CAPTATORI INFORMATICI

# Intercettazioni con trojan: efficienza investigativa e sfide giuridiche



La rivoluzione tecnologica ha trasformato le tecniche investigative, portando gli investigatori da pedinamenti fisici a monitoraggi elettronici. Il captatore informatico, nonostante le sfide tecniche e giuridiche, è diventato indispensabile. Tuttavia, il suo utilizzo solleva questioni su privacy e diritti costituzionali, richiedendo una preparazione avanzata per magistrati e investigatori

Pubblicato il 30 set 2024

**Pier Luca Toselli**
Digital forensics presso Ministero

La rivoluzione tecnologica che ormai ha pervaso ogni ambito e momento delle nostre vite abbia profondamente mutato anche le **tecniche investigative**, alle quali gli investigatori devono ricorrere.


Perquisizioni online e cross-border: le nuove sfide

30 Gennaio 2024

di **Pier Luca Toselli**

## Indice degli argomenti

## L'evoluzione degli scenari invetigativi

**Gli scenari investigativi hanno subito in poco tempo una rapida evoluzione** che ha portato, per esempio, gli investigatori da lunghe notti di pedinamenti e appostamenti a più comode soluzioni "da remoto" attraverso quelle tecniche che oggi definiamo di pedinamento e monitoraggio elettronico. Del resto, è noto a tutti, come l'evoluzione "digitale" nella quale siamo immersi se da un lato ha visto il concretizzarsi di nuove figure o "forme" di reato, dall'altro richiede, a cagione dell'utilizzo del "digitale", nuove tecniche investigative. Altrettanto innegabile, come ho più volte evidenziato, che oggi non esiste, "fatto", "scenario", "contesto" investigativo, che non veda coinvolto un dispositivo digitale utilizzato per la commissione di un reato o comunque oggetto e/o contenitore di dati utili

a comprenderne le dinamiche, responsabilità, effettività di quel determinato fenomeno[2].



## Le potenzialità sottovalutate dei trojan

**Non si può poi sottovalutare come sia i criminali, che gli investigatori, ignorino, le potenzialità di questi strumenti tecnologici** ritrovandosi, inconsapevolmente nel lasciare tracce che non avrebbero mai voluto lasciare, ovvero scoprirne alcune fino a qualche istante prima note ai più.[3] Ne consegue che le investigazioni non possono più prescindere dal considerare detti dispositivi digitali elementi essenziali per le indagini sia per il loro contenuto informativo e probatorio, sia quali "strumenti" utilizzati dagli stessi investigatori e magistrati per l'effettuazione delle indagini.

Nel prosieguo, tratterò, del cosiddetto "captatore informatico" che al di là delle difficoltà tecniche e giuridiche che lo caratterizzano risulta oggi più che mai uno **strumento indispensabile**, necessario sostituto (a seguito dell'evoluzione

tecnologica) delle tradizionali “intercettazioni telefoniche” ed unico strumento allo stato capace di poter coniugare nella propria “azione” oltre all’attività di intercettazione telefonica ed ambientale, quella di intercettazione telematica ormai necessaria per l’apprensione in tempo reale non solo delle **comunicazioni** (che ormai hanno preso il sopravvento ed effettuate attraverso le “chat”**[4]** di messaggistica sia attraverso messaggi testuali, che audio-video), ma anche degli **ulteriori “elementi” presenti sul dispositivo** (file, immagini, audio, etc.) che sempre più spesso risultano strategici nell’attività investigativa.

L’enorme diffusione (ove giuridicamente possibile) di questo strumento investigativo, se da un lato evidenzia un efficienza ed efficacia, senza pari, dall’altro a cagione dell’**innegabile pervasività e perniciosità nella sfera privata**, incidendo pesantemente anche su diversi diritti garantiti costituzionalmente (il domicilio privato, la corrispondenza), richiede un elevata preparazione tecnico-giuridica in capo a tutti coloro che a vario titolo (magistrati, polizia giudiziaria, tecnici addetti alle cd. “inoculazioni”) vengono coinvolti nel suo utilizzo.

