*A mia madre, con la speranza che sia sempre fiera di me.*

*A mio padre e mia sorella, che mi hanno sostenuto in ogni momento ed in ogni mia scelta.*

*Ad Antonio, Angela, Adolfo e Annarita, perché sono stati come una seconda famiglia.*

*A Francesco, amico da una vita e sempre presente, non solo nei momenti di bisogno.*

*Ad Umberto e Alessandro, amici e compagni imprescindibili.*

*A Lorenzo, Giovanni, Michele e Luigi, perché questo lavoro è anche merito vostro e delle innumerevoli ore passate a studiare assieme.*

*Agli amici di sempre, Claudia, Isabella, Franco e Federica, con la speranza di rimanere sempre così legati.*

*Ai "nuovi" amici, Baldo, Alberto, Enrico, Gabriele, Alessio, Vincenzo e Francesco, con la certezza che ci ritroveremo presto a lavorare assieme.*

*A Luca, con il ricordo di un anno passato assieme a Parma e il piacere di averti ancora come amico.*

*A Federico ed Eleonora, grazie per aver reso lo scambio a Varsavia indimenticabile.*

*All' Avv. Valentino Fracasso, per i tanti consigli e per l'idea sulla quale incentrare la mia tesi.*

*"La vita è come un'eco: se non ti piace quello che ti rimanda, devi cambiare il messaggio che invii" (James Joyce)*

# Indice sommario

## Capitolo 3..... p. 86

## Presupposti per l'utilizzo del virus *trojan*

# Introduzione

L'ingresso della tecnologia digitale nel processo penale rappresenta ormai un dato incontrovertibile in quanto, quotidianamente, si fa ricorso a determinati strumenti tecnologici che favoriscono diverse fasi del processo. Negli ultimi anni, sia da parte della giurisprudenza di merito e di legittimità nonché da numerosi autori in dottrina, si possono trovare diverse pronunce riguardanti strumenti tecnologici utilizzati durante le indagini da parte degli inquirenti. In particolare, si fa riferimento ai c.d. "captatori informatici", quali navigatori satellitari, programmi di clonazione degli hard-disk o, più recentemente, ai cosiddetti *software* informatici di controllo da remoto, come i *Trojan*. Le peculiarità di questi strumenti sono molteplici e sono state riconosciute anche da una recente pronuncia delle Sezioni Unite. In primis, a differenza di altri strumenti intrusivi, questi *software* possono essere installati da remoto ed attivati sul dispositivo da intercettare in modo occulto e a distanza. In secondo luogo, la gamma di operazioni permesse dall'utilizzo di questi strumenti informatici risulta molto più ampia rispetto ai normali strumenti intercettivi: l'accesso, con possibilità di estrarre copia anche in tempo reale, ai dati memorizzati sul dispositivo, la registrazione del traffico di dati in entrata e in uscita, ivi compreso quanto digitato sulla tastiera, la registrazione delle telefonate e anche delle videochiamate e, altra peculiarità di tale strumento, l'attivazione delle funzionalità di microfono/telecamera indipendentemente dalla volontà del possessore del dispositivo. Proprio quest'ultimo aspetto sottolineato rende il dispositivo utilizzato dall'utente in grado di essere utilizzato come strumento di registrazione di tutto ciò che avviene nel raggio di azione dello stesso, sfruttando quindi l'abitudine sempre più radicata di portare sempre con sé tali strumenti tecnologici, che possono spaziare da un semplice *smartphone* fino ai più recenti *Apple watch* o

*Google glass*. Questo tipo di strumento intercettivo quindi si va ad inserire nel complesso sistema relativo alle intercettazioni architettato dal codice penale e da quello di procedura penale, sollevando non pochi dubbi in merito alla sua applicabilità nonché alla sua utilizzabilità sia nel corso del processo sia nella fase investigativa. Il presente lavoro si pone quindi l'obiettivo di analizzare il quadro normativo italiano e sovranazionale relativo alle intercettazioni e alla possibilità di utilizzo dei c.d. "captatori informatici" come strumento investigativo.

Il primo capitolo sarà dedicato alla disciplina generale dell'ordinamento italiano dettata in tema di intercettazioni. Partendo dalla nozione stessa di intercettazione, dai suoi limiti oggettivi e soggetti, e dalla definizione di "intercettazione ambientale" o "fra i presenti", si analizzerà il contenuto del nuovo articolo 266-*bis* c.p.p. introdotto recentemente dal legislatore e che introduce la nuova disciplina relativa alle intercettazioni di comunicazioni informatiche o telematiche. Sempre all'interno del primo capitolo verranno inoltre presi in considerazioni due ulteriori aspetti relativi alle intercettazioni: la libertà e la segretezza delle comunicazioni e la tutela del domicilio. Il primo aspetto è sempre stato un punto critico della disciplina relativa alle intercettazioni, mentre il secondo aspetto, la tutela del domicilio, diventa uno dei nodi principali da sciogliere per l'effettivo utilizzo dei captatori informatici. Inoltre, per poter meglio delineare il quadro d'insieme, si farà riferimento anche ai principi costituzionali nonché a quelli stabiliti dalla normativa europea all'interno della Convenzione Europea dei Diritti dell'Uomo (CEDU).

Il secondo capitolo sarà dedicato all'analisi dell'utilizzo dei captatori informatici per scopi intercettivi. Il nuovo strumento nasce infatti da un'esigenza investigativa che si propone innanzitutto di rimanere al passo con i tempi e che, in secondo luogo, tenta di adattare i progressi tecnologici all'attività investigativa. Questa nuova esigenza verrà esposta

partendo dall'analisi di due casi concreti, il c.d. "Caso Hacking Team" relativo ad una società di *information technology* milanese rimasta vittima, nel 2015, di un attacco da parte di hacker informatici con seguente pubblicazione di materiale riservato e il "Caso Gamma Group", relativo ad una società di *information technology* tedesca. Prendendo spunto sempre dai sopracitati casi, nonché da pronunce giurisprudenziali e da riferimenti dottrinali si passerà a fornire una definizione di captatore informatico, analizzando anche le recenti proposte legislative in materia, volte a tentare di colmare un vuoto normativo per le intercettazioni che fanno uso di suddetto strumento. Nella parte conclusiva del capitolo verrà analizzato l'ambito di applicazione dei captatori informatici, prendendo in considerazione in particolare quanto espresso nelle recenti pronunce giurisprudenziali e quindi l'utilizzo nell'ambito dei "delitti di criminalità organizzata" e, inoltre, analizzando la disciplina derogatoria del d.l. 152/1991 dal titolo "Provvedimenti urgenti in tema di criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa".

Il terzo capitolo sarà invece dedicato ai presupposti per l'utilizzo del virus *trojan*, il *software* informatico utilizzato per il controllo da remoto del dispositivo posto sotto intercettazione. Il capitolo partirà dall'analisi della recente pronuncia delle Sezioni Uniti della Corte di Cassazione, la c.d. "Sentenza Scurato", delineando quindi attraverso l'utilizzo delle motivazioni della Corte in quali casi sia possibile utilizzare i captatori informatici come strumento investigativo e sottolineando di nuovo la nozione di "criminalità organizzata", altro presupposto fondamentale per l'utilizzo dei sopracitati strumenti. Verrà inoltre analizzata la funzione di garanzia svolta dal decreto di autorizzazione alle operazioni di intercettazioni e, in particolare, verranno sottolineati tre punti chiave: in *primis* i requisiti del decreto di autorizzazione, in secondo luogo i gravi indizi di reato disciplinati dall'art. 267 comma 1 c.p.p. e infine, le modalità

di esecuzione delle operazioni relative alle intercettazioni, ponendo però l'attenzione nella parte finale anche alla possibile necessità di molteplici decreti di autorizzazione in quanto diversi sono i tipi di intercettazione posti in essere tramite il captatore.

Il quarto capitolo sarà incentrato sull'utilizzo pratico del captatore informatico.
Partendo dal presupposto fondamentale della necessaria "neutralità tecnica" delle intercettazioni, si analizzerà l'applicazione pratica e il funzionamento del *software* spia partendo dall'installazione da remoto da parte degli agenti di polizia giudiziaria, quindi la cosiddetta fase di "infezione" del dispositivo, fino ad arrivare alla captazione dei contenuti del dispositivo sottoposto ad intercettazione e alla fase successiva al completamento della captazione delle informazioni desiderate. Si vedranno inoltre le svariate funzioni che il captatore informatico può ricoprire ed in particolare il suo utilizzo in funzione di *keylogger*, ossia l'intercettazione e la cattura di ciò che l'utente scrive utilizzando la tastiera del dispositivo, con la problematica ad esso connesso in quanto è un particolare tipo di attività posta in essere dal captatore di difficile inquadramento giuridico. La parte finale del capitolo sarà incentrata inizialmente sul problema della captazione delle e-mail in formato "bozza" e delle *chat* sviluppatesi non contestualmente con l'attività di captazione, ponendo numerosi interrogativi sull'effettivo utilizzo ma soprattutto sul valore attribuibile alle suddette, per poi passare alla disamina di un'ulteriore funzione del captatore informatico, ossia quella relativa alla possibilità di *download* e *upload* di *file* sul dispositivo intercettato e concludere, infine, con l'utilizzo del captatore informatico per il c.d. "pedinamento elettronico", ossia tramite la localizzazione satellitare del dispositivo sottoposto ad intercettazione.

Il capitolo quinto si incentrerà totalmente sul regime di utilizzabilità di

questo tipo di intercettazioni. All'inizio del capitolo verrà sottolineata la presa di posizione delle Sezioni Unite con l'emanazione della sentenza "Scurato" con cui i supremi giudici dichiarano l'irrilevanza, all'interno del provvedimento di autorizzazione dell'intercettazione, dell'indicazione del luogo ai fini della legittimità delle stesse, analizzando infine uno dei problemi che si pone dopo il "via libera" da parte delle Sezioni Unite all'utilizzo dei captatori informatici, ossia il possibile rischio di strumentalizzazione del reato associativo, reato per il quale, secondo le Sezioni Unite, il captatore può essere utilizzato lecitamente. In quest'ottica si pone quindi l'analisi effettuata rispetto al quadro normativo nazionale di riferimento, applicabile alle intercettazioni in generale e quindi alla loro ammissibilità all'interno di un procedimento penale. Tuttavia, essendo i captatori informatici uno strumento del tutto nuovo e, per certi versi, molto più invasivo rispetto alle tradizionali intercettazioni telefoniche, si pone il problema del difficile inquadramento giuridico dello strumento, problema affrontato da parte del legislatore con il disegno di legge "Orlando", con il quale si cerca di regolamentare l'utilizzo dei captatori.

Il sesto ed ultimo capitolo tratterà il tema dei captatori informatici da un punto di vista puramente sovranazionale, in particolare si prenderà in considerazione la normativa europea e nordamericana in tema di intercettazioni e conservazione dei dati, in modo da delineare il tipo di regolamentazione dello strumento adottata dagli Stati esteri. Verrà analizzata la Convenzione *Cybercrime* di Budapest del 23 novembre 2001 e, in modo da delineare in maniera più approfondita la questione a livello sovranazionale, si prenderà in considerazione il Regolamento Generale sulla Protezione dei Dati (GDPR) varato dal Parlamento Europeo e dal Consiglio d'Europa il 27 aprile 2016. Verranno inoltre presentati due casi concreti in tema di captatori informatici: in primo luogo si analizzerà l'esperienza tedesca, prendendo spunto da una sentenza della Corte

Costituzionale tedesca relativa alle misure di sorveglianza occulte; dall'altro lato si prenderà in considerazione il recente scandalo avvenuto negli Stati Uniti relativo alla *National Security Agency* (NSA), l'Agenzia di sicurezza nazionale statunitense la quale, secondo quanto ricostruito grazie alle dichiarazioni e alla pubblicazione di *file* sensibili di un ex-dipendente della CIA di nome Edward Snowden, teneva sotto sorveglianza (occulta) milioni di persone, realizzando la più grande operazione di sorveglianza di massa conosciuta dall'uomo e dando vita al c.d. scandalo *Datagate*.

# Capitolo 1

# Le intercettazioni e i principi fondamentali

SOMMARIO: 1 – Nozione di intercettazione. – 1.1 – Limiti oggettivi e soggettivi. – 1.2 – Le intercettazioni "tra presenti" o c.d. "ambientali". – 1.3 – Il nuovo articolo 266-*bis* c.p.p. – 2 – Libertà e segretezza delle comunicazioni. – 3 – La tutela del domicilio. – 3.1 – Normativa nazionale: l'inviolabilità del domicilio. – 3.2 – Normativa europea: convenzione europea dei diritti dell'uomo.

## 1 – Nozione di intercettazione

La disciplina sulla intercettazioni, per evidenti ragioni tecnologiche, non poteva essere prevista nei codici antecedenti all'invenzione del telefono, datata 1876 e nondimeno, la limitata diffusione di tale strumento per un lungo periodo di tempo ha portato il legislatore dell'epoca, in particolare con il codice italiano del 1913, ad occuparsi di tale fenomeno in termini estremamente indiretti e astratti, qualificando tale disciplina come una "comunicazione a distanza tra privati"[1]. La prima disciplina organica sul tema delle intercettazioni può essere rinvenuta quindi nel vigente codice di procedura penale, allorquando parte della dottrina aveva impostato un

[1] C. PARODI, *Le Intercettazioni. Profili operativi e giurisprudenziali,* in *Giurisprudenza Oggi*, di P. CENDON, Giappichelli Editore, 2002, pp. 11 e ss.

confronto tra intercettazione e sequestro, sulla scia di una equiparazione legislativa dei colloqui tra persone ai documenti cartacei[2]. Tale teoria ha avuto vita molto breve in quanto, in primo luogo il progresso tecnologico ha messo in evidenza la profonda differenza esistente tra documenti cartacei e dati forniti dalle moderne tecnologie di captazione, in secondo luogo la stessa *ratio* dell'intercettazione, sottesa a ricercare elementi investigativi non noti, è del tutto diversa da quella del sequestro, in cui gli elementi sono già noti e se ne vuole assicurare il possesso in ambito di indagine e processuale, infine, mentre il sequestro è un atto "a sorpresa" ma palese, l'intercettazione ha una natura necessariamente nascosta[3]. Il codice del 1988, come il precedente, non contiene una definizione esplicita di intercettazione ma, pur mancando, essa può essere considerata tecnicamente come un mezzo di ricerca della prova, in considerazione della sua collocazione all'interno del titolo III del libro III del codice di procedura penale relativo ai mezzi di ricerca della prova. La semantica stessa, con il termine intercettare in relazione al conversare o comunque al comunicare, suggerisce un'attività di interposizione nell'ascolto di una comunicazione tuttavia senza ostacolarla né impedirla. Il senso letterale del termine è infatti ripreso in toto dalla norma di cui all'art. 266 c.p.p. che individua l'attività intercettiva «con chiaro riferimento alla sola presa di cognizione, tralasciando qualsivoglia accenno all'interruzione o all'impedimento[4]». Tuttavia, in modo da poter stabilire i confini di applicazione dell'istituto, l'art. 266, comma 1, c.p.p., con una formula "aperta" aggiunge alle figure delle conversazioni e comunicazioni anche quelle indicate dall'amplia clausola «altre forme di telecomunicazione». Da un lato il legislatore ha voluto quindi ricomprendere, seguendo il

[2] P. G. GOSSO, Voce *Intercettazioni telefoniche*, in *Enciclopedia del diritto*, vol. XXI, 1971, pp. 890 e ss.
[3] P. BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria,* in *Studi di diritto processuale* raccolti da Giovanni Conso, Giuffrè Editore, 2002, pp. 9 e ss.
[4] P. BRUNO, *Intercettazioni di comunicazioni o conversazioni*, in *Dig. Disc. Pen.,* 1993, vol. VII, pp. 178 e ss.

progresso tecnologico, nuovi mezzi di comunicazione, mentre dall'altro ha voluto estendere le garanzie riconosciute alle persone sottoposte ad intercettazione. La stessa giurisprudenza riconosce la correttezza di tale impostazione interpretativa e inoltre specifica che, le intercettazioni regolate dagli artt. 266 e segg. c.p.p. «consistono nella captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo, attuata da soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato[5]». Sia la collocazione all'interno del codice di procedura penale, sia l'autorevole dottrina e la giurisprudenza, consentono dunque di enucleare, pur in assenza di una espressa definizione legislativa in tema, un chiaro concetto di intercettazione. Si tratta quindi, di una attività di indagine preliminare – in quanto finalizzata all'assunzione da parte del Pubblico Ministero di elementi "indispensabili" per la prosecuzione delle indagini – che si fonda sulla captazione di altrui conversazioni in maniera clandestina e non consentita dagli interlocutori[6]. Tutte quelle citate sopra sono considerazioni di carattere generale sulla categoria "intercettazioni", le quali necessitano l'individuazione degli elementi caratteristici di tale strumento di ricerca della prova. Tali elementi, sia sotto il profilo dei presupposti sostanziali che di quelli strettamente informali, delineano un regime particolarmente rigoroso ma giustificato dalle gravi forme di "compressione" dei diritti riconosciuti dalla carta costituzionale. Vista

[5] Cass., sez. un., 24 settembre 2003, Torcasio, in *C.E.D. Cass.*. n. 225465. In questo senso anche: Cass., sez. II, 16 febbraio 1985, Barresi, in *Foro it.,* 1986, II, p. 670; Cass., sez. VI, 19 febbraio 1981, Semitaio, in *CP*, 1982, p. 1529; Cass., sez. V, 6 novembre 1978, Triberti, in *CP*, 1981, p. 510.

[6] G. MARALFA, *Le intercettazioni*, in *Dir. Pen.,* Editore G. Pirapini, 2004, p. 12; F. CAPRIOLI, *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, *Riv. it. dir. e proc. pen.*, 1991, p. 155; A. DALIA e M. FERRAIOLI, *Manuale di diritto processuale penale,* Padova, 2003, p. 511; P. TONINI, *Manuale di procedura penale*, Giuffrè, Padova, 2000, p. 368.

l'invasività di tale strumento occorre quindi che vengano predeterminati gli scopi della misura limitativa[7], che venga fissato un termine massimo di durata di ciascuna operazione intercettiva, al termine della quale, nel caso permangano i motivi idonei a giustificarla, l'autorità giudiziaria dovrà emettere un nuovo provvedimento autorizzativo[8] e che vengano individuati infine i casi e i modi in cui le libertà in gioco possano essere limitate[9].

Per questo motivo, quattro devono ritenersi le caratteristiche peculiari delle intercettazioni:

1 - la captazione deve essere necessariamente clandestina, in relazione al modo con il quale il dialogo si apprende;

2 - la terzietà del captante, ossia deve essere effettuata da un soggetto estraneo rispetto agli autori delle comunicazioni o conversazioni;

3 - la riservatezza del dialogo, rispetto alla volontà dei dialoganti;

4 - la formalizzazione dell'apprensione del contenuto di comunicazioni o conversazioni deve avvenire come conseguenza dell'atto di intercettazione.

