intercettazioni nel sistema processuale penale: tra garanzie e prospettive di riforma*, Asiago,2011, p.11.

Articoli

ATERNO S., *Il captatore informatico tra esigenze investigative e limitazione della privacy: un bilanciamento necessario e urgente (I parte),* in *Sicurezza e Giustizia*, 2017, 3, p.20

BATTINIERI L., *Le perquisizioni on line tra esigenze investigative e ricerca atipica della prova*, in *Sicurezza e Giustizia*,2013, 4, p.44.

BONTEMPELLI M., *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont*., 20 Dicembre 2018, p. 2.

CAJANI F., *Odissea del captatore informatico*, in *Cassazione Penale*,2016, 11, p. 4151.

CALAVITA O., *L'odissea del trojan horse*, in *Dir. pen. cont*.,2018, 11, p.57.

CAMALDO L., *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico*, in *Dir. pen. cont*., 24 settembre 2019, p.17.

CAPRIOLI F., *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in *Riv. it. dir. proc. pen*., 1991, p.171.

CONSO G., *La criminalità organizzata nel linguaggio comune*, in *Giustizia Penale*,1992, 3, pp. 385-392.

CURTOTTI D., *Il captatore informatico nella legislazione italiana*, in *Jiusonline*,2017, 3, p. 391.

DE NOZZA M.S., *E-mail parcheggiate su server all'estero, similitudini con il cloud compunting : La Parola alla Cassazione*, in *Sicurezza e Giustizia*,2016, 4, p.52.

DE SÁ E CUNHA LEONOR CHASTRE P., *L' utilizzo del captatore informatico trojan horse nella procedura penale portoghese*, in *Parola alla difesa*, 2016, 1, p. 183

FELICIONI P., *Acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo Penale e Giustizia*, 2016, 5, p.132.

FLOR R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in *Dir. pen, cont*., 20 settembre 2012, p.6.

GIORDANO L., *Dopo le Sezioni Unite sul "Captatore Informatico" avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo, Dir. pen. cont*..,2017, 3, p. 186

GIORDANO L., *La prima applicazione della sentenza "Scurato" nella giurisprudenza di legittimità, Dir. pen. con*t.,2017, 9, p.186.

GITTARDI C., *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n.216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria*, in *Dir. pen. cont*., 13 Aprile 2018, p.25.

GIUNCHEDI F., *Appunti su alcune criticità sulla nuova disciplina delle intercettazioni*, in *Archivio Penale, Speciale Riforme*, 2018.

GRIFFO M., *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, in *Dir. pen. cont*., 2018, 2, p.23.

ILLUMINATI G., *Introduzione Convegno "Le Intercettazioni: problemi antichi e sfide nuove",* Roma 6 Luglio 2017, I sessione Le direttive del d.l. n. 4368, in *Jusonline*, 2017, 3, p.330.

IOVENE F., *Le c.d. perquisizioni on line tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont*. ,2014, 3, p.331

LA CORTE G., *Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata*, in *Giurisprudenza Penale*, 2017, 6, p.7

LE FÈVRE P., *Il regime della captazione dei dati informatici nel diritto francese*, in *Parola alla Difesa*, 2016, 1, p. 181.

MANCUSO E., *La perquisizione on line*, in *JusOnline*,2017, 3, p.420.

MANZIONE D., *Una normativa «d'emergenza» per la lotta alla criminalità organizzata e la trasparenza e il buon andamento dell'attività amministrativa (D.l. 152/91 e L.203/91): uno sguardo d'insieme*, in *Legislazione penale*, 1992, p.851.

MENDICINO S., *Legittimità delle intercettazioni: il delicato tema della motivazione dei decreti autorizzativi*, in *Diritto e Giustizia*, 2016, 82, p.10.

NICOLICCHIA F., *I limiti fissati dalla Corte Costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in *Archivio penale*,2017, 2, p. 4-5.