## il captatore informatico: definizione e funzionamento

La definizione captatore informatico, fa ovviamente riferimento all’azione svolta da quelli che più tecnicamente possiamo definire “virus Trojan” (Trojan Horse), il riferimento mitologico rende immediatamente, anche al profano, una rappresentazione sul suo funzionamento. Si tratta d**i una categoria specifica di malware che attraverso diverse tecniche di inganno si infiltra/inocula nel sistema informatico “target/bersaglio”** ed una volta insidiatosi permette (sia concessa dai “puristi” la sintesi) di svolgere diverse azioni, invero, una volta attivati, i cosiddetti “Trojan Horse” possono eseguire una serie di operazioni malevole, quali il furto di dati, la sorveglianza del sistema, o l’apertura di backdoor per consentire accessi non autorizzati.

I trojan si distinguono proprio per la loro capacità di **aggirare i sistemi di sicurezza** tramite metodi di offuscamento e polimorfismo, rendendo difficile la

loro individuazione e rimozione da parte degli strumenti software e hardware comunemente deputati al loro contrasto.

## Tecniche di distribuzione e consegna dei trojan

La loro distribuzione può avvenire attraverso diverse tecniche, anche di ingegneria sociale, atteso che lo scopo è quello per l'appunto di "installare/inoculare" il Trojan Horse nel dispositivo "target". Essi, quindi, possono essere **"distribuiti" attraverso siti web compromessi**, piuttosto che **allegati** e-mail, **software scaricati** da fonti non attendibili etc., invero, le tecniche di "consegna" sono in continua evoluzione dinanzi a sempre più sofisticati strumenti di contrasto e a protezione da queste "inoculazioni" vi è sempre più il ricorso a nuove (e vecchie)**[5]** tecniche nell'ovvio tentativo di far pervenire e far operare questi insidiosi trojan sul bersaglio di interesse.

Concentrerò il "focus" sull'utilizzo del captatore quale strumento per le "odierne" intercettazioni ambientali, anche se come peraltro già evidenziato in nota (1), questo strumento viene utilizzato, non senza criticità a causa della sua pervasività, anche per numerose alte operazioni.

## Captatore informatico come microspia elettronica

Mi concentrerò pertanto sulla **funzione di microspia elettronica** evoluzione delle microspie tradizionali utilizzate per le intercettazioni ambientali, che, come vedremo, pongono non pochi interrogativi e difficoltà tecnico-giuridiche.

Circoscriverò l'ambito a questo aspetto anche in relazione ad **una recente Sentenza della Corte di cassazione**, espressione di quanto sia elevato l'interesse attorno all'utilizzo di questo delicato strumento investigativo.

## I vantaggi dei trojan per gli investigatori

Il ricorso all'utilizzo dei "trojan" può rappresentare molteplici vantaggi in capo agli investigatori che senza pretesa di esaustività riassumo qui per punti,

richiedendo ciascuno un approfondito studio e dibattito:

- **Riduzione del rischio di essere scoperti** e di vanificare le attività investigative. E 'evidente come la possibilità di agire da remoto, in modo occulto e con strumenti che non "palesano" la presenza degli operatori si risolva in un enorme vantaggio per quest'ultimi;
- **Dilatazione delle capacità e funzionalità investigative**, lo strumento non solo "capta" le conversazioni, attraverso l'attivazione da remoto del microfono e della telecamera (ove presente) del dispositivo target, ma laddove "inoculato" su dispositivi "mobili" (notebook, tablet, smartphone etc.) permette di seguire, più corretto dire "pedinare", il soggetto utilizzatore di quel dispositivo. Sempre su questo punto si considerino poi le potenzialità costituite dal trojan di affiancare in un'unica soluzione strumenti per:
- **la captazione di tutto il traffico telematico e telefonico**;
- carpire attraverso il microfono e la webcam/fotocamera le **conversazioni** che vengono effettuate in prossimità del dispositivo infetto;
- effettuare **una perquisizione da remoto del dispositivo infetto**, finanche di intere partizioni del disco ovvero di singoli file ed artifacts ritenuti corpo del reato, cose pertinenti il reato;
- il **tracciamento e positioning del soggetto**;
- **carpire password ed altre digitazioni** del soggetto attraverso le funzioni "Keylogger" ove applicabili ovvero attraverso l'apprensione "on line" delle password ed altre digitazioni effettuate sul target da parte del soggetto attinto dall'attività investigativa.

Questi due punti risultano già ampiamente sufficienti a scatenare un acceso dibattito sul trojan che ovviamente non esauriremo in queste poche righe.