Un punto non pacifico rimane quello relativo all'utilizzo di strumenti meccanici di captazione e se possa esso essere un elemento decisivo per qualificare un'intercettazione o meno. L'art. 268, comma 3, c.p.p., laddove individua gli impianti utilizzabili per il compimento delle operazioni intercettive, sembra far pensare che, l'utilizzo di tali strumenti sia collegato in maniera imprescindibile al concetto normativo di

[7] V. GREVI, *Appunti in tema di intercettazioni telefoniche operate dalla polizia giudiziaria*, in *Riv. it. dir. e proc. pen.*, 1967, p. 733.
[8] V. GREVI, *Intercettazioni telefoniche e principi costituzionali*, in *Riv. it. dir. e proc. pen.*, 1971, p. 1079.
[9] P. BARILE e E. CHELI, *Corrispondenza (Libertà di)*, in *Enciclopedia del diritto*, vol. X, Giuffrè, Milano, 1962, p. 749.

intercettazione. D'altro canto, la *ratio* della norma sembra far ritenere del tutto sufficiente un qualsiasi apparato in grado di "fissare" l'evento comunicazione, onde consentirne una prova storica diretta e quindi del tutto slegata dalla capacità di ricostruzione di soggetti terzi[10]. I primi due requisiti, quello della clandestinità e quello della riservatezza, vengono verificati di volta in volta rimanendo in costante rapporto fra di essi. In primo luogo, gli stessi presuppongono che la captazione sia avvenuta servendosi di uno strumento utilizzato dai soggetti intercettati tale da assicurare la riservatezza della trasmissione, sia essa una conversazione o una comunicazione. Tipico strumento è quello telefonico: chi utilizza questo tipo di strumento è infatti propenso a credere che la comunicazione con un soggetto terzo non sia captabile da altri soggetti. L'utilizzo del telefono viene quindi inteso come una volontà inequivoca di "escludere" i terzi, in modo tale da non poter essere ricondotta alla fattispecie di cui all'art. 617, comma 1, c.p.p. (Cognizione, interruzione o impedimento illecito di comunicazioni o conversazioni telegrafiche o telefoniche). Diversa la situazione in cui due soggetti vengano a colloquio ad alta voce in un luogo pubblico o in pubblico locale, situazione in cui si deve ritenere che essi abbiano implicitamente rinunciato alla riservatezza della conversazione[11]. La stessa Cassazione ha ritenuto legittimo l'ascolto casuale di un colloquio ogni qual volta esso si verifichi in conseguenza dell'avere gli interlocutori parlato ad alta voce ovvero senza preoccuparsi di evitare interferenze di terzi[12]. Con riferimento al soggetto attivo dell'intercettazione, la natura dell'istituto implica che l'attività intercettiva sia posta in essere necessariamente da un soggetto estraneo rispetto agli

[10] A favore della prima ipotesi A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, p. 11; G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, op. cit., pp. 37 e ss. A favore della seconda ipotesi P. BRUNO, *Intercettazioni*, op. cit., p. 179; R. D'AJELLO, *Le intercettazioni di conversazioni e comunicazioni,* in *Riv. pen. econ.,* 1990, p. 108.
[11] R. DELL'ANDRO, *Colloqui registrati ad uso probatorio*, in *R. it. d. proc. pen.* 84, pp. 118 ss.
[12] Cass. sez. I, 28 febbraio 1979, Martinet, *C.P.M.A.,* 1982, p. 598.

autori delle comunicazioni o conversazioni, escludendo altresì l'ipotesi secondo la quale sarebbe possibile annoverare tra i possibili autori dell'intercettazione lo stesso destinatario dell'atto comunicativo[13]. L'ultimo requisito è quello della formalizzazione dell'atto e va a concatenarsi con la previsione normativa di cui all'art. 234, comma 1, c.p.p. secondo la quale: «E' consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo». L'articolo sopracitato è compreso nel titolo riguardante i mezzi di prova, laddove l'art. 266 e ss. c.p.p. sono ricompresi nel titolo III, con oggetto i mezzi di ricerca della prova. La differenza tra i due istituti risulta quindi chiara nel momento in cui si presta particolare attenzione al titolo in cui sono inseriti: documenti, sequestri, ispezioni, perquisizioni sono istituti diretti ad inglobare all'interno del procedimento prove che esistono di già al di fuori dello stesso e, presumibilmente, a prescindere da esso, facendo quindi entrare la realtà esterna nel procedimento ed assumendo una valenza probatoria. L' intercettazione, al contrario, è oggetto di un materiale probatorio che non "preesiste" al procedimento e che prende forma solo a seguito di una serie tassativa di atti giurisdizionali. Riportando un esempio spesso utilizzato in dottrina, una bobina riportante la voce di due soggetti potrà dunque assumere una duplice valenza: sarà considerata come un documento nel momento in cui esiste da un momento precedente al procedimento ovvero si è formata a prescindere da quest'ultimo o ancora documenta una conversazione in cui l'autore della registrazione era parte diretta della comunicazione registrata; in tutti gli altri casi sarà invece considerata come un documento formatosi dall'atto di ricerca della prova tramite intercettazione.

Ultima distinzione da farsi in tema di intercettazioni è la suddivisione delle stesse in due sottocategorie, a seconda della loro diversa finalità,

[13] Cass. sez. I, 2 marzo 1999, Cavinato, *Gazz. Giur.,* 1999, n. 29, p. 32.

rispettivamente delle intercettazioni preventive e processuali. Quelle preventive hanno una funzione di pubblica sicurezza, mirando quindi alla prevenzione dei reati (artt. 266 disp. att. e coord. e art. 4 d.l. 27 luglio 2005, n. 144, conv. dalla legge 31 luglio 2005, n. 155). Per quanto riguarda invece le intercettazioni processuali, esse hanno la funzione di consentire lo sviluppo delle indagini (artt. 266-271 c.p.p., per cui non sono ammissibili dopo il rinvio a giudizio[14]) oppure di agevolare le ricerche del latitante (art. 295 comma 3, 3-*bis* e 3-*ter*, c.p.p.).

## 1.1 – Limiti oggettivi e soggettivi

Occorre inoltre analizzare i limiti oggettivi e soggetti a cui soggiacciono le intercettazioni, ossia per quali tipi di reati è concesso utilizzare questo strumento di ricerca della prova e verso quali soggetti[15]. Per quanto riguarda quelli oggettivi, l'intercettazione di comunicazione è infatti consentita quando si tratti di procedimenti riguardanti:

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'art. 4 c.p.p. Questa previsione ha creato alcuni effetti paradossali che ancora oggi si riverberano sul nostro ordinamento, come ad esempio la possibilità di utilizzo dell'intercettazione per il furto aggravato e non per il favoreggiamento personale (art. 378 c.p.) o reale, o, peggio ancora, per il favoreggiamento volto al fine di far conseguire il prezzo della liberazione della vittima agli autori del delitto di sequestro di persona a scopo di estorsione;

[14] GIP Trib. Torino, 25 novembre 2005, *DG*, 2005, 15, 83.
[15] Sul tema dell'inutilizzabilità, diffusamente, si segnala C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.,* 2011, pp. 3653 e ss.

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'art. 4 c.p.p. L'ipotesi di cui sopra risulta tuttavia talmente ampia da generare situazioni al limiti dell'inverosimile. L'intercettazione risulta per esempio pienamente giustificabile per i delitti di peculato (art. 314 c.p.) o di concussione (art. 317 c.p.) mentre è di difficile applicazione per delitti del calibro di millantato credito (art. 346 c.p.). Inoltre, essa risulta inapplicabile per esempio nei procedimenti per i delitti di corruzione per un atto di ufficio (art. 318 c.p.) o istigazione alla corruzione (art. 322 c.p.), ove il ricorso all'intercettazione presenterebbe indubbi vantaggi[16];

c) delitti concernenti sostanze stupefacenti o psicotrope. Seguendo questa ipotesi si assiste ad un abbandono da parte del legislatore del criterio quantitativo in favore di quello qualitativo, determinato cioè dalle particolari caratteristiche di taluni reati. In questo modo, per le ipotesi di cui alla lettera in esame, l'intercettazione risulta ammessa anche per i fatti di lieve entità, magari riguardanti droghe c.d. leggere;

d) delitti riguardanti le armi e le sostanze esplosive. Anche in questo caso si assiste ad un'assoluta genericità della locuzione normativa, consentendo un'ampia libertà di intercettazione in relazione a questa fattispecie;

e) delitti di contrabbando. Di nuovo, la previsione risulta talmente lata da includere qualsiasi ipotesi di contrabbando reperibile nelle leggi in materia;

f) reati, includendo quindi anche le contravvenzioni, di ingiuria, minaccia, usura, abusiva intermediazione finanziaria, molestia o disturbo alle persone col mezzo del telefono. In questo caso il problema interpretativo che si pone è di più ampia portata. Innanzitutto, in riferimento alla molestia o disturbo col mezzo del telefono, si potrebbe obiettare una certa

[16] L. FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997, p. 81.

superfluità in quanto la prova del fatto può essere fornita dalla testimonianza della persona offesa, alla quale è consentito documentare anche con la registrazione, personalmente effettuata, il contenuto delle telefonate. Inoltre si pone un dubbio circa un'interpretazione restrittiva o estensiva della norma per i reati di ingiuria, minaccia, molestia o disturbo delle persone col mezzo del telefono. Non è chiaro infatti se il legislatore li intenda come reati di cui agli art. 594, 612 e 660 c.p. o se si riferisca a quelli in cui l'ingiuria o la minaccia sono elementi costitutivi. Infine, il punto più critico dell'ipotesi in questione è la modalità della commissione di suddetti reati, ossia tramite l'utilizzo del telefono, locuzione che limita fortemente quindi l'intercettazione;

f *bis*) delitti previsti dall'art. 600 ter, comma 3, c.p. (fattispecie in tema di pornografia minorile)[17].

Per quanto riguarda i limiti soggettivi invece, sono presenti diversi soggetti che possono essere classificati come soggetti passivi di un'intercettazione:

a) terzi estranei. Spesso ci si è chiesto se è possibile sottoporre ad intercettazione anche chi è estraneo all'indagine e la risposta positiva è quella che risulta più convincente. Essa può essere spiegata pensando ad esempio all'utilità di un'intercettazione disposta sull'utenza dei familiari del sequestrato a scopo di estorsione in modo da poter acquisire notizie circa le eventuali trattative per il pagamento del riscatto o ancora, all'ipotesi in cui si possiedano gravi indizi per ritenere che qualcuno sia sottoposto a richieste estorsive che non ha voluto denunciare. La stessa giurisprudenza ha messo in luce inoltre, che è lo stesso art. 267, comma 1, c.p.p. ad autorizzare l'intercettazione sull'utenza di un terzo, richiedendo solo

[17] C. DI MARTINO e T. PROCACCIANTI, *Le intercettazioni telefoniche*, in *Enciclopedia*, di P. Cendon, CEDAM, 2001, pp. 38 e ss.

«gravi indizi di reato», non di colpevolezza[18]. La situazione oggi è tuttavia mutata in quanto il vigente codice di procedura penale contiene un principio-guida nell'assunzione delle prove, ossia il principio di pertinenza, riscontrabile nell'art. 187 c.p.p., la cui rigorosa applicazione nel caso di specie richiede che debba essere provato uno specifico collegamento con l'indiziato;

b) coimputati e prossimi congiunti. Non sembrano sussistere validi motivi per i quali escludere che l'intercettazione possa essere disposta anche nei confronti di soggetti il cui contributo conoscitivo sarebbe inutilizzabile se acquisito sotto forma di testimonianza. Si fa riferimento in particolare ai coimputati nello stesso reato o in un reato connesso (art. 197 c.p.p.) ed ai prossimi congiunti od al convivente dell'imputato (art. 199 c.p.p.). La *ratio* delle due ipotesi è la stessa, in quanto si vuole evitare che il soggetto chiamato a deporre sia posto nell'alternativa di mentire o di nuocere a sé stesso o al prossimo congiunto, tuttavia fa riferimento alla sola prova testimoniale e per questo non risulta applicabile nel campo delle intercettazioni;

c) titolari di segreti. In questo caso si fa riferimento alla categoria degli «altri professionisti» indicati nell'art. 200 c.p.p. e ai potenziali depositari di segreti d'ufficio e di Stato. Per quanto riguarda i primi, l'art. 271 c.p.p. pone un divieto riguardante l'acquisizione di notizie e non si estende al compimento dell'atto; mentre, in relazione ai secondi, non sussiste sulla carta nemmeno il divieto di acquisizione di notizie;

d) Presidente della Repubblica. Esso gode di un'immunità assoluta dalle intercettazioni, salvo il caso in cui la Corte Costituzionale non ne abbia disposto la sospensione dalla carica per alto tradimento o attentato alla Costituzione;

[18] Cass. sez. I, 16 gennaio 1995, Catti ed altri, *GP*, 1996, III, 226.

e) membri del Parlamento. Dopo la modifica dell'art. 68 Cost., l'autorizzazione a procedere non è più necessaria contro un membro del Parlamento, rimane tuttavia necessaria la suddetta richiesta nel momento in cui si tratti di disporre un'intercettazione telefonica, salvo i casi in cui il parlamentare sia colto nella flagranza di un delitto per il quale l'arresto è obbligatorio, così come stabilito dall'art. 380 c.p.p.;

f) Presidente del Consiglio, ministri ed altri inquisiti che siano anche parlamentari. Solo all'interno di un procedimento per i reati di cui all'art. 96 Cost. essi possono essere sottoposti ad intercettazione telefonica, salvo i casi in cui siano colti nell'atto di commettere uno dei delitti indicati dall'art. 343, comma 3, seconda parte, c.p.p.;

g) Giudici della Corte Costituzionale. La stessa autorizzazione prevista per i parlamentari dall'art. 68, comma 2, Cost. è richiesta anche per questi soggetti, finché sono in carica.

## 1.2 – Le intercettazioni "tra i presenti" o c.d. "ambientali"

Le intercettazioni "tra i presenti", più note con la formula "intercettazioni ambientali", sono rimaste estranee al codice e alle leggi speciali fino al d.l. 8 giugno 1992, n. 306 (convertito con modifiche dalla l. 7 agosto 1992, n. 356), che all'art. 3-*bis* ne fa per la prima volta menzione. Il codice del 1988 infatti ha optato per l'introduzione dell'istituto affiancando alle intercettazioni telefoniche quelle di comunicazioni tra presenti, tuttavia ponendo un limite ben preciso. In tutte le ipotesi elencate dal primo comma dell'art. 266 c.p.p., il secondo comma della stessa norma consente anche l'intercettazione tra presenti, puntualizzando tuttavia che qualora

queste comunicazioni avvengano nei luoghi indicati dall'art. 614 c.p. (Violazione di domicilio), l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa, bilanciando così la particolare insidiosità del mezzo di ricerca della prova con le esigenze di *privacy* e di inviolabilità del domicilio della persona[19].

Questo particolare tipo di intercettazione è riferito quindi a dialoghi captati tra persone simultaneamente presenti nello stesso luogo, non richiedendo l'ausilio di strumenti tecnici per la trasmissione del suono[20]. Anche per questo tipo di colloqui la protezione accordata dagli artt. 266-271 c.p.p. scatta soltanto nel momento in cui il discorso sia riservato[21]. Tale forma di intercettazione è completamente diversa da quella telefonica, in quanto essa avviene non servendosi di un particolare mezzo di diffusione del segnale, quale ad es. il telefono, ma tra persone che si trovano in uno stesso ambiente, generalmente l'una al cospetto dell'altra. Subentrano quindi diversi aspetti, tipici delle modalità esecutive delle intercettazioni *inter praesentes*, che celano profili ambigui e di discrezionalità troppo accentuata in capo al Pubblico Ministero o alla polizia giudiziaria[22]. Le modalità esecutive alle quali si faceva riferimento poc'anzi sono molteplici: in primo luogo, mediante l'introduzione e la permanenza nei luoghi indicati dall'art. 614 c.p. di operatori, dotati di opportuna strumentazione captativa, che celano la propria presenza agli intercettati; ed ancora,

---

[19] Una disciplina derogatrice di quella prevista dall'art. 266 c.p.p. è stata introdotta, in relazione ai delitti di criminalità organizzata, dall'art. 13 d.l. 13 maggio 1991, n. 152, recante provvedimenti urgenti in tema di lotta alla criminalità organizzata, convertito, con modifiche, nella legge 12 luglio 1991, n. 203 e da ultimo dall'art. 23, legge 1 marzo 2001, n. 63.

[20] Vedasi per tutti G. SPANGHER, *La disciplina italiana delle intercettazioni di comunicazioni o conversazioni*, *AP*, 1994, 3-15, 5.

[21] F. RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Giuffrè, 2001, p. 74.

[22] A tal proposito vedasi P. FERRUA, *Studi sul processo penale*, vol. III, Torino, 1997, p. 121, il quale rileva che il decreto di autorizzazione ambientale non possa, ad esempio, autorizzare l'intrusione domiciliare per predisporre strumenti di ascolto.

mediante la partecipazione diretta alla conversazione di operatori che portino indosso, opportunamente camuffati, strumenti intercettivi; infine, e forse è lo scenario che si verifica con più frequenza, il posizionamento nell'ambiente di dispositivi chiamati più comunemente microspie o "cimici", occultati e collegati ad apparati di ricezione e registrazione esterni.

Le modalità sopra evidenziate comportano quindi una palese e profonda intromissione all'interno della vita privata del soggetto sottoposto ad intercettazione, anche qualora il soggetto sia all'interno del suo domicilio. Il legislatore ha voluto bilanciare questo squilibrio stabilendo che, qualora l'intercettazione venga svolta in uno dei luoghi indicati nell'art. 614 c.p., debba anche sussistere il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa. A tal proposito, la dottrina ha obiettato a gran voce, dichiarando che «non è chiaro per quale motivo si debbano disegnare dei confini "territoriali" di maggiore o minore tutelabilità del diritto alla segretezza delle comunicazioni: il dialogo riservato è tale a prescindere dal luogo in cui avviene, e dovunque si svolga, esso merita la medesima tutela. Anche ad ammettere poi che la comunicazione "domestica" vada maggiormente protetta, resta da chiedersi perché mai il legislatore ne abbia ritenuto sacrificabile la segretezza in ragione del fatto che nel domicilio si svolga anche l'attività criminosa e non, ad esempio, in considerazione della particolare gravità del reato per cui si procede[23]». Tuttavia, tutte queste prese di posizione da parte della dottrina, corrono il rischio di rimanere lettera morta nel momento in cui si presta attenzione al 2° comma dell'art. 266 c.p.p. Il legislatore pone infatti l'accento non sull'attività criminosa in corso di svolgimento, accantonando così tutte le autorevoli opinioni dottrinali che basavano sulla flagranza di reato

[23] F. CAPRIOLI, *Intercettazione e registrazione*, op. cit., in *Riv. it. dir. e proc. pen.*, 1991, p. 172.

l'elemento essenziale del comma in questione[24], ma bensì sul «fondato motivo di ritenere che..». Esso dunque, non postula che detta attività risulti, poi, essere stata effettivamente realizzata, ma che se ne possa ragionevolmente ritenere la sussistenza con giudizio *ex-ante*, all'atto dell'emanazione del provvedimento di autorizzazione all'effettuazione delle operazioni di intercettazione[25]. In parole povere, l'utilizzabilità delle prove raccolte dipende tutta dalla motivazione del provvedimento autorizzativo e dal modo in cui vengono spiegati gli indizi sulla flagranza di reato[26]. Assume quindi la veste di ruolo chiave la motivazione utilizzata dal p.m. in relazione all'uso di apparecchiature non situate presso la procura della Repubblica. Come specificato infatti dall'art. 268, comma 3, c.p.p.: «Le operazioni possono essere compiute esclusivamente per mezzo degli impianti installati nella procura della Repubblica. Tuttavia, quando tali impianti risultano insufficienti o inidonei ed esistono eccezionali ragioni d'urgenza, il p.m. può disporre, con provvedimento motivato, il compimento delle operazioni mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria». Tuttavia sorgeva un problema di ordine puramente psicologico, in quanto l'intercettazione tra presenti risulta ontologicamente improponibile da una postazione distante dal luogo di captazione, quale quella della procura della Repubblica territorialmente competente. Per detta ragione, molte volte il p.m. sembrava dare per "scontato" il fatto che tali forme di intercettazione devono avvenire per forza in locali diversi da quelli "tradizionali". La Suprema Corte ha tuttavia sciolto qualsivoglia dubbio in merito a tale comportamento discostandosi ampiamente da tale teoria e precisando che, in base al fatto che l'art. 268, comma 2, c.p.p. fa esplicito riferimento alle "comunicazioni tra i presenti" assimilandole in toto a quelle telefoniche e altre forme di

[24] In particolare A. GIARDA, *Sub artt. 266-267*, in *Codice di procedura penale. Commentario* a cura di A. Giarda, vol. II, IPSOA, Milano, pp. 11-19.
[25] Cass. sez. VI, 16 febbraio 1999, Stellino ed altri, *Gdir*, 1999, fasc. 17, p. 87. In termini analoghi Cass. sez. I, 12 dicembre 1994, Manzi, *ANPP*, 1995, p. 710.
[26] A. CAMON, *Le intercettazioni*, op. cit., pp. 185 e ss.

telecomunicazione, si rende così necessario il provvedimento motivato da parte del Pubblico Ministero[27]. Sussisterebbe quindi in capo al p.m. un obbligo di motivazione in qualsiasi caso, anche se, quasi a voler attenuare le conseguenze estremamente gravi di tale mancanza, lo stesso potrebbe essere adempiuto in un momento successivo; la Suprema Corte ha infatti precisato che la mancanza di tale motivazione comporterebbe, ai sensi dell'art. 271 c.p.p., la semplice inutilizzabilità delle intercettazioni compiute; pertanto, un provvedimento integrativo da parte del Pubblico del Ministero, purché anteriore all'utilizzazione delle risultanze delle operazioni intercettive, può essere ammesso, in modo da consentire il controllo da parte del Giudice[28]. Si deve tuttavia segnalare che in epoca più recente rispetto al sopradescritto orientamento, le Sezioni Unite Penali hanno dichiarato l'inutilizzabilità delle intercettazioni effettuate fuori dagli impianti di ascolto delle Procure senza l'autorizzazione del p.m. che giustifichi tali modalità, indicando come necessario il provvedimento motivato da parte dello stesso, in quanto tali intercettazioni comportano un sacrificio molto più intenso ed ampio dei diritti tutelati dall'art. 15 Cost. Particolare rilevanza assumono quindi i requisiti di "urgenza" e "necessità" previsti in via generale e il loro rispetto da parte degli agenti investigativi[29].