NOCERINO W., *Le Sezioni unite risolvono l'enigma: utilizzabilità del captatore informatico nel processo penale*, in *Cassazione penale*, 2016, p. 3568.

NOCERINO W., *Prime riflessioni a margine del nuovo decreto legge in materia d'intercettazioni*, in *Sistema Penale*, 2020, 1, p.65.

PALMIERI L., *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza Scurato alla riforma sulle intercettazioni*, *Dir. pen. cont.*, 2018, 1, p. 64.

PELOSO C., *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *Dir. pen. cont.*, 2017,1, p. 159.

PRETTI D., *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in *Dir. pen. cont.*,2018, 1, p. 193

ROMANO S.-SORIO C., *L'utilizzo dei c.d. trojan horse nelle indagini penali e la tutela progressiva della libertà e segretezza delle comunicazioni*, in *Law and Media Working Paper Series*,2016, 14, p.4.

SERAFIN S., *Whatsapp, Crittografia end to end e sicurezza, riflessi nel procedimento*, in *Cammino Diritto*, 2016, 4, p. 61-62.

SPANGHER G., *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giust.pen.web*, 2018, p. 1 ss.,

TESTAGUZZA A., *I Sistemi di Controllo Remoto: fra normativa e prassi*, in Dir. pen. proc., 2014, p. 759.

TORRE M., *Il Captatore informatico nella legge delega 23 Giugno 2017, n.103*, in *Jusonline*, 2017, 3, p.438.

TRESCA M., *I programmi spia: il diritto alla privacy di fronte ai nuovi strumenti tecnologici d'indagine*,2006, in *Amministrazione in Cammino*,2016, 4, p.2.

VIGNA P.L., *Il processo accusatorio nell'impatto con le esigenze di lotta alla criminalità organizzata*, in *Giustizia penale*,1991, 3, p. 466.

ZICCARDI G., *Parlamento Europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Archivio Penale*,2017, 1, p. 247-248.

ZONARO M., *Il Trojan: Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento d'intercettazione*, in *Parola alla Difesa*, 2016, 1, p. 165.

Note a sentenza

LASAGNI G., *L'uso di captatori informatici (trojans) nelle intercettazioni "tra presenti"*, nota a Cass., sez. un., 28 aprile 2016, n. 26889, Scurato, in *Dir. pen. cont.*, 7 Ottobre 2016, p. 11.

VENGONI A.-GIORDANO L., *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, nota a *Bundersverfassungsgericht, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09,* in *Dir. pen. cont.*, 8 Maggio 2016, p. 2.

Sitografia

CARUSO C., *La libertà e segretezza delle comunicazioni nell'ordinamento costituzionale*,21 ottobre 2013, in www.forumcostituzionale.it, p.5.

NELLO ROSSI A.-BALSAMO A., *Memoria per la Camera di Consiglio delle Sezioni Unite del 28 Aprile 2016*, in www.questionegiustizia.it/doc/memoria-ssuu-procura-generale-trojan.pdf., p.3.

PARODI C., *La riforma "Orlando": la delega in tema di "captatori informatici*", 4 Aprile 2017, in www.magistraturaindipendente.it, p. 3.

PIEROZZI F., *Il caso "Haking Team": quis custodiet ipsos custodes? Problematiche e sfide per una più efficiente patnership tra settore privato e agenzie d'intelligence nella cybersecurity*, in www.dsps.unifi.it, p.4-7.

Segnalazione al Parlamento e al Governo sulla disciplina delle intercettazioni mediante captatore informatico, 30 aprile 2019, in www.garanteprivacy.it

SENOR M., *Di trojan-microspia, e-mail che non sono corrispondenza e della colpa veniale di chi usa server stranieri*, 26 Ottobre 2016, in www.filodiritto.com, p.6.

SURACI L, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni: qualche rilievo critico*, in www.pluriscedam.utetgiuridica.it, 05 gennaio 2018, p. 5.