## La "sana competizione" tra investigatore e investigato

Sul primo punto ritengo si tratti della "sana competizione" tra investigatore ed investigato, fintanto che il primo risulta **legittimato all'utilizzo dello strumento**

ed il secondo consapevole dei **rischi** e dei nuovi strumenti di investigazione saprà (forse) cautelarsi, del resto per quanto l'inoculazione del trojan possa avvenire anche in modo "occulto" e da remoto è altrettanto vero come l'azione del trojan sia accompagnata da una ormai nota "sintomatologia" costituita essenzialmente da un ingiustificato consumo della batteria dei dispositivi (salvo ovviamente siano continuamente alimentati – PC Desktop) e da un aumentato consumo del traffico dati che ove attentamente monitorato potrebbe sollevare ipotesi di essere stati "infettati" e conseguentemente il soggetto insospettito potrebbe rivolgersi ad un tecnico informatico, per la verifica di ciò.

## Normativa e giurisprudenza sul captatore informatico

Per quanto riguarda la sua "evoluzione" sul piano investigativo e normativo, va evidenziato come fino al dicembre 2017**[6]**, **non vi fosse una norma che ne disciplinava l'utilizzo**, soprattutto sul piano del precipuo utilizzo di cui qui ci occuperemo, quale mezzo di "intercettazione ambientale" ex art. 266 comma 2 del c.p.p., prima di questa data, la giurisprudenza chiamata più volte ad esprimersi, cercava di ricondurre l'utilizzo dello strumento a quanto già "tipizzato" dal codice di procedura penale ovvero considerando determinati utilizzi del trojan del tutto "atipici"**[7]**.

Tuttavia, tali soluzioni lasciavano acceso **un fervente dibattito[8]** soprattutto laddove tra i molteplici "utilizzi" del trojan si doveva considerare quello che poi ne sarebbe divenuto il principale, ovvero quello di intercettazione ambientale, in particolare delle comunicazioni tra presenti, e … non, come meglio vedremo nel prosieguo.

### Le intercettazioni tramite trojan su dispositivi mobili

Specificatamente il D.lgs. 29 dicembre 2017 n. 261 differenzia tra le intercettazioni relative a delitti di criminalità organizzata e quelle relative agli altri reati stabilendo presupposti e limiti differenziati e specifici. Per quanto riguarda

**le intercettazioni tramite trojan installato su dispositivi "mobili"** (portatili) nei procedimenti riguardanti i delitti di criminalità organizzata, è possibile richiederle e autorizzarle anche solo sulla base di sufficienti, e non gravi indizi di reato, anche allorquando vi sia solo necessità e non indispensabilità per la prosecuzione delle indagini, il legislatore ha altresì stabilito che in tali casi la durata delle operazioni sia di 40 giorni prorogabile di volta in volta per altri 20 giorni allorquando ne permangano i presupposti e le motivazioni.

## Estensione dell'uso del trojan ai reati contro la PA

Un successivo intervento legislativo**[9]** ha esteso l'uso del trojan anche alle indagini riguardanti alcuni reati contro la pubblica amministrazione, commessi da pubblici ufficiali e incaricati di un pubblico servizio, punibili con la reclusione oltre i 5 anni, prevedendo che previa indicazione delle ragioni che giustifichino l'utilizzo, lo stesso potrà essere utilizzato al pari di ciò che avviene per i delitti di criminalità organizzata anche all'interno di quei luoghi previsti dall'art. 614**[10]** del C.P.

## Le recenti sentenze della Corte di cassazione

Una recente Sentenza della IV Sezione Penale della Corte di Cassazione, evidenzia come l'utilizzo di un così delicato strumento di indagine se dal un lato dimostra tutta la sua efficacia ed efficienza dall'altro si scontra continuamente con **molteplici complessità tecnologiche e legali**, segno evidente che l'invasività del trojan in talune "sfere" Costituzionalmente protette e tutelate sollecita un continuo dibattito nel delicato equilibrio tra diritti costituzionalmente protetti e le diverse esigenze in conflitto (per esempio: accertamento dei reati e protezione della privacy).

Una recente sentenza è intervenuta in tema di captatore informatico "lumeggiando" meglio il complesso articolato normativo, sviluppatosi attorno l'utilizzo del captatore informatico. La Sentenza ha riguardato il ricorso per

Cassazione, in tema di misure cautelari, da parte dell'indagato (per il reato di cui all'art. 73, comma 4 e 80 D.P.R 309/90 – detenzione di stupefacenti), attinto dall'applicazione della misura della custodia cautelare in carcere. La misura era stata erogata in quanto l'indagato veniva accusato di detenzione di sostanze stupefacenti a seguito di alcune **intercettazioni eseguite mediante captatore informatico**. In particolare, la condotta contestata al ricorrente derivava dalle intercettazioni svolte attraverso un captatore informatico, autorizzato nell'ambito di altro procedimento per tentato omicidio (artt. 56 e 575 C.P.).