## 1.3 – Il nuovo articolo 266-*bis* c.p.p.

La rilevanza del progresso tecnologico e del fenomeno informatico è stata sottolineata dal legislatore con l'introduzione delle nuove fattispecie previste dalla l. 23 dicembre 1993, n. 547 – c.d. *computer's crimes* -, che reca modifiche nella disciplina delle intercettazioni, tramite un

[27] Cass. sez. I, 26 febbraio 2000, Delle Grottaglie, *C.E.D. Cass.*, n. 216282.
[28] Cass. sez. IV, 9 febbraio 2000, Arizi, *C.E.D. Cass.*, n. 215658.
[29] Cass. sez. un., 28 novembre 2001, Policastro ed altri, *GDir*, 48/2001, 74.

adeguamento sia sostanziale che procedurale. L'interpretazione sistematica degli artt. 266 e 266-*bis*, c.p.p., induce a pensare che il legislatore abbia voluto riservare l'intercettazione informatica ai soli reati introdotti con la legge sopra citata, oltre a quelli di cui all'art. 266[30], c.p.p. Tale bisogno sorge dalla semplice constatazione che le organizzazioni criminali mostrano un crescente interesse verso strumenti di comunicazione che consentano, allo stesso tempo, rapidità ed efficacia di collegamenti geografici e sicurezza delle conversazioni, inducendo il legislatore ad introdurre tramite la soprarichiamata legge le intercettazioni c.d. informatiche o di «di comunicazioni informatiche o telematiche», come qualificate dall'art. 266-*bis* c.p.p.[31] Il citato articolo consente quindi l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi. Il concetto stesso di sistema informatico è stato oggetto di una pronuncia da parte della Suprema Corte, nella quale è stata riconosciuta tale natura alla rete telefonica fissa sia per le modalità di trasmissione del flussi di conversazione sia per l'utilizzazione delle linee per il flusso dei c.d. "dati esterni alle conversazioni". Secondo tale pronuncia, deve ritenersi un sistema informatico «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 un'attività di "codificazione" e di "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni",

[30] In questo senso L. FILIPPI, *L'intercettazione*, op. cit., Milano, 1997, p. 82; per l'interpretazione più ampia vedasi invece G. FUMU, *Sub. art. 266-bis*, in *Commentario Chiavario*, ed. III agg., 1997, p. 131.

[31] G. BUONOMO, *Metodologia e disciplina delle indagini informatiche*, in R. Borruso, G. Buonomo, G. Corasaniti e G. D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pp. 135 e ss.

costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature che sfruttano tali tecnologie costituisce giudizio di fatto insindacabile in Cassazione ove sorretto da motivazione adeguata ed immune ad errori logici[32]». Il sistema telematico invece, è caratterizzato dal fatto che gli elaboratori non sono collegati tra loro da un cavo di connessione, ma utilizzano cavi telefonici e modulatori di toni oppure ancora satelliti artificiali. Ciò che distingue quindi il sistema informatico dal sistema telematico è soltanto il metodo utilizzato per la trasmissione dei dati a distanza[33]. Il principale problema con la fattispecie disciplinata dal nuovo art. 266-*bis* c.p.p. risulta essere l'ampiezza di tale disposizione, tale da ricomprendere non solo le previsioni dettate dall'art. 266 c.p.p. ma anche qualsiasi altro tipo di reato purché commesso tramite l'utilizzo di strumenti informatici. L'autorevole dottrina si è quindi divisa in due filoni: da un lato l'interpretazione restrittiva è sostenuta da quanti ritengono che la tassatività delle ipotesi in cui sono ammesse le intercettazioni non può venire meno solo per un certo tipo di esse e che, per assicurare alla giustizia autori di determinati reati – realizzabili esclusivamente tramite l'uso di strumenti informatici – è necessaria la violazione della *privacy* via computer, poiché le normali intercettazioni non sarebbero utili a tal fine[34]; dall'altro lato invece c'è chi sostiene che l'art. 266-*bis*, c.p.p., ha una portata più ampia di quella che se ne può desumere a prima vista, poiché si limita ad esigere che l'uso di tecnologie informatiche non sia l'elemento costitutivo del reato bensì che esso sia commesso con l'utilizzo di tali strumenti. Secondo questa seconda ipotesi interpretativa dunque, nella

[32] Cass. sez. VI, 14 dicembre 1999, Piersanti, *C.E.D. Cass.*, n. 214945.
[33] C. DI MARTINO e T. PROCACCIANTI, *Le intercettazioni telefoniche*, op. cit., p. 44.
[34] In questo senso vedasi L. FILIPPI, *L'intercettazione*, op. cit., pp. 82 e ss; L. UGOCCIONI, *Sub art. 11 L. 23/12/1993 N. 547 (Criminalità informatica), LP,* 1996, pp. 142 e ss.

previsione normativa rientrerebbero sia i delitti che sono necessariamente posti in essere con l'utilizzo di un computer sia quelli per i quali l'autore si sia servito di tali tecnologie, informatiche o telematiche, anche solo occasionalmente[35]. Tale ultima teoria deve però ritenersi maggiormente condivisibile in quanto tramite la stessa, viene in effetti riconosciuto il diritto per gli organi preposti all'accertamento e alla repressione di reati di lottare tecnicamente alla pari con qualsivoglia forma di attività criminosa. La mancata precisazione dell'ampiezza della norma in sede giurisprudenziale permette, allo stato attuale, di ipotizzare un uso estremamente estensivo dell'atto di ricerca della prova fornito dall'art. 266-*bis* c.p.p. Va tuttavia sottolineato che, alla luce dell'art. 266 c.p.p. e della sua formulazione, una semplice interpretazione estensiva dello stesso avrebbe consentito l'intercettazione di tutte le conversazioni telematiche, ivi comprese anche quelle annoverate dal nuovo art. 266-*bis* c.p.p., semplicemente prendendo in considerazione la definizione di comunicazione come un qualsiasi scambio di dati, informazioni, immagini o suoni che intercorre tra due o più soggetti. Risulta tuttavia di fondamentale importanza la nuova previsione codicistica nel momento in cui si affronta il tema delle intercettazioni puramente "informatiche", ossia le intercettazioni aventi ad oggetto più computer in grado di interagire tra loro senza utilizzare lo strumento telefonico, rendendo tali intercettazioni non esperibili alla luce dell'art. 266 c.p.p. Nel dettato della norma infatti, quando si legge «altre forme di comunicazione», essa fa riferimento alle comunicazioni tra elaboratori elettronici che avvengono utilizzando la linea telefonica con l'utilizzo di un *modem*, ma non anche alle comunicazioni tra elaboratori elettronici che avvengono all'interno di una *LAN* (*Local Area Network*) o con qualsiasi altro mezzo diverso da quello telefonico (p. es. via *telefax*). Essendo tale norma insuscettibile di interpretazione estensiva perché soggetta alla riserva di legge di cui all'art. 15 Costituzione, ove il

[35] Tra i sostenitori della teoria estensiva vedasi A. CAMON, *Le intercettazioni*, op. cit., p. 67.

legislatore non avesse fatto richiamo espresso ai reati indicati nell'art. 266 c.p.p. all'interno del nuovo art. 266-*bis* c.p.p. tali intercettazioni sarebbero risultate irrealizzabili. L'ultimo dubbio fugato dal legislatore con la modifica dell'art 623-*bis* c.p. (Altre comunicazioni e conversazioni) era quello legato alla necessità dell'effettiva presenza di persone fisiche e non solamente di elaboratori per poter qualificare una conversazione fra persone come tale. Il legislatore, modificando il sopracitato articolo ha inserito espressamente tra le forme di comunicazione quelle informatiche o telematiche[36]. Da ciò deriva la c.d. indagine informatica, cioè quella tesa non solo all'identificazione dell'autore di crimini informatici, ma anche quando si utilizzano determinate tecnologie informatiche e telematiche nello svolgimento di indagini relative a reati comuni[37] (ad esempio, l'intercettazione telematica operata sulle comunicazioni avvenute da uno spacciatore di sostanze stupefacenti).

Oggetto delle intercettazioni saranno quindi connessioni – fisse o occasionali – tra sistemi informatici o telematici, ossia tra computer collegati o in rete o via *modem* o tramite qualsiasi altra forma. Sotto il profilo prettamente esecutivo l'intercettazione potrà essere effettuata in diversi modi:

- deviando su un computer le comunicazioni intercettate, memorizzando quindi tali dati prima della ritrasmissione;

- inoltrando sul computer un "registro" in grado di memorizzare gli inserimenti e/o alterazioni dei dati contenuti sul dispositivo;

- registrando su un apposito supporto, nel caso di intercettazioni telematiche, i flussi, dopo aver provveduto ad attivare una linea telefonica

[36] C. SARZANA di S. e C. IPPOLITO, *Informatica e diritto penale*, Giuffrè, Milano, 1994, p. 224.
[37] M. IASELLI, *Nuove tecnologie per nuove tecniche investigative, ma a rischio privacy*. *Dalle indagini sul caso D'Antona un esempio da seguire*, in *DGius,* 2003, 43, pp. 91 e ss.

appositamente fornita di *modem* per captare le informazioni[38].

Le modalità operative possono inoltre essere condizionate da scelte di tipo meramente "funzionale", legate quindi alle esigenze investigative. In primo luogo si può intercettare l'intero flusso dei dati dell'utente, ipotesi suggeribile nel momento in cui le indagini siano destinate a soggetti o situazioni che non consentono di perdere alcuna informazione sull'attività dei soggetti. In secondo luogo potrebbe rendersi necessaria l'intercettazione della sola posta via web o del *server* di posta del *provider* italiano, conosciuta anche come intercettazione a "costo zero" ed effettuata tramite un *forward*, ossia un inoltro, dalla casella postale*/mail-web* del *provider* sulla casella di posta della polizia giudiziaria delegata. Si utilizza questo metodo nel momento in cui l'indagine afferisce a comunicazioni che avvengono principalmente via posta, come ad es. ingiurie o minacce. In ultimo luogo, potrebbe rendersi necessaria l'intercettazione della sola posta via *web* su *server* estero o su *server* diverso dal *provider* che consente l'accesso ad internet. In quest'ultimo caso, l'unica soluzione utilizzabile è quella di intercettare tutto il flusso di dati dell'utente, in quanto l'utente medio utilizza più connessioni ad internet e quindi generalmente gestisce le proprie caselle postali, spesso anche più di una, presso altri *provider*, italiani ed esteri.

# 2 – Libertà e segretezza delle comunicazioni

Le intercettazioni di comunicazioni o conversazioni, così come analizzate e descritte nei paragrafi precedenti, costituiscono senza ombra di dubbio uno dei mezzi più pericolosi nelle mani degli inquirenti, in quanto consentono l'acquisizione di prove alla totale insaputa dell'interessato e del suo interlocutore. Sono presenti tuttavia delle garanzie costituzionali

[38] G. BUONOMO, *Profili penali*, op. cit., p. 155.

che tutelano l'interessato da questa potente forma di invasione della sfera privata. Il riferimento non può che andare all'art. 15 della Costituzione, ai sensi del quale la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. Il Costituente, dopo aver proclamato ciò nel comma 1 di suddetto articolo, afferma nel comma 2, che la loro limitazione può avvenire solo per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge. La seguente previsione trova riscontro innanzitutto nel diritto internazionale pattizio, avendo da tempo la disciplina assunto l'arduo compito di proclamare e diffondere il rispetto dei diritti umani, a cominciare dagli aspetti di tutela connessi, come in questo caso, alla libertà personale, domiciliare e di comunicazione. Diversi sono i riferimenti al diritto internazionale, primo fra tutti l'art. 12 della Dichiarazione universale dei diritti dell'uomo del 1948, secondo il quale nessun individuo può essere sottoposto ad interferenze arbitrarie nella sfera della propria vita privata. L'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, attuata con la legge 4 agosto 1955, n. 848, attribuisce poi ad ogni persona il diritto al rispetto della sua vita privata e familiare, del domicilio e della corrispondenza[39].

La sopra citata libertà di comunicazione tutela una pluralità di soggetti: innanzitutto essa spetta a tutti gli individui, siano essi cittadini stranieri o apolidi o anche minori di età purché muniti di capacità naturale; in secondo luogo ai soggetti collettivi privati, muniti o meno di personalità

[39] La giurisprudenza della Corte europea ha enucleato tuttavia i principi a cui deve attenersi la normativa nazionale nel momento in cui pone delle limitazioni a tali diritti. In particolare, è stato affermato il principio per cui la limitazione del diritto previsto all'art. 8 «deve essere predeterminata da regole di diritto, siano esse di fonte legislativa o di creazione giurisprudenziale, chiare e precise in modo da rendere ogni interferenza ragionevolmente prevedibile, dovendo sussistere adeguate garanzie contro l'abuso di potere dell'autorità pubblica». Così, Commissione Europea dei diritti dell'uomo, *caso Silver e più*, 11 ottobre 1980, in *Publications of the European Court of Human Rights*, serie B, vol. 51, 1987, p. 73.

giuridica. La norma infine garantisce tanto il mittente quanto il destinatario della comunicazione, tutelando la libertà e la segretezza non solo dell'inviare ma anche del ricevere un determinato messaggio[40]. L'oggetto della tutela invece deve essere ricercato all'interno della stessa nozione di comunicazione e risulta quindi necessario un ulteriore chiarimento in merito ai termini "libertà" e "segretezza" citati dall'art. 15 Cost. Ciò che colpisce di queste due locuzioni è che esse rappresentano un'endiadi, ossia non può dirsi di aversi effettiva libertà di comunicazione se non è garantita la sicurezza, tuttavia presentano due profili distinti, dal momento che limitazioni della libertà possono non tradursi in interferenze sulla segretezza (così ad es. per il c.d. fermo della corrispondenza); al contempo però possono profilarsi violazioni, opportunamente sanzionate all'interno dell'ordinamento, che incidono sull'uno o sull'altro profilo ( ad es. l'art. 616 c.p. punisce senza distinzione tanto la distruzione della corrispondenza quanto la rivelazione dei contenuti della stessa). Entrambe si riferiscono alla corrispondenza e a ogni altra forma di comunicazione[41], in quanto libero è l'atto comunicativo che non subisca indebite coercizioni o restrizioni, da parte sia di privati che di pubblici poteri, mentre la segretezza attiene al contenuto delle conversazioni riservate che, in quanto tali, sono arbitrariamente sottratte alla conoscibilità da parte di terzi. La stessa giurisprudenza costituzionale ha costantemente riconosciuto, a partire dalla sentenza n. 34 del 1937[42], che «la libertà e la segretezza della corrispondenza e di ogni altro mezzo di comunicazione costituiscono un diritto dell'individuo rientrante tra i valori supremi costituzionali, tanto da essere espressamente qualificato dall'art. 15 Cost. come diritto inviolabile».

---

[40] C. MORTATI, *Istituzioni di diritto pubblico*, vol. 2, CEDAM, 1976, p. 1062.
[41] G. DI STASI, *La tutela costituzionale della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione,* in *Riv. amm. R.I.,* 1994, p. 1129.
[42] C. cost., sent. n. 34 del 6 aprile 1973, in *Giur. cost.,* 1973, p. 330.

A tutela dell'inviolabilità della libertà e della segretezza delle comunicazioni la Costituzione pone dunque una duplice riserva, sia di legge che di giurisdizione, demandando al legislatore ordinario la determinazione delle «garanzie» che consentono limitazioni dei diritti elencati nel dettato costituzionale e al provvedimento motivato da parte dell'autorità giudiziaria la disposizione delle suddette restrizioni. Per quanto riguarda il primo aspetto, ossia la riserva di legge, si ritiene che essa sia una riserva di legge assoluta, escludendo quindi l'intervento di fonti secondarie e demandando al legislatore la disciplina relativa alla materia in questione. In relazione invece alla riserva di giurisdizione, la garanzia risulta quindi duplice: da un lato la Costituzione riserva alla sola autorità giudiziaria il potere di limitare la libertà e la segretezza, mentre dall'altro lato richiede necessariamente un provvedimento motivato che giustifichi tale limitazione, in modo tale da assicurarne il controllo giurisdizionale nei vari gradi di giudizio. Se ne può ricavare quindi una sorta di presunzione assoluta di illegittimità delle misure che incidono sulla segretezza e sulla libertà ma che non prevedono il previo coinvolgimento dell'autorità giudiziaria. L'art. 15 Cost. esprime quindi una situazione tipica di inviolabilità da interferenze e non un diritto alla tutela, in particolare la prima situazione ha una valenza prettamente negativa rispetto alle intrusioni, esemplificandosi in una «libertà da…», mentre l'altra situazione si configura con una valenza positiva, qualificandosi come «diritto di…». Pertanto risulta chiaro che la norma costituzionale non riserva alla legge di fissare l'intensità e la dimensione dell'intangibilità di tali libertà, ma piuttosto di consenteirne una limitazione, nei casi e nei modi stabiliti dalla legge[43].

Tutto ciò fa si che occorrano una serie di garanzie specifiche ed ulteriori, in modo tale da garantire un ragionevole bilanciamento delle esigenze

[43] Cass. sez. un., 24 settembre 1998, n. 21, in *Arch. n. proc. pen.,* 1998, n.4, p. 539.

confliggenti sul tema. Nel tentativo di instaurare e mantenere tale difficile equilibrio, la Corte Costituzionale si è costantemente pronunciata[44] - con interventi di *self restraint* – indicando quali profili di tutela devono essere in qualsiasi caso curati[45]:

a) innanzitutto la necessità di procedere ad un bilanciamento dei due interessi costituzionali contrapposti, da un lato la segretezza delle comunicazioni e dall'altro l'esigenza della repressione penale, in modo da evitare che il diritto alla segretezza risulti oltremodo sacrificato;

b) la sussistenza di concrete e gravi esigenze di giustizia;

c) la sussistenza di fondati motivi per ritenere che il mezzo di ricerca della prova consenta di conseguire dei risultati utili ai fini investigativi;

d) la predeterminazione della «durata» per la quale si impone la limitazione della segretezza;

e) un controllo sulla legittimità del provvedimento di autorizzazione che limita il diritto alla segretezza;

f) la segretezza delle risultanze dell'atto;

g) l'utilizzazione limitata al solo materiale rilevante per l'imputazione di cui si discute;

h) la presenza di garanzie interconnesse all'identificazione dei soggetti partecipanti alla conversazione, oltre che del tempo e del luogo della stessa;

i) l'invalicabilità degli attuali limiti all'utilizzazione degli esiti delle intercettazioni in procedimenti diversi, fissati dall'art. 270 c.p.p.