Riferimenti giurisprudenziali

Corte Costituzionale

Corte cost., sent., 4 maggio 1972, n. 77

Corte cost., sent., 6 aprile 1973, n.34

Corte cost. sent.,6 aprile 1973, n.34

Corte cost., sent.,23 luglio 1991, n.366

Corte cost. sent., 26 ottobre 1993, n.81

Corte cost., sent.,24 febbraio 1994, n.63

Cort. cost., sent.,24 aprile 2002, n.135

Corte cost. sent., 24 Ottobre 2007 n. 348

Corte. cost., sent., 31 Ottobre 2007, n. 349

Corte cost., sent.,7 maggio 2008, n.149

Cost. cost., sent.,8 Ottobre 2008, n.336

Cort. cost. sent., 15 Gennaio 2013, n.1

Cort. cost., sent.,15 gennaio 2013, n.1

Corte Edu

Corte Edu, sent., 2 agosto 1984, Malone c. Regno Unito.

Corte Edu, sent.,2 settembre 2010, Uzun c. Germania.

Corte Edu, sent., 13 settembre 2018, Big Brother e altri c. Regno Unito.

Corte Edu, sent. del 23 Febbraio del 2016, Capriotti c.Italia.

Corte Edu, sent. del 6 Giugno 2019, Bosak e altri c. Croazia.

Corte Edu, sent., 4 dicembre del 2015, Zakharov c.Russia.

Cass., sez. I, 20 dicembre 1991, n. 5032, Marsella, in *C.e.d. Cass*., Rv.190009.

Cass. pen., sez. un., 1 agosto 1995, n.11, Costantino ed altro, in *C.e.d. Cass*., Rv. 202002.

Cass.,pen, sez. VI, 16 Ottobre 1995, n.1626, in *C.e.d. Cass*., Rv.203738.

Cass. pen., sez.I ,22 Gennaio 1996, n.1904, Porcaro, in *C.e.d. Cass*., Rv. 203799

Cass. pen., sez. VI, 26 Marzo 1996, Sollecito, n.5363, in *C.e.d. Cass*., Rv.205075

Cass. pen., sez.un., 20 novembre 1996, n.21, Glicora ed altri, in *C.e.d. Cass*., Rv. 206955.

Cass.pen., sez. I, 3 Marzo 1997, n. 3901, Telese, in *C.e.d. Cass*., Rv. 207379.

Cass. pen., sez.VI, 20 novembre 1997, n.1972, Pacini Battipaglia, in *C.e.d. Cass*., Rv. 210045.

Cass. pen., sez. VI, 21 novembre 1997, n. 4533, Avantaggiato, in *C.e.d. Cass*., Rv.210316

Cass. pen., sez VI, 14 settembre 1998, n.1934, in *C.e.d. Cass*., Rv. 211593

Cass. pen., sez. VI, 18 Giugno 1999, n. 9428, Patricelli, in *C.e.d. Cass*., Rv. 214127.

Cass.pen., sez. IV, 16 marzo 2000, n.7063, Viskovic, in *C.e.d. Cass*., Rv. 217688.

Cass. pen., sez.VI, 10 gennaio 2003, n. 3443, Mostra, in *C.e.d. Cass*., Rv. 224743;

Cass. pen., sez.VI, 10 gennaio 2003, n.6962, Cherif Ahmed, in *C.e.d. Cass*., Rv. 223733

Cass. sez.un.,24 settembre 2003, n.36747, Torcasio, in *C.e.d. Cass*., Rv. 225465.

Cass. pen., sez.un., 23 novembre 2004, n. 45189, in *C.e.d. Cass*., Rv. 229246

Cass. pen., sez. VI, 19 novembre 2005, n. 11654, Siciliano, in *C.e.d. Cass*., Rv. 233689.

Cass. pen. sez.un., 28 Marzo 2006, n.26795, Prisco, in *C.e.d. Cass.*, Rv. 234270.