La situazione in trattazione appare oltremodo alquanto comune e diffusa nell'ovvia considerazione che **il captatore informatico come abbiamo visto meglio sopra effettua diverse operazioni di intercettazione (ambientale, telefonica, telematica) senza alcun "filtro"** e che è alquanto comune che nel corso delle intercettazioni svolte per un determinato reato, si pervenga anche alla "scoperta", "documentazione", "prova", "indizio" etc. di altri reati diversi da quello/i in radice all'emissione del provvedimento autorizzatorio l'uso del captatore.

## Utilizzo dei risultati delle intercettazioni: aspetti giuridici

In definitiva la sentenza qui citata Corte Suprema di Cassazione Quarta Sezione Penale n. 25401-24 Sent. N. Sez. 747/2024 CC- 20/06/2024 RGN 15130/2024 – Pres. Patrizia Piccialli Cons. est. Mariarosa Bruno, ha preso in considerazione **la possibilità di utilizzare le informazioni acquisite attraverso un captatore informatico per indagare e procedere su reati diversi da quelli in "motivazione"** al provvedimento autorizzatorio che ha consentito l'inoculazione ed esercizio del captatore informatico.

La Corte richiama in particolare l'art. 270 c.p.p. che nell'attuale formulazione dispone:

"1. **I risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti**, salvo che risultino rilevanti e

indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.

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** qualora risultino indispensabili per l'accertamento dei delitti indicati dall'articolo 266, comma 2-bis.

2. Ai fini della utilizzazione prevista dal comma 1, i verbali e **le registrazioni delle intercettazioni sono depositate presso l'autorità competente** per il diverso procedimento. Si applicano le disposizioni dell'articolo 268, commi 6, 7 e 8.

3. Il pubblico ministero e i difensori delle parti hanno altresì **facoltà di esaminare i verbali e le registrazioni** in precedenza depositati nel procedimento in cui le intercettazioni furono autorizzate.".

## La "distinzione" tra l'intercettazione di comunicazioni tra presenti e non presenti

Soffermandosi in particolare sul comma 1 bis, la Cassazione evidenzia come le restrizioni previste dal legislatore riguardino esclusivamente le conversazioni tra presenti (ovvero quella funzione particolare e specifica del captatore in grado attraverso l'attivazione del microfono di acquisire e captare le conversazioni tra presenti che si stanno svolgendo in un determinato luogo). La stessa Corte evidenzia come "il captatore informatico come è noto, è un programma informatico intrusivo (c.d.malware) che si installa su dispositivi mobili (cellulare, computer, tablet), dotato di diverse funzionalità: esso infatti consente la intercettazione di chiamate vocali, di chat e di messaggi istantanei; consente inoltre l'ascolto di conversazioni tra presenti, permettendo di intercettare le conversazioni che si svolgono tra più persone che si trovino nelle vicinanze del dispositivo"".

Gli Ermellini introducono pertanto una netta “distinzione” tra l’intercettazione di comunicazioni tra presenti e non presenti. La Corte enfatizza con riferimento all’**art. 270 comma 1 bis c.p.p.** la precisazione voluta dal legislatore attraverso la frase “ *i risultati delle intercettazioni tra presenti”,* sottolineando come la scelta di limitare l’utilizzo in altri procedimenti e fuori della previsione del decreto autorizzativo a delitti di particolare gravità e allarme sociale, costituisca di fatto l’attuazione del necessario “bilanciamento” di valori costituzionalmente garantiti e contrastanti, individuati qui specificatamente nel diritto dei singoli alla libertà e segretezza delle comunicazioni contrapposta all’interesse pubblico di repressione dei reati e contrasto alla criminalità.

Pertanto, laddove (come nel caso di specie) l’intercettazione del captatore non abbia interessato una conversazione tra presenti, ma di fatto venga ad essere costituita da una chiamata “vocale” tra un presente ed una persona non presente nel luogo in cui si trova il dispositivo inoculato utilizzato per l’intercettazione, la disciplina concernente l’utilizzo di detti risultati, andrà ricondotta alle previsioni di cui al primo comma dell’art. 270 c.p.p.