[44] Vedasi, fra le principali, C. cost. 23 luglio 1991, n. 366; C. cost., 11 marzo 1993, n. 81; C. cost., 24 febbraio 1994, n. 63.
[45] P. BALDUCCI, *Le garanzie*, op. cit., p. 40.

(utilizzazione in altri procedimenti).

Le sopra indicate garanzie rientrano quindi tra quelle che devono essere doverosamente presenti e rispettate, in quanto deducibili dalla norma costituzionale in esame e a cui, in qualsiasi modo si intenda disciplinare le intercettazioni di comunicazioni, non si può in alcun caso rinunciare o derogare, pena l'illegittimità delle relative disposizioni. Inoltre, risulterebbe incongruo non prevedere «casi e modi» per la libertà di comunicazione, previsti per esempio dall'art. 13 Cost., nonché quella garanzia di sindacabilità che risulta già assicurata per i provvedimenti restrittivi della libertà personale dall'art. 111 Cost.[46]. Se si ritenesse altrimenti, «si avrebbe una sorta di rinvio in bianco alla potestà del giudice, le cui decisioni sarebbero praticamente incontrollabili[47]». In questo senso, la limitazione della libertà di comunicazione deve risultare strettamente necessaria al raggiungimento nonché al soddisfacimento dell'interesse concorrente, in questo caso l'amministrazione della giustizia, e l'atto della Autorità giudiziaria deve risultare sorretto da adeguata e specifica motivazione, in modo da dimostrare in maniera efficace la sussistenza in concreto e non puramente in termini astratti di esigenze istruttorie[48]. Con particolare riferimento alle intercettazioni telefoniche infine, in applicazione delle delucidazioni sopravvenute dal giudice costituzionale, si è affermato che ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche conservati in appositi archivi informatici dei gestori telefonici, sia sufficiente il decreto motivato emanato dal p.m., non essendo necessaria, considerata la diversa intrusione nella sfera di riservatezza del soggetto, l'osservanza delle disposizioni relative alle intercettazioni di comunicazioni

[46] A. PACE, *Commento all'art. 15 Cost.*, in *Commentario della Costituzione*, di G. Branca, Zanichelli, Bologna, 1977, p. 107.
[47] G. ILLUMINATI, *La disciplina*, op. cit., p. 7.
[48] S. BARTOLE, R. BIN, V. CRISAFULLI e L. PALADIN, *Commentario breve alla Costituzione*, in *Breviaria Iuris*, di G. Cian e A. Trabucchi, seconda edizione, CEDAM, 2008, p. 124.

e o conversazioni di cui agli art. 266ss c.p.p. Il controllo giurisdizionale sul provvedimento di acquisizione di tali dati, che attiene quindi ad un mezzo di ricerca della prova, risulta attuabile mediante la rilevabilità, anche d'ufficio, in ogni stato e grado del procedimento, dell'eventuale inutilizzabilità, essendo l'art. 191 c.p.p. applicabile anche alle c.d. prove "incostituzionali" perché assunte con modalità lesive dei diritti fondamentali[49].

# 3 – La tutela del domicilio

Uno dei principali problemi sorti nell'applicazione della normativa relativa alle intercettazioni di comunicazioni tra presenti è quello della esatta definizione di privata dimora. Nelle trattazioni dottrinali infatti, così come anche nelle pronunce giurisprudenziali, aventi ad oggetto il tema delle intercettazioni, l'analisi dei profili costituzionali non può discostarsi innanzitutto dall'art. 15 Cost., disposizione cardine dell'argomento ed ampiamente trattata nel paragrafo precedente, e dall'art. 14 Cost. che, preordinato a garantire l'inviolabilità del domicilio da intrusioni indebite, merita sicuramente una menzione particolare nel momento in cui si passano in rassegna le operazioni che interferiscono con il libero godimento di questo spazio costituzionalmente tutelato. In particolare, il dettato dell'art. 14 Cost. stabilisce che il domicilio è inviolabile e non vi si possono eseguire ispezioni, perquisizioni o sequestri, se non nei casi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. La disposizione in esame assume notevole importanza ogniqualvolta ci si voglia confrontare con istituti o modalità investigative che richiedano una intrusione *invito domino*, sia essa coattiva o clandestina, nei luoghi che rappresentano la proiezione spaziale della

[49] Cass. sez. un., 8 maggio 2000, D'Amurri, *C.E.D. Cass.*, n. 215841; Cass. sez. un., 30 giugno 2000, Tammaro, *C.E.D. Cass.*, n. 216247.

persona, nonché uno dei presupposti per l'esplicazione della vita privata del soggetto[50]. Oltre alle limitazioni espressamente citate nel dettato della norma, si può riferimento alle intercettazioni ai sensi dell'art. 266, comma 2, c.p.p., nonché a taluni mezzi atipici, quali possono essere le videoriprese eseguite in luoghi di privata dimora o il rilevamento tramite *global positioning system* (*GPS*), laddove si ha ragione di ritenere che siano coperti dalla previsione, ad esempio, i veicoli su cui è installato il ricevitore satellitare. Se si prende in considerazione il secondo comma dell'art. 14 Cost. è facile notare che anche la tutela del domicilio risulta inoltre garantita innanzitutto da una riserva di legge assoluta e rinforzata, in modo che solo la legge possa stabilire in che modo e quando la libertà in esame può essere sacrificata o compressa, inoltre è presente anche una riserva di giurisdizione, di modo che solo l'autorità giudiziaria, di nuovo con provvedimenti motivati, possa deciderne in concreto il sacrificio o la compressione[51].

## 3.1 – Normativa nazionale: l'inviolabilità del domicilio

Il domicilio viene considerato, nel complesso panorama relativo ai diritti fondamentali di libertà, come proiezione spaziale della persona ed assume una valenza essenzialmente negativa, concretizzandosi di fatto nel diritto di preservare da interferenze esterne, pubbliche o private, determinati luoghi in cui si svolge la vita intima di ciascun individuo[52]. La titolarità della libertà domiciliare va riconosciuta a più soggetti: in primo luogo alle

[50] A. AMORTH, *La costituzione italiana*, Giuffrè, Milano, 1948, p. 62.
[51] S. BARTOLE, R. BIN, V. CRISAFULLI e L. PALADIN, *Commentario breve*, op. cit., p. 118.
[52] C. cost., 24 aprile 2002, n. 135, in *Giur. cost.,* 2002, pp. 1062 e ss.

persone fisiche, siano esse cittadini, stranieri o apolidi, e, in secondo luogo, alle persone giuridiche e alle associazioni di fatto. La libertà di domicilio trova tutela per tutto il tempo in cui sussiste il presupposto di fatto della disponibilità di un determinato luogo, a prescindere dal titolo in ragione del quale il soggetto occupi tale luogo. Nel momento in cui venga meno il titolo che giustifica la proprietà, il possesso o la detenzione dell'immobile viene meno anche la garanzia dell'inviolabilità domiciliare[53]. Sussistono inoltre particolari ipotesi interpretative qualora un medesimo luogo costituisca domicilio per una pluralità di soggetti, titolari ciascuno di un distinto diritto domiciliare avente ad oggetto lo stesso luogo. Nell'ipotesi di interferenze pubbliche, la limitazione a tale diritto deve riguardare solamente il destinatario della misura adottata, senza che ricorra alcun pregiudizio per la libertà domiciliare degli altri soggetti. Per quanto riguarda invece l'ipotesi di interferenze private, la dottrina risulta concorde nel valutare caso per caso la soluzione di volta in volta praticabile, avendo particolare riguardo al bilanciamento degli interessi in gioco. Si possono distinguere diverse ipotesi:

a) nel caso di convivenza familiare, la giurisprudenza ed anche parte della dottrina ritengono prevalente lo *ius prohibendi* sullo *ius admittendi* dei titolari, con la naturale conseguenza, a titolo puramente esemplificativo, del necessario consenso di entrambi i coniugi circa il legittimo ingresso di un estraneo nel domicilio familiare[54];

b) diversa invece l'ipotesi in cui ci si trovi in presenza di una convivenza diversa da quella familiare. Risulta in questo caso controversa, ad esempio, la posizione della domestica qualora decida di far entrare estranei, contro la volontà del datore di lavoro, nella camera assegnatale per contratto; ancora, la legittimità di vietare tale condotta da parte dell'albergatore nel caso in cui il cliente decida di introdurre estranei nella

[53] Cass. sez. V, 11 maggio 1999, n. 7597, in *Giust. pen.,* 2000, II, p. 308.
[54] Cass. sez. V, 3 aprile 1987, in *Foro it.,* 1988, c. 272.

camera. In qualsiasi caso, la mera e transitoria convivenza non limita di certo la titolarità del diritto domiciliare e, di conseguenza, nemmeno può limitare la limitazione da parte del possessore dell'immobile di condotte simili a quelle sopra esaminate;

c) nell'ipotesi di comunità gerarchicamente organizzate – a titolo esemplificativo una caserma o un monastero – la possibilità di limitare il diritto domiciliare andrà riconosciuta in linea di massima al superiore in grado;

d) in ultimo, lo stabilimento industriale costituisce privata dimora dell'imprenditore in tutti i suoi locali[55], specificando che, in caso di assenza del titolare dell'impresa, lo *ius excludendi* spetta legittimamente in capo al dipendente più alto di grado.

Preliminare quindi ad ogni altra osservazione sul tema, risulta l'esatta determinazione del concetto stesso di domicilio, la cui mancata esplicitazione si deve principalmente a due fattori: da un lato la necessità di non irrigidire il sistema cristallizzandolo al vertice della gerarchia delle fonti e, dall'altro, alla considerazione della sua parziale superfluità, potendosi il concetto desumere dalla legislazione ordinaria. Si può partire innanzitutto dai lavori preparatori, secondo i quali il concetto di domicilio consiste in una nozione particolarmente ampia, fatta propria anche dalla giurisprudenza, che abbraccia «ogni luogo di cui la persona fisica o giuridica abbia legittimamente la disponibilità, per lo svolgimento di attività connesse alla vita privata o di relazione e dal quale intenda escludere i terzi[56]». Lo stesso concetto è stato poi ripreso dalla giurisprudenza penale, la quale individua certamente una stretta connessione tra una persona ed un luogo, generalmente chiuso, in cui si

[55] Cass. sez. V, 18 novembre 1985, Perini, in *Mass. giur. lav.,* 1986, p. 426.
[56] P. CARETTI e U. DE SIERVO, *Istituzioni di diritto pubblico*, VIII ed., Giappichelli, Torino, 2006, p. 602.

svolge la vita privata, in modo da sottrarre chi occupa detto luogo da interferenze esterne o in generale di terzi. Ciò premesso, la giurisprudenza penale sottolinea che tale concetto non può però essere esteso fino a farlo coincidere con un qualunque ambiente che tenda a garantire riservatezza, risultando dunque necessario un elemento di «stabilità» nella relazione che intercorre tra il soggetto ed il luogo[57]. E' opportuno specificare inoltre che, durante gli ultimi anni, si è venuto ad affermare il concetto del «domicilio informatico», che costituisce il bene giuridico protetto, anche a livello costituzionale, nel reato di accesso abusivo a sistema informatico (art. 615-*ter*, c.p., introdotto dal legislatore nel 1993). Esso non può esaurirsi in una mera specificazione del domicilio tutelato dall'art. 614 c.p., ma deve essere considerato come proiezione spaziale, anche fisica, della persona indicante una nuova tipologia di bene tutelato, ossia la «riservatezza informatica» che si risolve poi in concreto nella fruizione indisturbata del sistema informatico e telematico[58]. Particolare attenzione deve essere posta ai mezzi di trasporto, in quanto rimane molto controversa la possibilità di considerarli come luogo di domicilio. Secondo un primo orientamento, essi costituirebbero «privata dimora» solamente qualora sussista l'attualità dell'uso a fini privati: è il caso, ad esempio, della roulotte o del camper adibito ad abitazione permanente oppure temporaneamente, ad esempio dal turista. Un secondo orientamento invece, sostenuto tanto dalla Corte Costituzionale quanto da altre pronunce della Cassazione penale, afferma che l'autovettura deve riconoscersi come domicilio tutelato *ex* art. 14 Cost, ivi compreso il bagagliaio, anche se tale orientamento è stato corretto dalla stessa Suprema Corte con numerose pronunce successive[59].

A tali conclusioni riguardanti la nozione di domicilio si è giunti anche

[57] Cass. sez. un., 28 luglio 2006, P.A., *C.E.D. Cass.,* n. 233974.
[58] Cass. sez. VI, 4 ottobre 1999, Piersanti, cit., c. 133 e ss.
[59] Tra le tante, Cass. sez. I, 6 giugno 2003, Faraci, in *C.E.D. Cass.,* n. 225141; Cass. sez. VI, 10 dicembre 2002, Palumbo, *ivi*, n. 223961

tramite un'esegesi accurata e approfondita dell'art. 614 c.p. (Violazione di domicilio), il quale, in tema di violazione di domicilio estende la relativa tutela all'abitazione, ai luoghi di privata dimora e alle appartenenze[60]. Per quanto riguarda il concetto di «abitazione», l'esegesi della norma penale porta a considerare tale ogni luogo ove la persona, singolarmente o con altri, legittimamente dimora. Deve quindi trattarsi di un luogo adibito o adibibile al riposo notturno, anche se l'uso è solo saltuario o occasionale. Non importa che il luogo sia chiuso o aperto, immobile o mobile, ciò che conta è che lo spazio sia delimitato verso l'esterno, in modo tale da rendere palese la volontà del titolare di tale spazio di escludere terzi soggetti. Inoltre, la fruizione di tale luogo deve essere attuale da parte di colui che detiene il potere dello *ius excludendi*, rendendo per esempio un appartamento abbandonato o disabitato inidoneo ad essere qualificato come domicilio. Il concetto invece di «privata dimora» risulta più ampio di quello di abitazione, in quanto richiama, per esclusione, ogni altro luogo in cui si svolge la vita privata del soggetto, ove quindi la persona, continuativamente o saltuariamente, svolge attività, per dovere o per scelta, rispetto alle quali ha potere di accettazione o di esclusione della presenza di terzi. In ultimo, il concetto di «appartenenze» include tutti quei luoghi che integrano in senso sia logistico che di servizio la funzione che l'abitazione o il luogo di privata dimora svolgono per il soggetto che ne dispone legittimamente, così da consentirgli, per natura dei luoghi, di escludere gli altri da intromissioni che violino la vita domestica o privata, rientrando in tale schema ad esempio, giardini condominiali o pianerottoli.

Resta quindi da verificare se il comma 2 dell'art. 14 Cost., nel trasporre le garanzie contemplate dall'art. 13 Cost. a presidio della libertà personale, circoscriva l'elenco degli atti restrittivi dell'inviolabilità domiciliare ad un numero chiuso, costituito in questo caso da ispezioni, perquisizioni e

[60] M. SINISCALCO, *Domicilio (violazione di)*, in *Enc. dir.,* XIII, Milano, 1964, p. 871.

sequestri. Il tenore letterale della norma pone quindi il problema, di non poco conto, della natura tassativa o esemplificativa dell'elencazione. Dalla sua soluzione dipende quindi l'ampiezza degli strumenti sui quali i pubblici poteri potranno fare affidamento per il perseguimento di obiettivi collidenti con i valori in esame. Ispezioni, perquisizioni e sequestri, non esauriscono le limitazioni ammesse alla libertà domiciliare in quanto si tratta di misure storicamente radicate e positivamente disciplinate all'epoca della stesura della carta costituzionale: ne consegue in maniera del tutto logica che, in maniera simile per quanto accade per la libertà personale e di corrispondenza, le interferenze da parte della pubblica autorità non risultano tipizzate in modo esaustivo e tassativo dalla Costituzione. Particolarmente utile sul punto è il dibattito sviluppatosi con riferimento alle intercettazioni domiciliari, sia sotto il profilo della legittimità delle captazioni, sia sotto il profilo delle modalità esecutive delle stesse, le quali richiedono l'ingresso di appartenenti alle forze dell'ordine nei luoghi protetti per l'installazione delle trasmittenti[61]. Parte della dottrina ha sostenuto la tesi dell'incompatibilità con il dettato costituzionale dell'art. 266, comma 2, c.p.p., laddove consente l'occulta apprensione del contenuto di comunicazioni avvenute all'interno del domicilio, in quanto le intercettazioni risultano omesse dall'indicazione dei mezzi di limitazione della libertà domiciliare elencati dall'art. 14 Cost. Dette critiche tuttavia non hanno incontrato adesione da parte della giurisprudenza, grazie alla quale si è sviluppato un orientamento incline ad ammettere la legittimità costituzionale delle intercettazioni contemplate dall'art. 266, comma 2, c.p.p., sul presupposto di un bilanciamento di diversi interessi tra loro confliggenti. In tale ottica infatti si è pronunciata la Cassazione, stabilendo che necessariamente l'inviolabilità del domicilio «va correlata alla facoltà attribuita alla legge ordinaria di prevedere e regolare intromissioni nel

[61] Tale modalità operativa può essere ovviata solo ricorrendo a strumenti idonei alla captazione del suono attraverso le pareti, quali possono essere i microfoni direzionali o le finestre come nel caso dei c.d. "cannoni laser".

privato anche con la limitazione di ogni forma di comunicazione (art. 15 Cost.) per atto motivato dell'autorità giudiziaria, limitazione conseguente al privilegio che compete all'interesse pubblico la cui attuazione è demandata al p.m. dalla Costituzione (art. 112)[62]». Ad una soluzione analoga si è giunti, sempre tramite numerose pronunce giurisprudenziali, circa la collocazione di microspie all'interno di un luogo di privata dimora, di cui si è asserita la legittimità in quanto si tratta di una modalità di "attuazione naturale" dell'operazione intercettiva[63].

## 3.2 – Normativa europea: convenzione europea dei diritti dell'uomo

Uno studio accurato delle norme relative alle intercettazioni di comunicazioni contenute nell'attuale codice di procedura penale non può prescindere dal prendere come parametro di riferimento non solo l'ordinamento interno, ma anche i principi sanciti a livello europeo. Il primo profilo di interesse risulta essere quello della normativa della c.d. *privacy*. In particolare, l'art. 5 della direttiva 97/66/CE del Parlamento europeo e del Consiglio d'Europa del 15 dicembre 1997, relativo al trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, sancisce un importante principio, la riservatezza delle comunicazioni[64] e vieta in particolare «l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza il consenso

[62] Cass. sez. I, 19 ottobre 1992, Liggieri, in *Cass. pen.,* 1995, p. 991.
[63] In questo senso, Cass. sez. VI, 21 gennaio 1998, Greco, in *Dir. pen. proc.,* 1998, p. 1234; Cass. sez. I, 23 marzo 1994, Pulito, in *Giust. pen.,* 1995, III, c. 217; Cass. sez. VI, 20 febbraio 1991, Morabito, in *Giur. it.,* 1991, II, p. 466; Ass. Cassino, 27 gennaio 1992, in *Foro it.,* 1993, II, c. 570.
[64] R. GALBIATI, *Autorità garanti – Profili processuali*, in *Foro it.,* 1998, IV, c. 43.

di questi ultimi, eccetto quando sia autorizzato legalmente», cioè quando la restrizione di tale riservatezza costituisca una misura necessaria alla salvaguardia di interessi di sicurezza dello Stato, della difesa, della pubblica sicurezza, del perseguimento di reati ai sensi dell'art. 14, comma 1, della medesima direttiva. In questo ambito si può evincere come lo strumento delle intercettazioni sia poliedrico, in quanto costituisce sì un potentissimo strumento nelle indagini penali, ma può assumere funzioni anche in ambiti non penalistici. Esempio peculiare di ciò è l'intercettazione delle conversazioni o comunicazioni degli avvocati, relative anche a procedimenti diversi da quello che vede coinvolto il cliente[65]. Si può notare quindi come, l'evoluzione dei processi tecnologici si è accompagnata alle esigenze di tutela sempre nuove e, in alcuni casi, crescenti, legate alla diffusione di forme di comunicazione ben diverse da quelle immaginate inizialmente dal legislatore.