Cass. pen., sez. II, 24 aprile 2007, n. 35300, Caruso, in *C.e.d. Cass*., Rv. 237848.

Cass., Sez.III, 25 Febbraio 2010, n.12562, in *C.e.d. Cass*., Rv.246594.

Cass. pen., sez.I , 2 marzo 2010, n.16293, in *C.e.d. Cass*., Rv.246656

Cass.pen., sez. V, 29 aprile 2010, n.16556, Virruso, in *C.e.d. Cass*., Rv.246954

Cass.pen., sez. V, 26 ottobre 2012, n.42021, in *Foro.it*, 2012, 12, 2, 709.

Cass., Sez. VI, 27 novembre 2012, n. 15009, Bisignani, in *C.e.d. Cass.*, Rv. 2548865.

Cass. pen., sez. VI, 8 Maggio 2013, n. 19783, in *C.e.d. Cass*., Rv. 255472.

Cass. pen., sez. II, 30 dicembre 2013, n.51867, in *C.e.d. Cass*., Rv. 258074.

Cass. pen., sez. un., 26 giugno 2014, n. 32697, in *C.e.d. Cass*., Rv. 259777

Cass. pen., sez. un., 26 giugno 2014, n.32697, in *C.e.d. Cass*., Rv. 259777.

Cass. pen., sez.III, 2 dicembre 2014, n.14954, in *C.e.d. Cass*., Rv. 263045

Cass. pen. sez. III , 29 gennaio 2015, n.12536, in *C.e.d. Cass*., Rv.262999.

Cass.Pen., Sez. III, 17 Febbraio 2015, n.20418, in *C.e.d. Cass*., Rv.263625.

Cass. pen., sez. II, 18 febbraio 2015, n.12625, Moi, in *C.e.d. Cass.*, Rv. 262927.

Cass. pen., sez. un., 26 marzo 2015, n.17325, in *C.e.d. Cass*., Rv. 263020.

Cass. pen., sez.II ,1 aprile 2015, n.19730, in *C.e.d. Cass*., Rv.263527.

Cass., sez. VI, 26 maggio 2015, n.27100, Musumeci, in *C.e.d. Cass*., Rv. 265655.

Cass. pen. sez.VI, 21 Luglio 2015, n.34809, in *C.e.d. Cass*., Rv. 264447

Cass.Pen., Sez. VI, 28 luglio 2015, n.33231, in *C.e.d. Cass*., Rv. 264462.

Cass. pen., sez. III, 10 Novembre 2015, n.50452 in C.e.d. Cass., Rv. 265615

Cass., Sez.II, 18 dicembre 2015, n.1924 in *C.e.d. Cass*., Rv.265989;

Cass. pen., Sez. III, 21 gennaio 2016, n. 2608, in *C.e.d. Cass*., Rv.266423.

Cass. pen., sez.IV, 8 Aprile 2016, n.16670 in C.e.d. Cass., Rv.266983.

Cass. pen., sez. IV, 28 Giugno del 2016, n.40903, in *C.e.d. Cass*., Rv. 268228

Cass., sez. un., 28 aprile 2016, n. 26889, Scurato, in *C.e.d. Cass*., Rv. 266905

Cass. pen. sez.un., 23 Marzo 2017, n.31345, *C.e.d. Cass*., Rv. 270076.

Cass., sez. VI, sent. 13 giugno 2017, n.36874, Romeo, in *C.e.d. Cass*., Rv.270812.

Cass.pen, sez.V, 23 Giugno 2017, n.49040, in *C.e.d. Cass*., Rv.271852.

Cass. pen., sez.V, 14 luglio 2017, n.43977, in *C.e.d. Cass.*, Rv. 271754.

Cass. pen., sez. VI,18 settembre 2017, n. 42566, in *Guida al diritto*, 2017, 41, 96.

Cass. pen, sez. II, 22 maggio 2018, n.22972, in *C.e.d. Cass*., Rv. 273000.