## Massima della sentenza e nuovi paradigmi

Si giunge pertanto alla seguente massima: “in tema di utilizzazione dei risultati di intercettazioni effettuate con captatore informatico per delitti diversi da quelli per cui è stato emesso il decreto autorizzativo, ha affermato che il disposto dell’art. 270, comma 1-bis, cod. proc. pen., nella parte in cui limita l’utilizzazione all’accertamento dei delitti indicati all’art. 266, comma 2-bis, cod. proc. pen., è riferito esclusivamente alla captazione di conversazioni intercorse tra presenti, mentre per quelle che non si svolgono tra **presenti opera** la clausola di salvezza contenuta nell’”incipit” del medesimo art. 270, comma 1-bis, cod. proc. pen., che rinvia alle condizioni previste nel primo comma dell’art. 270 cod. proc. pen.”.

La sentenza effettuando questa distinzione, impone agli addetti ai lavori, magistrati e forze dell’ordine **nuovi paradigmi sull’utilizzo del captatore**

**informatico**.

## Complessità e necessità di regolamentazione

Come già detto sopra la "casistica" qui affrontata risulta giocoforza ampia e diffusa essendo probabilmente più unici che rari quei casi in cui l'attività di captazione resta circoscritta "esclusivamente" ai reati per cui è stata autorizzata l'attività attraverso il trojan.

Ancora una volta l'intervento della Cassazione si è manifestato in tutta la sua funzione nomofilattica ed unificatrice diretta ad assicurare la certezza nell'interpretazione della legge.

Un intervento così puntuale e dirimente segna di fatto i **confini circa l'utilizzazione dei risultati delle intercettazioni in altri procedimenti,** in un momento in cui il diffuso ricorso al captatore informatico, (spesso unico strumento capace nella sua funzione di "captatore occulto", di superare le barriere e difese poste a difesa degli interessi delle più perniciose e pericolose organizzazioni criminali, nonché di contrastare efficacemente quei crimini contemplati dall'art. 266 c.p.p.**[11]**), viene "facilmente" a scontrarsi con fondamentali diritti Costituzionali, a cagione della potenzialità e pervasività nella sfera privata, dello strumento.

Ben vengano quindi tutti gli interventi che attraverso precise indicazioni possano tracciare i confini entro i quali gli investigatori possono "allargare" l'utilizzo dei risultati delle autorizzate attività di intercettazione ad altri procedimenti, evitando così anche a seguito della novella del 2019 (decreto legislativo 161) che :*" si apra la strada alla libera circolazione probatoria delle risultanze delle captazioni digitali, determinando anche una sostanziale violazione della garanzia di riserva della giurisdizione prevista dall'art. 15 della Costituzione."* **[12]**

## Il necessario bilanciamento tra tecniche investigative e diritti costituzionali

L'utilizzo dei captatori informatici rappresenta per le moderne investigazioni **un enorme vantaggio in termini di efficienza, efficacia e sicurezza**. In particolare, la possibilità di poterli inoculare ed utilizzare all'insaputa dell'indagato mette a disposizione degli investigatori e della magistratura un potentissimo strumento capace di concentrare in un tutt'uno molteplici "azioni investigative" senza le quali probabilmente diversi reati sarebbero oggi più che mai difficili, se non impossibili da perseguire**[13]**.

Nell'evidenziare che la Sentenza qui in commento si è occupata principalmente ed esclusivamente di una sola di queste azioni, (l'intercettazione di una conversazione tra una persona presente ed una no) **la strada che si dipana innanzi all'utilizzo di questi strumenti nelle moderne indagini appare anche lunga e dai contorni tutt'altro che definiti,** invero molteplici e sempre più complesse sono le "situazioni" che si concretizzano di volta in volta innanzi agli investigatori e che richiedono sforzi interpretativi di non facile e non sempre sicura soluzione, nell'intento di "qualificare", "giustificare" "legittimare" una di quelle molteplici azioni, nuova ed in evoluzione.

Se da una parte le intercettazioni costituiscono l'apice, la punta di diamante di azioni che impattano pesantemente in quel bilanciamento di valori costituzionalmente garantiti e contrastanti tra loro, tanto da sollecitare la Suprema Corte in una presa di posizione assolutamente chiara e dirimente, come nel caso qui trattato, dall'altra vengono tralasciate altre **complesse e pervasive azioni del "trojan"**, come le attività di perquisizioni da remoto piuttosto che la videosorveglianza nella privata dimora, piuttosto che l'acquisizione delle digitazioni della tastiera o le visualizzazioni dello schermo, ossia quelle azioni "residuali" ma altrettanto strategiche ed invasive che il trojan è in grado di porre e potrà porre in essere.