In questo complesso panorama legislativo, l'analisi della normativa relativa alle intercettazioni di comunicazioni e conversazioni non può nemmeno discostarsi dai principi sanciti dalla Convenzione europea dei diritti dell'uomo in tema di salvaguardia e rispetto della vita privata. La sopracitata Convenzione, firmata a Roma il 4 novembre 1950, è stata introdotta nell'ordinamento interno con la legge ordinaria n. 848 del 1955 e possiede dunque forza di "legge ordinaria". Tuttavia, in primo luogo la Corte costituzionale, occupandosi nel 1993 di un caso relativo all'art. 6, ne ha analizzato il "maggior grado di resistenza" e la sua "non derogabilità" considerando le norme convenzionali come «derivanti da una fonte riconducibile ad una competenza atipica e, come tali, insuscettibili di abrogazione o di modificazione da parte di disposizioni di legge

[65] Per Cass. sez. VI, 8 giugno 1995, in *Arch. n. proc. pen.,* 1995, p. 863, «i divieti e le limitazioni stabiliti dall'art. 103 c.p.p. per gli atti ivi menzionati debbono ritenersi operanti con riguardo non ai soli soggetti che esercitano attività defensionale nel procedimento nell'ambito del quale si collocano gli atti predetti, bensì a tutti coloro che, debitamente iscritti negli albi professionali, abbiano assunto difese in qualsivoglia altro procedimento».

ordinaria[66]»; in secondo luogo, il legislatore del 1987, riconoscendo l'inderogabilità degli articoli della Convenzione europea sui diritti dell'uomo, ha trasposto tale considerazione nella legge delega che ha dato vita all'attuale codice di procedura penale e all'esigenza di "conformità" e di "adeguatezza" ai principi in essa espressi. Di particolare rilevanza al fine di ottenere un quadro quanto più completo possibile in tema di intercettazioni, risulta essere l'art. 8 della Convenzione, il quale è formato da due commi: nel primo si riconosce il rispetto della vita privata, in quanto, secondo il tenore letterale della norma, «ogni persona ha diritto al rispetto della sua vita familiare, del suo domicilio e della sua corrispondenza»; nel secondo invece, si ammette una limitata compressione di tale diritto in presenza di particolari situazioni, in quanto «non può aversi interferenza di un'autorità pubblica nell'esercizio di questo diritto a meno che questa ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione di reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà degli altri». Analizzando in particolare il primo comma, risulta evidente come esso tenda a garantire la tutela di una vasta gamma di diritti che possono ricondursi, per mezzo di un'unica espressione, al diritto alla *privacy*[67]*.* La Corte europea ha affermato, a questo proposito, come nella previsione della norma rientri «qualsiasi limitazione al rispetto della vita privata[68]», per cui in questa articolata gamma di violazioni rientrano, oltre alle intercettazioni delle comunicazioni telefoniche o tra presenti, la corrispondenza[69], le riprese audiovisive all'interno di luoghi di privata dimora o nei luoghi che tali devono intendersi[70] e infine, l'introduzione nel

[66] C. cost., 19 gennaio 1993, n.10, *GiC*, 1993, n. 52.
[67] C. DI MARTINO e T. PROCACCIANTI, *Le intercettazioni*, op. cit., p. 8.
[68] C. eur., 15 marzo 2000, Khan c. Regno Unito, n. 35394/97.
[69] C. eur., 14 marzo 2002, Puzinas c. Lituania, n. 44800/98.
[70] C. eur., 12 maggio 2005, Ocalan c. Turchia, n. 46221/99.

domicilio[71]. La tutela della telefonia o della telecomunicazione non viene citata espressamente nel tenore della norma, tuttavia la giurisprudenza della Corte europea dei diritti dell'uomo la colloca all'interno della tutela prestata dall'art. 8 della Convenzione europea sui diritti dell'uomo, in quanto riconosciuta attraverso i concetti di «vita privata» e «corrispondenza»[72]. Inoltre, secondo la Corte, ogni intercettazione include di per sé la caratteristica di «ingerenza della pubblica autorità» nella sfera privata, anche quando «di essa non si sia fatto un uso processualmente rilevante»[73]. Tuttavia, prestando particolare attenzione al tenore letterale della norma e sulla scorta della giurisprudenza della Corte europea, si può trarre una prima conclusione in merito alla conformità alla norma dell'art. 8 CEDU di qualsiasi attività volta a carpire notizie e informazioni attraverso interferenze nella vita privata: l'intercettazione o la raccolta di dati di connessione tra privati deve, prima di tutto, essere prevista da una legge dello Stato, la quale deve giustificare e disciplinare tale intrusione secondo quelle finalità. In questo senso, il legislatore della normativa vigente sembra sia riuscito a raggiungere tale equilibrio richiesto dalla normativa europea, in quanto la disciplina contenuta nel codice soddisfa ampiamente la condizione richiesta per poter giustificare un'interferenza nella sfera privata[74]. L'art. 267 c.p.p. sancisce infatti che le intercettazioni devono essere autorizzate dal giudice per le indagini preliminari preventivamente ovvero, in casi di urgenza, convalidate, quando vi sono gravi indizi di reato e quando ciò appare indispensabile alla prosecuzione delle indagini, cioè in scenari in cui, in una «società democratica», si profili la necessità di operare in accordo a quanto stabilito dall'art. 8, comma 2, della Convenzione europea dei diritti dell'uomo. Coerentemente con

[71] C. eur., 23 settembre 1998, McLeod c. Regno Unito, in *Recueil des arrêts et décisions*, VII, 1998, p. 2791, § 52.
[72] C. eur., 6 settembre 1978, Klass e altri c. Germania, n. 5029/71, punto 41.
[73] C. eur., 25 marzo 1998, Kopp c. Svizzera, n. 23224/94.
[74] C. ROSSI, *Il rispetto della corrispondenza nella Convenzione europea dei diritti dell'uomo. Le intercettazioni nella legislazione italiana*, in *Riv. int. dir. uomo,* 1994, p. 67.

quanto affermato sopra quindi, la Corte europea dei diritti dell'uomo ha riscontrato la violazione di tale norma in presenza di interferenze nella vita private dovute non soltanto ai casi in cui le norme interne fossero troppo generiche, ma anche laddove la carenza si riferisse alle modalità di intrusione[75]. Sembra dunque che sin qui, si possa esprimere un giudizio di generale conformità della legge italiana in materia di intercettazioni rispetto alle disposizioni della Convenzione europea dei diritti dell'uomo anche se, il pericolo maggiore, può essere rappresentato dalla "prassi" che, disattendendo in alcuni casi la norma, può anteporre le importanti esigenze di difesa sociale a così importanti diritti soggettivi. Di particolare interesse è una recente decisione di merito che riguarda in generale la possibilità di registrazione e documentazione dei rapporti tra privati, in totale disaccordo con la giurisprudenza delle Sezioni Uniti, ma fondata sull'art. 8 CEDU e dotata di particolare suggestione. L'organo giudicante ha affermato infatti che la registrazione di una conversazione telefonica eseguita da uno degli interlocutori all'insaputa dell'altro è inutilizzabile *ex* art. 191, comma 1, c.p.p. in quanto acquisita in violazione dei divieti stabiliti dalla legge ed in particolare da quelli imposti dall'art. 8 della Convenzione europea dei diritti dell'uomo[76]. Il principio espresso dal Tribunale di Roma, per quanto suggestivo, risulta tuttavia non condivisibile per due motivi fondamentali: in primo luogo, l'attività di registrazione privata risulta ontologicamente distinta dall'interferenza pubblica; in secondo luogo, anche se si decidesse di valutare quest'ultima esclusivamente in base alla possibilità di utilizzo processuale di tali registrazioni, esiste una norma specifica – l'art. 234 c.p.p. (La prova documentale) – la quale prevede tali forme di documentazione proprio in relazione all'esigenza generale di accertamento e repressione dei reati[77].

[75] C. eur., 25 gennaio 1997, Halford c. Regno Unito, *ivi*, p. 613.
[76] GIP Trib. Roma, ord. 14 febbraio 2000, *CP*, 2000, 1931, con nota di C. Carmona.
[77] C. PARODI, *Le intercettazioni*, op. cit., pp. 44 e ss.

In chiusura, su questo punto va ricordato che diverse indicazioni proveniente dalle decisioni della Corte europea sono state riprese anche a livello di direttive e di documenti ufficiali degli organi europei. In tema di intercettazioni, una in particolare risulta degna di nota, ossia la «Dichiarazione ufficiale del Parlamento europeo» del 16 settembre 1998, concernente le relazioni transatlantiche, dove è stato espressamente enunciato il principio di proporzione e contenimento più volte richiamato dalla giurisprudenza europea[78]. Secondo il Parlamento europeo in particolare «il punto di vista secondo cui l'intercettazione di tutte le comunicazioni rappresenterebbe la miglior protezione contro la criminalità organizzata sarebbe contrario all'art. 8 CEDU anche se fosse ammesso dalla legislazione statale, poiché un sistema di servizi d'informazione che captasse qualsiasi comunicazione costituirebbe comunque una violazione del principio di proporzionalità[79]».

[78] A. BARGI e S. FURFARO, *Le intercettazioni di conversazioni e* comunicazioni, in *La prova penale*, di A. Gaito, in *Trattati brevi*, vol. II, *Le dinamiche probatorie e gli strumenti per l'accertamento giudiziale*, UTET GIURIDICA, 2010, pp. 109 e ss.
[79] Sessione plenaria, processo verbale parte II, B4-0803, 0806 e 0809/98.

# Capitolo 2

# L'utilizzo dei captatori informatici per scopi intercettivi

SOMMARIO: 1 – La necessità del nuovo strumento ai fini investigativi. – 1.1 – Il caso Hacking Team. – 2 – La definizione di captatore informatico. – 2.1 – Proposte legislative in materia. – 3 – Ambito di applicazione. – 3.1 – Definizione di "delitti di criminalità organizzata". – 3.2 – Disciplina derogatoria del d.l. 152/1991.

## 1 – La necessità del nuovo strumento ai fini investigativi

Il diritto si sta muovendo sempre più in fretta verso la digitalizzazione, nel senso che nella società odierna, anche nel corso di investigazioni correlate a reati "tradizionali", vengono in essere, sempre con più frequenza, aspetti tecnologici. L'evoluzione storica della disciplina di studio e di ricerca, denominata *computer forensics*, è strettamente collegata al progresso dell'*information and communication technology* nell'era moderna, in quanto, contestualmente al cambiamento portato nella società dalle nuove tecnologie, in particolare dall'elaboratore elettronico e dalle reti, si è verificato un profondo mutamento delle modalità di rilevazione, gestione, raccolta e analisi di elementi che, in senso lato e con

un significato profondamente generico, si potrebbero definire fonti di prova, prova, indizio o testimonianza[80]. La *computer forensics* è, di conseguenza, l'estensione naturale di teorie, principi e prassi proprie della scienza forense intesa in senso lato, applicate però al mondo dell'informatica e delle nuove tecnologie. Una prima definizione tecnica iniziale potrebbe quindi essere la seguente: per *computer forensics* si intende quella scienza che studia il valore che un dato correlato ad un sistema informatico o telematico può avere in ambito sociale, giuridico o legale[81]. Tale definizione può essere tuttavia scissa in due ulteriori definizioni diverse: la prima, quella cioè che prende in considerazione la *computer forensics* pura, che comprende solo ed esclusivamente l'ambito legale, o processuale, dell'acquisizione, analisi e esposizione del dato, risultando quindi fondamentale l'aspetto legale e il fatto che il dato sia "inquadrabile" in un contesto giuridico, poiché altrimenti non si potrebbe parlare in senso stretto di *forensics*; la seconda definizione invece, prende spunto da una consolidata tradizione di *forensics* aziendale, la quale consiste in una simulazione di attività che potrebbero essere finalizzate alla produzione della prova in giudizio, con la peculiarità che tale attività sono effettuate in ambito interno aziendale, seguendo, in alcuni casi, identiche metodologie[82]. Ai fini della seguente trattazione si prediligerà, per motivi di attinenza, la prima definizione, anche se in molti casi i fini delle due teorie possono risultare gli stessi: scoprire un determinato fatto, le sue prove, i collegamenti ad uno o più soggetti, valutare poi se tale fatto può essere nocivo o meno ed elaborare infine dei metodi corretti per

[80] In questo contesto, detti termini, non sono utilizzati in riferimento ad un determinato e predefinito sistema processuale, ma semplicemente come indicazione di eventi che in determinati contesti – non necessariamente giudiziario – siano idonei a fornire un certo tipo di informazione.
[81] G. ZICCARDI, *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali,* vol. II, seconda edizione, Giuffrè Editore, Milano, 2013, p. 236.
[82] J. S. RINGOLD III, *Corporate Forensics Toolkit*, in Internet all'indirizzo http://mn-isfa.org/presentations/corporateforensicstoolkit.ppt.

giungere a tali conclusioni. La suddetta disciplina risulta quindi essere multidisciplinare, in quanto si vedono coinvolte all'interno di essa competenze ed aree molto diverse tra di loro: si può rilevare *in primi*s un aspetto prettamente informatico, successivamente uno prettamente giuridico (sia processuale che tecnico) e infine uno puramente investigativo. Si può citare il dato, puramente a titolo esemplificativo, secondo il quale negli Stati Uniti d'America, considerato anche il diverso *curriculum studiorum*, si avvicinano a queste tematiche soggetti che spesso hanno conseguito due lauree, una in materie informatiche ed una in materie giuridiche. Tornando alla tripartizione della *computer forensics* citata sopra, si può notare, relativamente agli aspetti puramente informatici, che essi sono essenzialmente correlati alla conoscenza del computer e dei dati, alla compressione delle procedure e del *software*, alla capacità di utilizzo pratico degli strumenti informatici più efficaci ed affidabili per effettuare le operazioni richieste. Relativamente alle capacità d'indagine, esse riguardano principalmente il problema relativo a cosa cercare e dove cercarlo, e nel caso di presenza di grandi quantitativi di dati, risultano essere dei requisiti essenziali per portare a termine le attività investigative. In ultimo, gli aspetti legali sono principalmente correlati ai seguenti temi: conoscenze di diritto processuale, soprattutto in tema di corretta modalità di acquisizione delle prova (si noti bene: correttezza di carattere non esclusivamente tecnologica, ma anche procedurale), conoscenze dei limiti e dei diritti previsti dalla legge sempre relative all'acquisizione delle prove e infine, possono giovare aspetti di analisi e profilazione dei comportamenti criminali e di psicologia giudiziaria. L'unione di tutti gli aspetti sopra citati contribuisce a formare il panorama attuale della *computer and network forensics*.

La necessità di affidarsi a tali nuove tecniche di indagini deriva soprattutto dal fatto che il mancato adeguamento a tali cambiamenti da parte di larghissimi settori della società interessati a queste tematiche giuridiche,

in particolare magistrati, avvocati, operatori di polizia giudiziaria, i quali dimostrano spesso una nulla o lacunosa preparazione tecnologica, ha portato ad adottare metodi di indagine errati e inefficaci, o in altri casi, all'automazione di deleghe e di *expertise*. In un recente articolo[83] pubblicato dagli esperti Mattiucci e Delfinis, gli stessi autori hanno individuato il *forensic computing* come «scienza emergente» e «disciplina sostanziale atta a validare la scientificità dell'operato del Ra. C.I.S. (Raggruppamento Carabinieri Investigazioni Scientifiche)». A questo proposito risulta preminente l'analisi delle memorie digitali al fine di poter correttamente individuare possibili indizi ed elementi probatori che possano correttamente indirizzare le indagini dei Reparti territoriali e speciali dell'Arma. L'approccio adottato dai due autori risulta quindi tipicamente penalistico-investigativo e parte del presupposto fondamentale secondo il quale ogni utente di un sistema informatico, nel momento in cui opera su un qualsiasi sistema di elaborazione, crea, spesso a sua completa insaputa, una serie di tracce che possono divenire prove di un'attività illecita. In questa ottica quindi, al fine di recuperare dette informazioni, si rendono necessarie tecniche, procedure e sistemi specifici, i quali per forza di cose richiedono un avanzamento tecnologico al passo con i tempi, in modo da rendere le indagini più efficaci e allo stesso tempo capaci di recuperare prove e indizi che, con i metodi tradizionali, non verrebbero probabilmente raccolti.

L'analisi condotta dai due Autori citati porta quindi a proporre due definizioni[84] della *forensic computing*, le quali riuniscono i concetti essenziali della stessa e al tempo stesso pongono al centro della materia l'importanza del dato digitale:

a) «il processo di: identificazione, conservazione, analisi e presentazione

[83] M. MATTIUCCI e G. DELFINIS, *Forensic Computing,* in *Rassegna dell'Arma dei Carabinieri*, Anno LIV, aprile/giugno 2006, n. 2-2006, pp. 51 e ss.
[84] M. MATTIUCCI e G. DELFINIS, op. ult. cit., p. 61.

di *digital evidence* in processo garantendone l'ammissibilità», intendendo per *digital evidence* ogni «prova legale ottenuta attraverso sistemi digitali»;

b) «la raccolta e l'analisi di dati secondo una prassi che ne garantisca la libertà da distorsioni e pregiudizi cercando di ricostruire dati ed azioni avvenuti nel passato all'interno del sistema informatico».

Secondo altri, si è invece in presenza di una sorta di nuova specializzazione dell'attività svolta dalla polizia scientifica, come lo possono essere la balistica, la genetica, l'ematologia applicata, che entra forzatamente in gioco nel momento in cui le evidenze dell'azione criminosa sono reperibili solamente attraverso strumenti informatici e nel "mondo digitale"[85]. Quest'ultima definizione associa quindi, in modo inequivocabile, la *forensics* alla *scena criminis* in quanto viene logico pensare che, nel momento in cui nella stessa si rinviene un qualsiasi dispositivo tecnologico, esso necessiti di essere analizzato come del resto il restante materiale presente sulla scena, indipendentemente dal crimine che è stato perpetrato. L'analisi fornita dalla polizia scientifica può essere quindi decisiva in quanto i legami tra un qualsiasi dispositivo *hardware* e un crimine possono sfuggire all'inizio, ma tuttavia essere scoperti per mezzo di un'analisi successiva e più approfondita.

Come evidenziato precedentemente, oggigiorno qualsiasi scena del crimine presenta una moltitudine di dispositivi *high-tech* facendo sorgere quindi non solo il problema della loro identificazione, ma al tempo stesso di una loro corretta gestione in modo da poter estrapolare in modo completo le informazioni che tali oggetti possono contenere.

Tutto quanto sopra descritto ovviamente ha fornito le basi per la crescita di un settore, quello dell'*information technology*, fino a prima

[85] A. GHIRARDINI e G. FAGGIOLI, *Computer forensics*, Apogeo, Milano, 2007, p. 45.

sottovalutato dal punto di vista giuridico-legale, o quantomeno non sfruttato appieno.

## 1.1 – Il caso Hacking Team

Come specificato nel paragrafo precedente, un'effettiva lotta contro gravi forme di criminalità dipende in maniera sempre crescente dall'utilizzo di strumenti di indagine ad alto contenuto tecnologico. Proprio per questo motivo, il settore dell'*information technology* ha conosciuto un incremento elevato nell'ultimo decennio, in quanto la domanda da parte di vari tipi di "consumatori" è cresciuta di pari passo con il progresso in determinati campi della tecnologia. Le aziende hanno iniziato a sviluppare i loro servizi di consulenza informatica e a metterli a disposizione dei più disparati clienti, dalle forze di polizia ai servizi segreti fino ad arrivare agli stessi governi in carica. Esistono infatti una decina di società private al mondo che vendono *software* c.d. di spionaggio, cioè in grado di captare e di estrapolare diverse informazioni dai *device* oggetto di attacco, alle forze dell'ordine e alle agenzie di intelligence di tutto il mondo. Una di queste società ha sede in Italia, precisamente a Milano e prende il nome di "Hacking Team". Essa è formata da una quarantina di dipendenti, tra ingegneri e venditori, i quali forniscono i loro prodotti ad oltre 40 paesi nel mondo e rappresenta in modo inequivocabile quel fenomeno che è stato definito dal gruppo internazionale Reporter come «l'era dei mercenari digitali». Come sostenuto sul sito della società stessa, Hacking Team fornisce servizi catalogati come «strumenti di hackeraggio per le intercettazioni governative», destinati quindi alla lotta alla criminalità e al terrorismo. E' proprio "grazie" al terrorismo che il gruppo Hacking Team ha realizzato una rete di clienti e di affari che produce notevoli guadagni. L'11 marzo del 2004 infatti, durante l'ora di punta, dieci enormi esplosioni

colpirono quattro treni di pendolari di Madrid, uccidendo quasi 200 persone e ferendone altre 1800. Furono classificati come gli attentati più letali della storia spagnola ed erano stati organizzati e pianificati utilizzando un vero e proprio arsenale di mezzi tecnologici a basso costo come *social networks*, servizi di messaggistica istantanea e *software* di video conferenza. La polizia spagnola non disponeva allora di un reparto specializzato nella sicurezza informatica, nella repressione della criminalità tramite strumenti tecnologici e quindi non aveva, di fatto, nemmeno i mezzi per reagire a tale minaccia[86]. Il fondatore e CEO di Hacking Team, David Vincenzetti, decise allora di convincere l'allora governo spagnolo dell'importanza cruciale che poteva rivestire il suo *software* di spionaggio nella lotta al terrorismo. Il programma di cui si è fatto menzione poco fa risponde al nome di RCS, acronimo per il nome *Remote Control System*, elaborato dallo stesso Vincenzetti e da due sue collaboratori tra il 2003 e il 2004. Il *software*, prodotto simbolo del gruppo Hacking Team, è in grado di prendere il controllo dei dispositivi bersaglio senza poter essere rilevato, permettendo inoltre a chi lo utilizza di utilizzare altri tipi di *software* malevoli contro un nemico identificato. Il *software* quindi crea una sorta di "dossier" dell'obiettivo identificato: esiste quindi una sezione contenente una foto profilo del soggetto utilizzatore dei dispositivi sottoposti a controllo; un menù con i dispositivi che il soggetto utilizza, come *computer, smartphone, tablet*, etc., i quali permettono l'accesso ai dati personali dell'obiettivo, come l'email, il profilo *Facebook*, gli alter-ego utilizzati nella rete, *Skype*, i siti preferiti e quant'anche la posizione geografica. Naturale conseguenza di questa attività di spionaggio è il raccoglimento, nel corso del tempo, di una rete di informazioni di intelligence profonde e ramificate. Più nel dettaglio, le funzioni salienti del software RCS, comprendente anche lo *spyware* soprannominato DaVinci, risultano essere:

[86] C. DI STASIO, *La lotta multilivello al terrorismo internazionale: garanzia di sicurezza versus tutela dei diritti fondamentali*, Giuffrè, 2010, pp. 233 e ss.

a) raccolta segreta di email, SMS, cronologia telefonica e lista dei contatti;

b) intercettazione di tastiere;

c) spiare la cronologia delle ricerche *web* e "catturare" le schermate visualizzate sul dispositivo;

d) registrare telefonate;

e) usare i telefoni per intercettazioni di tipo ambientale;

f) mettere in funzione la foto-videocamera di telefoni o computer;

g) sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati.

Si può facilmente intuire perciò come le potenzialità di tale *software* siano quindi di portata molto ampia con la logica conseguenza di un possibile utilizzo distorto da parte di soggetti non proprio impeccabili dal punto di vista etico. Nonostante infatti il gruppo Hacking Team abbia sempre affermato, per mezzo dei suoi portavoce e anche nella stessa sezione dedicata alla politica dei clienti sul sito dell'azienda, di aver declinato le offerte di acquisto di tale programma da soggetti per esempio presenti nelle liste nere di Nazioni Unite, Unione Europea, NATO e ASEAN, sono stati riportati diversi casi in cui tali procedure di controllo sui potenziali clienti non hanno dato propriamente i frutti sperati, come ad esempio la vendita del *software* di spionaggio al Sudan per la cifra di 960mila euro, nel momento in cui il leader del paese era stato accusato di genocidio dalla Corte Penale Internazionale[87]. Proprio per questo motivo, nel giugno

[87] D. KUSHNER, *La storia di Hacking Team, dall'inizio*, in Internet al sito

del 2014, Hacking Team ricevette un fax da parte dell'ONU, a firma di un gruppo di esperti dell'ONU per il Sudan presieduti da Lipika Majumdar Roy Choudhury, secondo il quale «dal momento che il *software* si adatta perfettamente a sostenere operazioni militari di intelligence elettronica (ELINT), potrebbe rientrare potenzialmente nella categoria di "equipaggiamento militare" o "assistenza legata a prodotti vietati"», in quanto le sanzioni internazionali applicate dall'ONU per i crimini commessi dal Sudan vietavano la vendita di «armi […] incluso l'equipaggiamento militare», ratificate poi anche dall'Unione Europea, dal comitato per la politica estera e la sicurezza comune (PESC o in inglese CFSP)[88]. Come conseguenza di dette attività l'Italia adottò, il primo gennaio 2015, l'intesa di Wassenaar, un accordo internazionale che regola le esportazioni di beni ad uso duplice, creato nel 1996 e in seguito riadattato per includere anche gli strumenti di sorveglianza informatica, facendo in modo che il Governo italiano potesse esaminare, almeno in linea teorica, i possibili clienti di Hacking Team.

Le società di *information technology*, come Hacking Team e altre sparse in vari paesi del mondo, hanno tuttavia iniziato a subire diversi attacchi informatici da parte di hacker e attivisti per i diritti umani, i quali lamentavano che dette società facessero affari con paesi i cui regimi commettevano giornalmente violazioni dei diritti umani o perlomeno non mantenevano gli stessi standard stabiliti a livello internazionale. Il primo caso, probabilmente anche quello più conosciuto, è quello che coinvolse la società anglo-tedesca Gamma Group, produttrice dello *spyware* FinFisher ed hackerata, durante l'estate 2014, da un hacker soprannominato Phineas Fisher. Comparve infatti su *Twitter* un profilo chiamato @GammaGroupPR, nome palesemente parodistico, tramite il quale il

---

http://www.ilpost.it/2016/05/15/hacking-team/.

[88] Regolamento (UE) n. 747/2014 del Consiglio, 10 luglio 2014, concernente misure restrittive in considerazione della situazione in Sudan e che abroga i regolamenti (CE) n. 131/2004 e (CE) n. 1184/2004, in *GUUE*, L 203/1, 11 novembre 2014.

sopra citato hacker rilasciò oltre 40 gigabyte di dati sensibili facenti capo all'azienda produttrice del *software* di spionaggio, pubblicando successivamente anche una guida in cui lo stesso hacker spiegava come avrebbe violato la sicurezza informatica dell'azienda, una sorta di guida all'hacking. Tramite i documenti riservati pubblicati dall'hacker Phineas Fisher si scoprì che l'azienda anglo-tedesca vendeva il proprio *software* di spionaggio al governo del Bahrain, un piccolo stato situato su un arcipelago a largo delle coste occidentali del Golfo Persico. Lo stato è organizzato nelle vesti di una monarchia costituzionale, tuttavia sono state riportate diverse violazioni dei diritti umani, in particolar modo l'arresto di vari attivisti facenti capo a movimenti per i diritti umani, per i diritti delle donne e per l'affermazione della democrazia nel paese. Tali violazioni sarebbe state perpetrate anche grazie all'utilizzo del *software* spia venduto al governo di Bahrain da Gamma Group.

La stessa società Hacking Team rimase vittima di un attacco informatico nel luglio del 2015, orchestrato dallo stesso hacker e attivista noto come Phineas Fisher, il medesimo implicato nel caso Gamma Group, il quale entrò nell'account ufficiale della società su *Twitter* e pubblicò un messaggio che recitava testualmente: «Dal momento che non abbiamo niente da nascondere, pubblichiamo tutte le nostre mail, i nostri *file* e il nostro codice sorgente». Sotto tale messaggio era riportato un collegamento ipertestuale, in gergo un *link*, ad oltre 400 gigabyte con i dati più sensibili della società, rendendo quindi di dominio pubblico le reti di sorveglianza utilizzate da molteplici servizi di spionaggio in tutto il mondo[89]. Oltre ad aver reso sostanzialmente inutile il programma RCS, i documenti pubblicati dall'hacker Phineas Fisher riportavano dati ben più allarmanti. Essi contenevano infatti molte fatture che collegavano Hacking Team con regimi oppressivi del calibro di Etiopia, Bahrein, Egitto,

[89] V. PORCU, *"Vi spiego come ho attaccato l'Hacking Team"*, in Internet al sito http://www.repubblica.it/tecnologia/sicurezza/2016/04/20/news/hacking_team_attacco-138026549/.

Kazakistan, Arabia Saudita, Russia e Azerbaijan. Dopo aver sostenuto per svariati anni di eseguire controlli scrupolosi sui propri clienti e anche su quelli potenziali, si venne a scoprire che nonostante i sopra citati controlli, la violazione dei diritti umani in atto in alcuni dei paesi beneficiari di tali tecnologie non era di interesse per la società milanese, o almeno era stata valutata con leggerezza. Oltre le conseguenze internazionali dovute alle pubblicazioni di tali dati, la società Hacking Team ha subito anche conseguenze a livello nazionale. Il 31 marzo 2016 infatti, la Direzione generale per la politica commerciale internazionale (Autorità per l'esportazione di beni a duplice uso), la quale fa capo al dicastero dello Sviluppo economico (Mise), ha deciso di revocare, con "decorrenza immediata", l'autorizzazione globale concessa nel 2015 all'azienda e relativa alla vendita dei *software* spia a livello internazionale. Tale provvedimento è stato adottato soprattutto in funzione di quanto pubblicato dall'attacco hacker subito dalla società: stando ai documenti rilasciati infatti, l'azienda milanese avrebbe venduto tali tecnologie anche al governo del Cairo, recentemente coinvolto in tensioni di carattere politico-istituzionali con l'Italia a causa dell'omicidio di un cittadino italiano, Giulio Regeni. Il provvedimento emanato dal Mise risulta motivato «alla luce di mutate situazioni politiche» in alcuni degli stati esteri in cui Hacking Team aveva ricevuto l'autorizzazione a poter vendere i propri prodotti, in quanto oltre all'Egitto, la lista comprendeva altri 45 paesi[90]. Nonostante tali conseguenze, dopo tre mesi passati dai dipendenti di Hacking team a ripristinare e riscrivere il codice sorgente del proprio *software* spia, sembra che la società sia tornata ad operare normalmente sul mercato, vista sia la crescente richiesta di tali strumenti soprattutto alla luce degli attentati terroristici sempre più frequenti e anche grazie allo

[90] A. PITONI, *Hacking Team, revocata l'autorizzazione globale all'export del software spia: stop anche per l'Egitto dopo il caso Regeni,* in Internet al sito http://www.ilfattoquotidiano.it/2016/04/06/hacking-team-revocata-lautorizzazione-globale-allexport-del-software-spia-stop-anche-per-legitto-dopo-il-caso-regeni/2610721.

sviluppo da parte di Hacking Team di una versione nuova e migliorata di RCS.

# 2 – La definizione di captatore informatico

L'attacco informatico alla società Hacking Team ha portato di nuovo alla ribalta delle cronache l'utilizzo del *trojan*, il programma/virus tramite il quale è possibile captare e carpire le più disparate informazione dal dispositivo "infettato" dal suddetto *software*. In primo luogo si era registrata una posizione favorevole da parte dell'opinione pubblica rispetto all'utilizzo di tali tecnologie, ricordando a tal proposito come esse abbiano rappresentato l'elemento cardine ai fini investigativi durante il procedimento iniziato dalla procura di Napoli contro la loggia P4 il quale vedeva indagato anche il faccendiere Luigi Bisignani, il cui computer fu in pratica "trasformato" in una microspia proprio grazie all'utilizzo di un *trojan*. Nel dettaglio, «la chiave dell'inchiesta P4 sta anche in qualche byte di codice, in un programma per computer – un virus si potrebbe dire – che i p.m. Woodcok e Francesco Curcio sono riusciti ad installare nel portatile di Luigi Bisignani, trasformandolo di fatto in una cimice. Un esempio di tecnologia "da hacker" utilizzata per fini nobili: come un Robin Hood che intercetta gli indagati per aiutare la giustizia[91]». Tecnicamente questi programmi vengono definiti *trojan* e prendono il nome dal famoso cavallo utilizzato durante la guerra di Troia nell'Iliade di Omero: più nello specifico, questi *software* si installano all'insaputa del proprietario del *device* o dispositivo che si intende sottoporre a controllo, agendo in silenzio e nell'ombra, permettendo quindi di estrapolare informazioni ritenute rilevanti per chi ha installato il programma. In genere vengono

[91] A. SGHERZA, *Un virus per pc inchioda Bisignani. Lo stato diventa hacker a fin di bene*, in Internet al sito http://www.repubblica.it/politica/2011/06/22/news/mail_spia_hacker-18041273/.

utilizzati dagli hacker per poter rubare dati personali agli utenti, quali password o numeri di carte di credito, ma, in questo caso, il programma denominato "Querela", è stato interamente sviluppato dalle forze dell'ordine italiane ed ha la funzione peculiare di trasformare il dispositivo "infettato" in una cimice. Prendendo il controllo della scheda audio infatti, il *software* può catturare attraverso il microfono tutto quello che succede nel luogo dov'è situato il dispositivo ed inviarlo in tempo reale agli investigatori. Inoltre, esso è in grado di registrare direttamente dalla scheda audio, aggirando le difficoltà spesso associate alle intercettazioni di telefonate avvenute tramite l'utilizzo di *software* Voip (*Voice over internet protocol*, come per esempio *Skype*). "Querela" risulta quindi essere un esempio più che positivo di ciò che uno Stato può fare sfruttando la tecnologia, ma è solamente un caso limite, in quanto la tecnologia è diventata sempre più uno strumento di competizione internazionale e non sempre è utilizzata per fini nobili, vedasi per esempio il caso Hacking Team. L'utilizzo del programma sopra citato, oltre ad altri vari *trojan* utilizzati dalle forze dell'ordine nella loro attività investigativa, è sempre stato un uso costituzionalmente orientato, in quanto possibile grazie alla lacuna normativa sul tema[92]. Il caso Bisignani prima e il caso Hacking Team dopo, senza dimenticare anche quanto accaduto alla società anglo-tedesca Gamma Group, hanno portato alla luce la necessità di definire, soprattutto da un punto vista giuridico-normativo, lo strumento del c.d. captatore informatico, il sopra citato *trojan*. E' notabile fin da subito come parte dell'operatività del captatore informatico sia ricollegabile alla disciplina di cui agli artt. 266 e ss. c.p.p., anche prendendo in considerazione la definizione stessa di intercettazione processuale.

[92] Come specifica F. CORDERO, *Tre studi sulle prove penali,* Giuffrè, 1963, p. 164, «nel silenzio della Legge, ricostruire il filo che lega l'indagine individuando la corretta applicazione delle disposizioni espresse dal codice di rito non può che essere quesito che esige di essere risolto in base ad una interpretazione sistematica delle norme stesse, salvo poi verificare se la disciplina di cui si è ricostruito l'assetto non confligga con i principi della Costituzione».

L'ordinamento giuridico italiano non conosce una nozione unitaria di «intercettazione di comunicazioni», come è stato più volte osservato da numerosi autori in dottrina[93] in quanto tale espressione compare in diverse norme tra di loro eterogenee, ma le Sezioni Unite della Corte di Cassazione, con una pronuncia del 2003, hanno incluso in tale definizione le operazioni con carattere occulto e clandestino, avvenute anche tramite tecnologia informatica o telematica[94], includendo in questo modo anche lo strumento del captatore informatico. Tuttavia, appare subito evidente come, nonostante l'inclusione in tale definizione del virus *trojan*, esso sia idoneo anche a svolgere altri tipi di intercettazioni che non rientrano nell'alveo della pronuncia delle S. U., in particolare esso permette[95]:

a) l'acquisizione della corrispondenza giacente nel dispositivo, quale *res* precostituita e non contestualmente captata;

b) l'acquisizione dei dati attinenti al traffico telefonico o dei *log files*, essendo essi dei meri dati avvenuti all'esterno della conversazione telefonica stessa;

c) la captazione delle immagini, tramite l'attivazione occulta della *webcam*;

d) l'estrapolazione di dati, non aventi per forza ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del dispositivo o che in futuro potranno essere memorizzati lì.

[93] C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007, p. 4.
[94] Cass. sez. un., 28 maggio 2003, n. 36747, in *Cass. pen.,* 2004, p. 209.
[95] F. CAJANI, *L'odissea del captatore informatico,* in *Cass. pen., 2016,* n. 4143.

Tutte queste attività, seppur diverse dalla normale concezione di intercettazione, sono state oggetto di diverse pronunce da parte della Suprema Corte, la quale ha operato diversi interventi risolutivi: per quanto riguarda la captazione di immagini, sia pure se realizzata con strumenti tecnologici differenti da quello in esame, la Suprema Corte ha distinto, oltre alla natura dei luoghi in cui avviene la captazione, anche la natura dei comportamenti, comunicativi e non[96], alle quali esse fanno riferimento[97]; per quanto attiene invece all'estrapolazione di dati, in questo caso non attinenti alla corrispondenza e non aventi ad oggetto un flusso di comunicazioni, il caso è stato affrontato durante il procedimento Virruso[98], relativamente, nel caso di specie, ad una modalità investigativa che, seppur adottata nel 2004, ebbe riconoscimento giurisprudenziale di legittimità solamente nel 2010[99].

Il tema affrontato ha potuto trovare riscontro a livello internazionale, non essendo esso riconducibile ad una questione meramente relativa allo Stato italiano. Un esempio chiarificatore può essere quello relativo all'analisi apparsa sul *New York Times* a dicembre del 2015, in cui si sostiene che «poiché la legge americana ha fatto in modo che sia quasi impossibile ottenere delle prove digitali tramite canali legali, le forze dell'ordine si stanno dedicando a quelli illegittimi[100]». Analisi che risulta in parte condivisibile, soprattutto se si pensa alle molteplici funzionalità assicurate

[96] Cass. sez. V, 17 dicembre 2015, n. 11419, in *C.E.D. Cass.,* n. 266373.
[97] Cass. sez. VI, 10 novembre 1997, n. 4397, in *C.E.D. Cass.,* n. 210063.
[98] Cass. sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.,* n. 246954.
[99] Anche tale sentenza si colloca in quel filone giurisprudenziale relativo ai mezzi di prova atipici di cui si è fatta menzione sopra relativamente alla registrazione di immagini. Si può ritenere infatti legittimo il decreto del Pubblico Ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel *personal computer* dell'imputato
[100] A. KEANE WOODS, *Dark Clouds Over the Internet*, in Internet al sito https://www.nytimes.com/2015/12/01/opinion/dark-clouds-over-the-internet.html?_r=0. L'impostazione è stata poi successivamente ripresa anche da E. SEGANTINI, *Difesa di privacy e sicurezza alla rete serve una governance*, in Intenet al sito http://www.corriere.it/opinioni/15_dicembre_23/rassegniamoci-anche-internet-ha-bisogno-regole-b1f03282-a93b-11e5-8f07-76e7bd2ba963.shtml.

dall'utilizzo del captatore informatico all'interno di indagini particolarmente complesse, ma che solleva anche numerosi dubbi rispetto alla legittimità di tale strumento e, in particolar modo, alle modalità di utilizzo del medesimo. Anche alla luce di suddette preoccupazioni, una chiusura totale allo strumento non sarebbe tuttavia possibile per ragioni di prevenzione e repressione di una criminalità che fa vasto impiego di nuove tecnologie. L'uso del captatore risulta quindi indispensabile nel corso delle indagini per carpirne una parte quantitativamente rilevante di informazioni, per esempio in merito a possibili conversazioni avvenute tramite l'utilizzo di *app* di messaggistica istantanea, quali *Telegram* o *Whatsapp*, operazioni che, senza poter penetrare in maniera efficace e occulta all'interno del dispositivo in utilizzo ai soggetti indagati, risulterebbero impossibili. Tutto questo non intende dire che sia facile e "scontato" l'utilizzo di un captatore informatico, in quanto deve fare i conti con numerosi problemi, sia di natura tecnica (come può essere ad esempio il consumo di batteria insolito del dispositivo sottoposto ad intercettazione, o ancora la presenza di *antivirus* o di altri sistemi di protezione quali possono essere i *firewall*) sia di natura giuridica in merito alla sua legittima applicazione caso per caso. Si sancisce però l'esigenza secondo la quale anche i mezzi tecnologici utilizzati all'interno delle inchieste devono di conseguenza evolversi, in modo da non limitare l'efficacia dell'inchiesta giudiziaria tenendola al di fuori di tali tecnologie nella utopistica idea che se ne possa fare a meno[101].