Invero, **quest'ultime non hanno ancora ricevuto una specifica regolamentazione,** restando circoscritte ad altalenanti definizioni talvolta di mezzi di ricerca della prova "atipici", talaltre di tentavi di assimilarli "analogicamente" ad altri strumenti, tecniche, investigative già utilizzate, ma che anziché porre soluzioni e chiarezza, contribuiscono a rendere talvolta inspiegabile "lo spostamento dell'ago della bilancia dei diritti" in quel delicato bilanciamento più volte qui accennato.

## Conclusioni

Nell'invocare sempre più precisi e diretti interventi della Suprema Corte in questi contesti, non resta che rilevare come la complessità tecnica e giuridica formatasi attorno alle indagini "digitali" sia ormai un treno in corsa che richiede sempre più, dinanzi ad un inarrestabile progresso tecnologico che riverbera nelle indagini (fornendo ormai quotidianamente nuove possibilità tecnologiche-investigative), un'attenta valutazione, ponderazione e considerazione dei "diritti" in gioco.

Tutta questa complessità richiede allora che gli attori coinvolti attraverso un'attenta e precisa preparazione tecnico-giuridica sappiano sapientemente coniugare ed utilizzare le oramai infinite ed inarrestabili possibilità "investigativo-tecnologiche" in uno spazio che vede sempre più facilmente coinvolti diritti fondamentali costituzionalmente protetti.

**[1] https://www.agendadigitale.eu/sicurezza/investigare-nel-mondo-digitale-le-sfide-delle-perquisizioni-online-e-cross-border/** .

**[2]** Si è più volte fatto cenno in altri articoli di questa ormai inarrestabile pervasività del digitale tanto da poter affermare senza ombra di smentita che oramai la "prova" di qualsiasi illecito si rileva e/o desume (quest'ultimo riferimento è ai cd. "indizi") dall'esame dei dispositivi digitali coinvolti e dai dati in essi contenuti.

**[3]** si pensi ai file di LOG delle più elementari APP per dispositivi mobili, spesso creare per motivi di monitoraggio del funzionamento della stessa APP sono delle vere "fucine" di informazioni spesso ignote agli investigatori che ne scoprono le potenzialità molto spesso casualmente e magari per altri motivi lontani dagli scopi investigativi prefissati.

**[4]** WhatsApp, Telegram, Messanger etc.

**[5]** il riferimento è alle più tradizionali tecniche di inoculazione che prevedono un "inoculazione" diretta di questi "captatori" sul dispositivo "target" che con varie tecniche viene ad essere anche se per pochi minuti nelle mani /disponibilità della PG e tecnici operanti.

**[6]** D.Lgs. n. 216 del 29 dicembre 2017.

**[7]** Cass. Sez. Unite n. 26795 del 28 marzo 2006.

**[8]** L'elemento di maggior "contrasto" del resto era rappresentato invero dalla natura itinerante del trojan che ospitato su di un dispositivo, lo accompagnava in ogni dove soprattutto all'interno di quei luoghi di "privata dimora" ai quali la Costituzione riconosce una particolare tutela.

**[9]** Decreto Legge 161/2019 – convertito con modificazioni dalla Legge 28 febbraio 2020, n. 7.

**[10]** Ci si riferisce a: " … omissis … nell'abitazione altrui, o in un altro luogo di privata dimora… omissis…".

**[11]** 1. 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 dell'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, 517 quater e 633, secondo comma, del codice penale;

f-quater) delitto previsto dall'articolo 612 bis del codice penale.

f-quinquies) delitti commessi avvalendosi delle condizioni previste dall'articolo 416 bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.

2. Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita

nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, 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.

**[12]** Cfr. il "ritenuto in fatto" della Sentenza in commento Cass. Pen. Sez. IV n. 25401 del 20.06.2024.

**[13]** Appare evidente anche al profano come solo attraverso questi strumenti sia possibile da un lato carpire risultati probatori diversamente impossibili da ottenere e dall'altro reprimere quei reati che si sviluppano e proliferano nel segreto (oltre ai reati associativi, si pensi anche ai reati di corruzione, concussione etc.)





## Valuta la qualità di questo articolo