[101] L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in Internet al sito http://www.penalecontemporaneo.it/d/5267-dopo-le-sezioni-unite-sul-captatore-informatico-avanzano-nuove-questioni-ritorna-il-tema-della-funz.

# 2.1 – Proposte legislative in materia

Diversi sono stati i tentativi intrapresi, fino ad oggi, di creare una disciplina unitaria riguardante le intercettazioni la quale comprendesse anche i captatori informatici. In primo luogo bisogna prendere in considerazione il d.l. 18 febbraio 2015, n. 7, recante "*Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione"*, convertito successivamente in legge grazie alla legge di conversione 17 aprile 2015, n. 43[102]. Si era presa infatti in considerazione la possibilità, tramite il sopra citato decreto legge, di inserire all'interno dell'art. 266-*bis* c.p.p. relativo quindi alle intercettazioni informatiche, la possibilità di eseguire le intercettazioni menzionate dall'articolo anche «attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico». La proposta di modifica tuttavia riscontrò non poche opinioni negative, soprattutto da parte dell'opinione pubblica[103], la quale diffidava dal fatto che la disciplina di tali e peculiari tipi di intercettazioni sarebbe stata estesa, grazie alla modifica, a tutte le fattispecie per cui era prevista l'intercettazione "comunemente intesa". La proposta di modifica non fu successivamente approvata in sede di conversione nemmeno dopo la presentazione di un emendamento che, di fatto, ne avrebbe ristretto la portata ai soli reati con finalità di terrorismo. Tentativi simili furono effettuati rispettivamente

[102] D. l. 18 febbraio 2015, n. 7, in *G.U.* del 20 aprile 2015.
[103] Si veda ad esempio, in questo senso, *Il disegno di legge antiterrorismo contiene una norma anticostituzionale*, in Internet al sito http://www.ilpost.it/2015/03/26/disegno-legge-antiterrorismo-trojan-privacy/.

dalle proposte di legge C. 3470 del 2 dicembre 2015[104] e C. 3762 del 20 aprile 2016[105] ma, ad oggi, rimangono privi di esito. In particolare la seconda proposta di legge sopra citata, promossa dal deputato Stefano Quintarelli ed intitolata «Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali», sembra poter ottemperare all'equilibrio tra repressione della criminalità e rispetto di quelle garanzie individuali che possono essere messe a rischio con strumenti tanto invasivi quanto i captatori informatici. Diverse sono le peculiarità di questa precisa proposta di legge[106]:

a) innanzitutto è presente una definizione ben precisa dei reati per i quali sarebbe previsto l'uso dei captatori, estromettendo i reati commessi dai pubblici ufficiali contro la pubblica amministrazione, i delitti informatici e anche l'omicidio, la rapina e l'estorsione, configurando come possibile l'utilizzo di tali strumenti solo per «i procedimenti di criminalità organizzata di stampo mafioso o con finalità di terrorismo»;

b) in secondo luogo, la richiesta di poter utilizzare un captatore a fini intercettivi deve essere redatta dal Pubblico Ministero e convalidata da un giudice, il quale dispone quindi «l'osservazione dei dispositivi installati e l'acquisizione da remoto dei dati contenuti», aggiungendo inoltre che il decreto autorizzativo va notificato all'indagato entro 40 giorni dall'inizio dell'attività captativa del *trojan*;

---

[104] Proposta di legge di iniziativa della deputata Greco del 2 dicembre 2015, in *Atti Camera, XVII legislatura, Disegni di legge e relazioni,* stampato n. 3470.
[105] Proposta di legge di iniziativa dei deputati Quintarelli e Catalano del 20 aprile 2016, in *Atti Camera, XVII legislatura, Progetti di legge,* stampato n. 3762.
[106] C. FREDIANI, *Intercettazioni col trojan, ecco la proposta di legge*, in Internet al sito http://www.lastampa.it/2017/01/31/italia/cronache/intercettazioni-col-trojan-ecco-la-proposta-di-legge-MP8BJ2PB0jCwMt84ofRSlM/pagina.html.

c) la ricerca di determinati *file* sul dispositivo intercettato viene classificata come nuovo mezzo di ricerca della prova, denominato «osservazione e acquisizione da remoto», mentre le intercettazioni del traffico vocale vengono ricondotte all'alveo delle intercettazioni telefoniche e le intercettazioni audio/video a quello delle intercettazioni tra presenti;

d) il giudice deve necessariamente specificare su quali dispositivi il *trojan* può essere installato e «i motivi per i quali è necessaria l'installazione su dispositivi di soggetti non indagati», producendo quindi, con la possibilità di "infettare" dispositivi di soggetti non sottoposti ad indagini, non pochi dubbi sul punto;

e) la necessità dell'esecuzione materiale delle operazioni di intercettazione solo tramite la polizia giudiziaria e non tramite soggetti terzi, quali possono essere società come Area, IPS/Resi o altre che forniscono ed eseguono tali servizi per conto delle procure italiane;

f) il necessario possesso, da parte dei captatori informatici, di determinati requisiti, «requisiti stabiliti con regolamento del Ministro della Giustizia, di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali», prevedendo in particolare un sistema di omologazione dei captatori affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e, allo stesso tempo, la creazione di un Registro Nazionale dei Captatori informatici. Inoltre, si prevede il diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni effettuate con il captatore informatico, dalla sua installazione fino alla sua rimozione, garantendo anche la verifica del codice sorgente per escludere manipolazioni;

g) infine, alla luce degli scandali recenti che hanno visto il coinvolgimento di tali tecnologie, si prevede un inasprimento delle pene per coloro i quali dovessero abusare di detti strumenti.

Tempo addietro, lo stesso Quintarelli, informatico di professione oltre che deputato, aveva parlato così del captatore informatico: «L'uso di captatori informatici (*trojan, keylogger, sniffer,…)* quale mezzo di ricerca delle prove da parte delle Autorità Statali (giudiziarie o di sicurezza) è controverso in tutti i paesi democratici per una ragione tecnica: con quei sistemi viene compiuta una delle operazioni più invasive che lo Stato possa fare nei confronti dei cittadini, poiché quella metodologia è contestualmente una ispezione, una perquisizione, una intercettazione di comunicazioni, una acquisizione occulta di documenti e dati anche personali; tutte attività compiute in un luogo, i sistemi informatici privati, che equivalgono al domicilio. E tutte quelle attività vengono fatte al di fuori delle regole e dei limiti dettate per ognuna di esse dal Codice di Procedura Penale[107]».
L'ultima, in ordine temporale, proposta di legge di cui è necessario far menzione, è il c.d. ddl Orlando, dal nome dell'attuale Ministro della Giustizia, recentemente approvato dal Parlamento, con il quale si sdogana il *Trojan* come strumento di indagine, equiparandolo in linea generale alle intercettazioni. Il provvedimento approvato dal Senato e dalla Camera conferisce al Governo la delega per la riforma in generale del sistema delle intercettazioni, inserendo in quest'ambito anche l'utilizzo dei captatori informatici ma rimanendo tuttavia ancorato alle valutazioni espresse più volte dalla Suprema Corte di Cassazione in tema. In particolare, il Governo dovrà osservare i seguenti parametri[108]:

[107] M. NASI, *Decreto antiterrorismo, bocciato il trojan di stato*, in Internet al sito https://www.ilsoftware.it/articoli.asp?tag=Decreto-antiterrorismo-bocciato-il-trojan-di-Stato_12033.
[108] C. PARODI, Procura della Repubblica di Torino, *La riforma "Orlando": la delega in tema di "captatori informatici"*, in Internet al sito

a) la necessaria presenza del decreto autorizzativo da parte del giudice, il quale dovrà indicare le ragioni per le quali si rende necessario lo strumento del *trojan* per lo sviluppo delle indagini;

b) l'attivazione del microfono può avvenire e deve avvenire solo in conseguenza di apposito comando inviato da remoto e non con il semplice inserimento del captatore nel dispositivo intercettato;

c) la registrazione audio deve essere avviata dalla polizia giudiziaria o dal personale incaricato secondo circostanze da riportare nel verbale descrittivo delle modalità di effettuazione delle operazioni;

d) l'attivazione del dispositivo è sempre ammessa nel caso in cui si proceda per i delitti di criminalità organizzata e, fuori da tali casi, nei luoghi domiciliari solo nel caso in cui sia in corso un'attività criminosa, sempre nel rispetto dei limiti imposti per le intercettazioni telefoniche;

e) il trasferimento delle registrazioni è effettuato unicamente verso il *server* della Procura;

f) al termine delle registrazioni il captatore informatico deve essere disattivato e reso inutilizzabile in maniera definitiva;

g) la presenza di requisiti tecnici che descrivono quali captatori informatici possono essere utilizzati legittimamente;

h) in caso di concrete situazioni d'urgenza, il Pubblico Ministero può disporre l'utilizzo dei captatori informatici per delitti di criminalità

---

http://www.magistraturaindipendente.it/la-riforma-orlando-la-delega-in-tema-di-captatori-informatici.htm.

organizzata con successiva convalida da parte del giudice entro il termine massimo di 48 ore;

i) i risultati ottenuti dalle intercettazioni possono essere utilizzati a fini probatori soltanto nei reati ad oggetto del provvedimento autorizzativo e possono essere utilizzati in procedimenti diversi a condizione che siano del tutto indispensabili per l'accertamento dei delitti per i quali risulta la previsione dell'arresto obbligatorio in flagranza (*ex* art. 380 c.p.p.);

l) in ultimo, non possono essere in alcun modo conosciuti o conoscibili, divulgabili e pubblicabili i risultati di intercettazioni che abbiano coinvolto, anche solo occasionalmente, soggetti terzi alle indagini ovvero soggetti estranei ai fatti per cui si procede.

Il disegno di legge "Orlando", con la possibilità di una riforma ampia della giustizia penale, sembrerebbe quindi essere un'occasione imperdibile per poter essere in grado di avere una disciplina chiara e univoca sul tema dei captatori informatici, in modo da poter avere una normativa *ad hoc* che sia in grado di bilanciare da un lato l'esigenza di combattere la criminalità, anche con mezzi tecnologicamente più avanzati e, dall'altro lato, che garantisca al contempo il rispetto dei diritti umani garantiti dalla Costituzione, dalla CEDU e dalla Carta dei diritti fondamentali dell'Unione Europea. Invece, agli articoli 82 e 84, n. 5, lett. e), del ddl., si prevede di disciplinare «le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili», eliminando così la prospettiva di una normativa *ad hoc* e lasciando tale compito, per ora, alla sola proposta di legge avanzata dal deputato Quintarelli[109].

[109] M. SENOR, Centro Studi Processo Telematico, *Trojan di Stato: perché serve una base giuridica adeguata*, in Internet al sito

# 3 – Ambito di applicazione

La consapevolezza delle enormi potenzialità dello strumento del captatore informatico è stata acquisita solo gradualmente, poiché sia in dottrina che in giurisprudenza si sono succeduti nel tempo diversi orientamenti, volti ad analizzare il fenomeno pian piano nella sua totalità[110]. Riguardo a questo, è opportuno partire da una distinzione di natura tecnica tra la *on line search* e la *on line surveillance*. Alla prima categoria fanno capo infatti tutti quei programmi spia che consentono di produrre copia, totale o anche parziale, delle unità di memoria del sistema informatico bersaglio di tali programmi: in un secondo momento, le informazioni e i dati vengono trasmessi, ad intervalli regolari o stabili previamente, agli organi investigativi tramite la rete Internet e per mezzo di modalità del tutto occulte e protette (il fenomeno è conosciuto come la *one-timecopy* dei dati digitali presenti in un sistema informatico in un determinato momento). Per quanto riguarda questa prima categoria, tramite l'unico precedente giurisprudenziale edito[111], la giurisprudenza ha ricondotto tale figura a quella della prova atipica, per questo sottratta alla disciplina prescritta dagli artt. 266 e ss. c.p.p., ma allo stesso modo utilizzabile processualmente sulla base di un semplice decreto autorizzativo emanato dal Pubblico Ministero. Nel caso di specie, l'attività autorizzata dal Pubblico Ministero, consistente nell'estrarre e produrre copia di documenti memorizzati sull' *hard disk* del *computer* in uso all'imputato, aveva avuto ad oggetto non un «flusso di comunicazioni», quindi richiedente un dialogo con altri soggetti esterni, ma bensì «una relazione operativa tra microprocessore e video del sistema elettronico», ossia «un flusso

---

https://www.agendadigitale.eu/documenti/trojan-di-stato-perche-serve-una-base-giuridica-adeguata/.

[110] L. MONTEVERDE, *Le nuove "frontiere" delle intercettazioni*, in *Arch. pen.,* 3, 2014.

[111] Cass. sez. V, 14 ottobre 2009, n. 16556/10, Virruso, cit.

unidirezionale di dati» confinati all'interno dei circuiti del *computer* stesso[112].

Per quanto riguarda invece la seconda categoria, la c.d. *on line surveillance*, essa è composta da tutti quei programmi spia che riescono a captare il flusso informativo che intercorre tra le periferiche (quali possono essere video, tastiera, microfono o *webcam*) e il processore del dispositivo intercettato, permettendo in tal modo al centro remoto di controllo di poter monitorare in tempo reale tutto quello che viene visualizzato sullo schermo del dispositivo (*screenshot*), digitato attraverso la tastiera (*keylogger*) o ancora detto attraverso il microfono o visto per mezzo della *webcam* del sistema intercettato[113]. Per quanto riguarda questa particolare modalità, la giurisprudenza di legittimità ha elaborato diversi orientamenti, sostanzialmente tre, che si sono susseguiti tra il 2015 e il 2016, riferiti tutti a rispettivi giudizi *de libertate* relativi a reati di criminalità organizzata, per i quali erano state emesse ordinanze di custodia cautelare fondate essenzialmente su intercettazioni ambientali che avevano fatto uso dei c.d. "agenti intrusori" o virus informatici, installati su alcuni dispositivi in uso agli indagati, permettendo quindi di estrapolare il traffico dati e al contempo anche le conversazioni tra presenti, tramite l'attivazione del microfono e della videocamera dell'apparecchio. Nella prima fase, la giurisprudenza ha ritenuto del tutto infondate le censure relative all'utilizzo di tali provvedimenti coercitivi sia per ragioni di rito, in particolare attinenti alla genericità dei motivi, sia poiché si valorizzavano tutte le implicazioni possibili della specifica disciplina valevole per le intercettazioni nei provvedimenti di criminalità

---

[112] A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea. The "on line surveillance" between Italian criminal trial and European Court of Human Rights*, in *Cass. pen.,* fasc. 5, 2016, p. 2274b.

[113] P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziali e prospettive di riforma*, in *Proc. pen. e giust.*, n. 5, 2016, p. 124.

organizzata. In questo senso si è espressa la Cassazione[114], rigettando o dichiarando inammissibili altrettanti ricorsi *de libertate*, in quanto la Corte osservava che « la censura inerente alla mancanza di motivazione in merito al requisito che nei luoghi di privata dimora, oggetto di intercettazione ambientale, si stesse svolgendo attività criminosa, è infondata, poiché le captazioni sono state disposte, trattandosi di reati in materia di criminalità organizzata, ai sensi dell'art. 13 d.l. 13 maggio 1991, n. 152, conv. con modif., in l. 12 luglio 1991, n. 203, che testualmente prescinde da tale requisito, stabilendo che l'intercettazione di comunicazioni tra presenti è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 c.p. si sita svolgendo attività criminosa». Durante una seconda fase, la giurisprudenza ha ritenuto invece fondate censure del tutto simili a quelle confutate nella prima fase, sulla base del duplice assunto che il decreto autorizzativo delle intercettazioni ambientali dovrebbe individuare con precisione, a pena di inutilizzabilità, i luoghi nei quali esse dovranno avvenire, e che tutte le captazioni effettuate al di fuori di tali luoghi siano pertanto inutilizzabili in sede processuale. Nel dettaglio, la Cassazione ha ritenuto che l'intercettazione di conversazioni tramite il c.d. virus informatico, installato nell'apparecchio telefonico (nel caso di specie uno *smartphone*) dell'indagato, dia luogo ad un'intercettazione di tipo ambientale, disciplinata quindi dall'art. 266, comma 2, c.p.p., la quale potrà dirsi legittima solo quando il decreto autorizzativo abbia individuato in precedenza e con precisione i luoghi in cui detta attività captativa verrà espletata[115]. A tale conclusione la Corte è giunta sulla base dell'assunto legato totalmente ad una «corretta ermeneutica della norma di cui all'art. 15 Cost., la quale osterebbe all'attribuzione al disposto dell'art. 266, comma 2, c.p.p. di una latitudine operativa così ampia da ricomprendere

[114] Cass. sez. VI, 12 marzo 2015, n. 24237, Maglia, inedita.
[115] Cass. sez. VI, 26 maggio 2015, n. 27100, Musumeci, in *C.E.D. Cass.,* n. 265654.

intercettazioni ambientali effettuate in qualunque luogo». L'ultima fase, la terza, si è aperta di recente ed è destinata a concludersi molto probabilmente davanti alle Sezioni Unite, con la rimessione di tre questioni:

a) se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione;

b) se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano nei luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, c.p.p.;

c) se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo del virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.

Anche in questo caso, le Sezioni unite hanno risolto la questione, chiarendo che anche nei luoghi di privata dimora, ossia quelli *ex* art. 614 c.p., pure non singolarmente individuati o precisati e anche se ivi non si stia svolgendo l'attività criminosa, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispositivi elettronici portatili[116]. Si tornerà su questa sentenza varie volte, e in modo molto più approfondito, nel corso della trattazione in quanto rappresenta il punto di snodo per la disciplina dei captatori informatici.

[116] Cass. sez. un., 28 aprile 2016, Scurato, n. 26889, in *Dir. pen. cont.,* 4 luglio 2016, p. 22, in Internet al sito www.penalecontemporaneo.it.

Il nodo centrale, ricorrente in tutte le tre fasi sopra analizzate e perorate di volta in volta dalla giurisprudenza di legittimità, è l'utilizzo di tali strumenti informatici ad uso intercettivo nei procedimenti per criminalità organizzata. E' quindi fondamentale, ai fini di una comprensione più ampia del fenomeno in questione, la disamina del concetto stesso di criminalità organizzata così come elaborato dalla dottrina e dalla giurisprudenza.

## 3.1 – Definizione di "delitti di criminalità organizzata"

La nozione di "criminalità organizzata" è stata introdotta in Italia intorno alla metà degli anni settanta del secolo scorso, in relazione specialmente ai fenomeni di sequestri di persona e di diffusione degli stupefacenti e dei primi gruppi terroristici. Venne introdotta per la prima volta nell'ordinamento italiano dalla c.d. normativa antimafia e, nella sua originale formulazione, l'art. 1 della legge 31 maggio 1965, n. 575 ("disposizioni contro la mafia") stabiliva che la legge medesima dovesse essere applicata «agli indiziati di appartenere ad associazioni mafiose», senza tuttavia fornire un concetto preciso dal punto di vista normativo di associazione mafiosa, ma di fatto richiamando *per relationem* un concetto di matrice puramente sociologica. La prima comparsa del termine "criminalità organizzata" si ha con l'art. 14 del decreto legge 15 dicembre 1979, n. 625, modificato poi dall'articolo unico della legge di conversione 6 febbraio 1980, n. 15. La disposizione che può essere utilizzata come capofila del concetto di criminalità organizzata, secondo la normativa attuale, è quella fornita dall'articolo 13 della legge 19 marzo 1990, n. 55[117], che inserisce all'interno dell'art. 30-*ter* dell'Ordinamento Penitenziario il comma 1-*bis*, con cui si dispone che «per i condannati per i

[117] Nuove disposizioni per la prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale.

reati commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale, di criminalità organizzata, nonché per il reato indicato nell'articolo 630 del codice penale, devono essere acquisiti elementi tali da escludere l'attualità dei collegamenti con la criminalità organizzata». L'anno seguente viene poi introdotto il d.l. 13 maggio 1991, n. 152[118], con il quale – come si vedrà nel corso della trattazione – si introducono alcune norme di fondamentale importanza per la specifica materia. Anche il codice di rito prevede alcune fattispecie riconducibili a tale materia: l'art. 54-*ter* c.p.p., la cui rubrica recita «contrasti tra pubblici ministeri in materia di criminalità organizzata», l'art. 274, lett. c, c.p.p., in tema di esigenze cautelari, l'art. 371-*bis*, comma 3, lett. c, c.p.p., relativo alle prerogative del Procuratore nazionale antimafia o ancora l'art. 132-bis, disp. att. c.p.p., relativo alle priorità per la formazione dei ruoli di udienza e trattazione del processo. Tuttavia, nonostante il costante riferimento normativo al concetto di criminalità organizzata, nessuna delle norme in esame rinvia ad un concetto esplicito del fenomeno in questione. Questa carenza è stata arginata sia da parte della dottrina che da parte della giurisprudenza.

Per quanto riguarda la giurisprudenza, la Corte Suprema, analizzando il sopra citato d.l. 13 maggio 1991, n. 152, ha adottato due orientamenti, tra di loro opposti: talora ha applicato il concetto in modo estensivo, in senso criminologico e teleologico, con riguardo cioè alle finalità della norma speciale, la quale tenderebbe a far rientrare nel suo ambito applicativo le attività criminose più disparate, purché realizzate da una pluralità di soggetti che abbiano costituito un apparato organizzativo per commettere detti reati (interpretazione di tipo finalistico); dall'altro lato, talvolta essa viene interpretata in modo molto più rigido ed

[118] Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa.

ordinamentale, per mezzo dell'analitica individuazione delle fattispecie criminose, attraverso la selezione tramite la tecnica di normazione "per cataloghi", nel rispetto del principio di legalità e di tassatività nonché delle garanzie concesse a tutela della libertà personale dell'imputato (interpretazione di tipo tassativo)[119]. Prendendo ad esempio questa seconda impostazione dettata dalla Suprema Corte, cioè l'interpretazione di tipo tassativo, rientra in questo caso l'art. 51, comma 3-*bis* c.p.p. contiene un elenco di delitti che, utilizzando anche il richiamo al termine «criminalità organizzata» operato dall'art. 54-*ter* c.p.p., vengono comunemente considerati di criminalità organizzata in senso stretto. Essi definiscono infatti l'ambito di operatività delle DDA (Direzioni distrettuali antimafia) e, per effetto del rinvio dell'art. 371-*bis* c.p.p., anche l'attività di coordinamento rispetto alla Direzione nazionale antimafia[120]. Tuttavia è solo con la pronuncia delle Sezioni Unite del 2005[121] che la giurisprudenza di legittimità è giunta finalmente ad una definizione, estensiva, del concetto di criminalità organizzata. La Corte ha stabilito infatti che «ai fini dell'art. 240-*bis*, comma 2, disp. coord. cod. proc. pen., che prevede l'esclusione, operante anche per i termini di impugnazione dei provvedimenti in materia di cautela personale, della sospensione feriale dei termini delle indagini preliminari nei procedimenti per i reati di criminalità organizzata, quest'ultima nozione identifica non solo i reati di criminalità mafiosa e assimilata, oltre i delitti associativi previsti da norme incriminatrici speciali, ma anche qualsiasi tipo di associazione per delinquere, *ex* art. 416 c.p., correlata alle attività criminose più diverse,

---

[119] Cass. sez. un., 22 marzo 2005, n. 17706, Petrarca, con nota di F. DI CAMILLO, *L'ambito di operatività della nozione normativa di "criminalità organizzata"*, in Internet al sito http://www.altalex.com/documents/news/2005/12/12/l-ambito-di-operativita-della-nozione-normativa-di-criminalita-organizzata.

[120] F. DE LEO, *Pubblico Ministero*, in *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, di G. Lattanzi e E. Lupo, vol. I, Giuffrè, 2008, p. 493.

[121] Cass. sez. un., 22 marzo 2005, n. 17706, Petrarca, in *Cass. pen.,* 2005, p. 2916.

con l'esclusione del mero concorso di persone nel reato, nel quale manca il requisito dell'organizzazione». Nonostante quindi la mancanza di un esplicito riferimento legislativo sul tema, da un punto di vista prettamente giurisprudenziale si può ricavare una nozione utile a chiarificare il concetto in esame.

Per quanto riguarda la dottrina invece, da un lato si è ritenuto, in una chiave di lettura più socio-criminologica che penalistica, che non ci fosse nessuna coincidenza tra la nozione di criminalità organizzata e quella di semplice attività criminosa realizzata in forma associativa e volta a realizzare profitti economici di qualsiasi entità, affermando che deve necessariamente sussistere un elemento ulteriore costituito da una struttura organizzativa munita di complessità tali da farle assumere un valore in concreto preminente rispetto al contributo offerto dai singoli associati. Il tutto deve poi concretizzarsi in una significativa dimensione organizzativa, in una gestione delle attività illecite e del reinvestimento dei profitti scaturenti da tali attività ispirata a criteri di imprenditorialità, nonché nell'utilizzo di mezzi violenti al fine di acquisire posizioni favorevoli di preminenza o addirittura di monopolio nel settore, nel ricorso alla corruzione delle forze di polizia, del potere giudiziario o di quello amministrativo e, infine, alla intimidazione per sopprimere l'applicazione delle leggi e per ottenere decisioni politiche favorevoli agli scopi dell'associazione[122]. D'altro canto però, altra parte dell'autorevole dottrina[123], muovendo dalla necessità di fissare con precisione l'ambito di applicazione della nozione di criminalità organizzata, ha affermato di poter distinguere, a fronte di un'unica categoria generale, due sotto-categorie: quella dei c.d. «reati di criminalità organizzata in senso stretto, che si

[122] G. FIANDACA, *Criminalità organizzata e controllo penale*, in *Indice pen.,* 1991, pp. 5 e ss.
[123] G. CONSO, *La criminalità organizzata nel linguaggio legislativo*, in *Giust. pen.,* 1992, vol. III, pp. 385 e ss.

identificherebbero nei c.d. «reati distrettuali» previsti dall'art. 51, comma 3-*bis,* c.p.p., e quella dei c.d. «reati di criminalità in senso lato», facendo riferimento in questo caso a quelli già previsti dall'art. 407, comma 2, lett. a, c.p.p., prima della modifica apportata a tale norma dall'art. 6 del d.l. 8 giugno 1992, n. 306, tra i quali si possono annoverare gli artt. 270-*bis*, 285, 286, 289-*bis*, 305, 306 e 416, nei quali è previsto l'arresto obbligatorio in flagranza[124].

In ultimo è utile citare anche il testo definitivo dell'art. 8 della legge che contiene "Disposizioni per confermare il diritto interno alla legge quadro 2002/584/GAI del Consiglio dell'Unione Europea, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri", il quale, nell'individuare i casi di consegna obbligatoria, richiama un riferimento generico alla condotta «di partecipare ad un'associazione di tre o più persone finalizzata alla commissione di più delitti[125]».

## 3.2 – Disciplina derogatoria del d.l. 152/1991

Il 13 maggio 1991, in epoca di piena "emergenza mafiosa", viene approvato in parlamento il d.l. 13 maggio 1991, n. 152, successivamente convertito in legge tramite la legge di conversione n. 203/1991[126], recante "provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e di buon andamento dell'attività amministrativa". Il decreto legge in questione introduce nuove disposizioni volte ad inasprire il

[124] In questo senso vedasi G. BORRELLI, *Dei delitti in particolare*, in *Codice penale. Rassegna di giurisprudenza e dottrina*, di G. Lattanzi e E. Lupo, vol. 9, Giuffrè, 2008, pp. 137-138.
[125] Art. 8, Legge 22 Aprile 2005, n. 69, pubblicata in *Gazzetta Ufficiale*, n. 98, 29 aprile 2005.
[126] Decreto legge 13 maggio 1991, n. 152, pubblicato in *Gazzetta Ufficiale*, n. 110, 13 maggio 1991.

trattamento per i delitti connessi alle associazioni di stampo mafioso (vedasi ad es. la circostanza ad effetto speciale disciplinata dall'art. 7 del sopra citato d.l. con lo scopo di sanzionare più gravemente tutte quelle condotte «contigue», penalmente rilevanti, di «manifesta criminosità», ma connotate da una particolare inefferrabilità[127]) e offre inoltre uno spunto di riflessione in tema di intercettazioni con l'introduzione dell'art. 13 il quale, al primo comma, dispone testualmente: «In deroga a quanto disposto dall'articolo 267 del codice di procedura penale, l'autorizzazione a disporre le operazioni previste dall'articolo 266 dello stesso codice è data, con decreto motivato, quando l'intercettazione è necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistano sufficienti indizi. Nella valutazione dei sufficienti indizi si applica l'articolo 203 del codice di procedura penale. Quando si tratta di intercettazione di comunicazione tra presenti disposta in un procedimento relativo ad un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa».

Il primo dato che viene subito in risalto è il concetto di «sufficienti indizi». La povertà semantica del legislatore nel novellare le norme risulta ancor più evidente se si prende in considerazione il concetto di "partecipazione" all'associazione criminosa, il quale secondo il tenore della norma, consente che vengano disposte indagini assai invasive della *privacy* dell'individuo, a mezzo di intercettazioni telefoniche e ambientali, sulla base di una soglia indiziaria di fatto molto bassa, come cristallizzato dalla formula «sufficienti indizi», la quale è intesa relativamente al sospetto di connessioni di qualunque tipo con altri soggetti indiziati di essere implicati in attività criminali, o ancora sospettati di essere coinvolti anche solo in attività

[127] E. RECCIA, *L'aggravante ex art. 7 d.l. 152 del 13 maggio 1991: una sintesi di "inafferrabilità del penalmente rilevante"*, in *Dir. pen. cont.,* n. 2/2015, p. 251.

preparatorie di reati che verranno presumibilmente commessi in futuro. Risulta evidente in questi casi il rischio, non puramente teorico, di colpire con misure restrittive della libertà personale soggetti che abbiano solamente espresso – in conversazioni prontamente captate dagli inquirenti – propositi criminosi da realizzarsi successivamente con altri soggetti, senza necessità che alle parole sia poi susseguita fattualmente una condotta tale da implicare una concreta realizzazione di detti propositi[128].

Il secondo dato importante da sottolineare è il terzo periodo dell'art. 13 del d.l. 152/1991, periodo nel quale il legislatore inserisce una disciplina derogatoria relativamente all'articolo 266, comma 2, c.p.p. Così facendo il legislatore ha di fatto autorizzato, per i delitti di criminalità organizzata, la disposizione e l'utilizzo delle intercettazioni tra presenti anche nei luoghi di privata dimora individuati dall'art. 614 c.p. non più a condizione che vi siano «fondati motivi di ritenere che ivi si stia svolgendo l'attività criminosa», bensì «anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa». Tempo addietro si era già espressa la Corte Costituzionale in merito[129], dichiarando che non è possibile invocare automaticamente una violazione della libertà del domicilio ogni qual volta il mezzo utilizzato non sia già previsto a livello legislativo, in quanto diventato disponibile «solo per effetto dei progressi tecnici successivi». In quest'ottica la Suprema Corte si era espressa con una posizione molto garantista e palesemente in contrasto con quanto espresso dalla Corte Costituzionale per tramite della nota sentenza "Musumeci"[130], tramite la quale la Suprema Corte aveva sancito l'inutilizzabilità delle intercettazioni captate tramite l'utilizzo di un

[128] F. VIGANO', *Oltre l'art. 416-bis: qualche riflessione sull'associazione con finalità di terrorismo*, in *Scenari di mafia. Orizzonte criminologico e innovazioni normative*, di G. Fiandaca e C. Visconti, Giappichelli Editore, Torino, 2010, p. 177.

[129] C. cost., sent. 11 aprile 2002, n. 135, in *Giur. Cost.,* 2002, pp. 1062 e ss.

[130] Cass. sez. IV, 26 maggio 2015, Musumeci, n. 27100, cit., n. 265654.

captatore informatico in quanto erano state assunte al di fuori dei luoghi espressamente autorizzati nel relativo decreto di autorizzazione disposto dal Pubblico Ministero, con un interessamento di quei luoghi previsti dall'art. 614 c.p. La questione, in sé delicata e di difficile interpretazione, è stata riproposta recentemente alle stesse Sezioni Unite, le quali si sono pronunciate sul tema con la sentenza "Scurato"[131], mettendo innanzitutto in rilievo come la citata sentenza "Musumeci" abbia totalmente tralasciato di considerare che, nel caso di specie, potesse essere applicata la normativa derogatoria prevista dall'art. 13 d.l. 11 maggio 1991, n. 152, ritenendo quindi l'intercettazione legittimamente disposta anche qualora non fossero presenti motivi per cui si possa ritenere che nei luoghi di privata dimora si stia svolgendo attività criminosa. La Corte specifica quindi che nell'ambito delle intercettazioni tra presenti, anche a mezzo di captatore informatico, grazie alla disciplina derogatoria richiamata poc'anzi e purché si rimanga nel suo ambito di applicazione, sia possibile disporre dette intercettazioni a prescindere dai luoghi in cui esse verranno poi sviluppate, consentendo esplicitamente allo Stato di utilizzare «tutti i mezzi che la moderna tecnologia offre». La Corte rileva inoltre che il legislatore ha già operato di per sé un bilanciamento degli interessi in gioco tutelati, «optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio tenendo conto della eccezionale gravità e pericolosità […] delle minacce che derivano alla società ed ai singoli delle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di notevoli risorse finanziarie».

Viene così valorizzata oltremisura una disciplina derogatoria, introducendo una deroga dal particolare al generale che rischia di essere utilizzata in maniera troppo ampia, in quanto non esiste nel panorama normativo italiano una nozione di «criminalità organizzata», risultando quindi difficile pensare su cosa debba andare a basarsi il giudice delle indagini preliminari

[131] Cass. sez. un., 28 aprile 2016, Scurato, n. 26889, cit., 4 luglio 2016, p. 22, in Internet al sito www.penalecontemporaneo.it.

nel momento in cui si trovi davanti a delle informazioni acquisite dagli investigatori in forza di fatti connessi a delitti di criminalità organizzata. Va ricordato tuttavia, che all'epoca dell'emanazione di tale disciplina derogatoria, non solo non esistevano i virus informatici *trojan* così come non esistevano nemmeno dispositivi elettronici quali *smartphone, tablet, computer,* ecc., ma non era nemmeno immaginabile da parte del legislatore dell'epoca un mutamento tecnologico così profondo. In sostanza quindi, la pronuncia della Suprema Corte, appare come un intervento riparatore, così come se ne sono susseguiti tanti da parte della giurisprudenza di legittimità, volto a non "far saltare il banco" dichiarando inutilizzabili le intercettazioni effettuate tramite captazione informatica[132]. Resta tuttavia una questione non facile da dirimere, visto da un lato l'avanzare di nuove tecnologie utilizzabili sia da parte dello Stato che da parte della criminalità, e dall'altro l'esigenza di ottemperare costantemente un bilanciamento degli interessi in gioco da parte sia del legislatore che dalla giurisprudenza di legittimità, con la possibilità di sfociare in contrasti palesi e non occasionali tra pronunce della Suprema Corte stessa.

[132] In questo senso G. PERROTTA, *Ratio Legis*, n. 4, Primiceri Editore, 2016, pp. 181 e ss.

# Capitolo 3

# Presupposti per l'utilizzo del virus *trojan*

SOMMARIO: 1 – La sentenza "Scurato": utilizzo dei captatori nei soli procedimenti di criminalità organizzata. – 1.1 – Le motivazioni della Corte. – 1.2 – Principali obiezioni. – 2 – La funzione di garanzia del decreto di autorizzazione. – 2.1 – Requisiti del decreto di autorizzazione. – 2.2 – I presupposti dell'intercettazione – 2.3 – Le modalità di esecuzione delle operazioni. – 2.4 – La possibile necessità di molteplici decreti di autorizzazione per un unico captatore.

## 1 – La sentenza "Scurato": utilizzo dei captatori nei soli procedimenti di criminalità organizzata

Nonostante le pronunce di legittimità riguardanti l'utilizzo e l'essenza stessa del captatore informatico siano poche, in quanto risulta essere uno strumento relativamente recente, esse risultano tuttavia alquanto significative. Una delle prime pronunce che si possono ritrovare in materia[133] ha escluso, secondo il ragionamento adottato dai giudici di legittimità, la riconducibilità del captatore informatico a un tipico mezzo di ricerca della prova, collegandolo invece alla categoria delle prove atipiche

[133] Cass. sez. V, 14 ottobre 2009, Virruso, in *Mass. Uff.*, n. 246955.

*ex* art. 189 c.p.p.[134]. Tale classificazione era stata concepita partendo dalla base che l'attività del Pubblico Ministero era consistita nel prelevare e copiare alcuni documenti memorizzati sull' *hard disk* dell'apparecchio in uso all'indagato (nel caso di specie, un *personal computer*) e aveva avuto ad oggetto non un flusso di comunicazioni, ma «una relazione operativa tra microprocessore e video del sistema elettronico», ossia un'attività confinata esclusivamente all'interno del dispositivo. Tecnicamente il p.m. autorizzava tale attività investigativa per mezzo di un decreto di acquisizione di atti, ai sensi dell'art. 234 c.p.p. ma, in realtà, il decreto disponeva l'acquisizione non solo dei *file* già esistenti, ma anche di tutti quei dati che sarebbero stati inseriti successivamente nella memoria rigida del *personal computer*, realizzando così un vero e proprio monitoraggio occulto e continuativo del dispositivo in uso all'indagato. Il giudice dell'abbreviato ritenne processualmente legittima tale attività investigativa, inquadrandola come prova atipica a rigore della disciplina dettata dall'art. 189 c.p.p. In seguito alla richiesta della difesa, in appello, di sussumere la sopra citata attività all'interno della disciplina delle intercettazioni telematiche e quindi di ritenere la prova incostituzionale e inutilizzabile a norma dell'art. 191 c.p.p. per violazione degli artt. 14 e 15 Cost., la Corte di legittimità rispose in maniera negativa. In primo luogo, non si configurava nessuna violazione dell'art. 14 Cost. perché l'apparecchio monitorato non era collocato in un luogo domiciliare o di privata dimora ma nei locali dell'ufficio pubblico comunale; in secondo luogo, non c'era stata alcuna violazione dell'art. 15 Cost. poiché quanto estratto in copia non era un testo inoltrato e trasmesso tramite il sistema informatico, ma bensì soltanto predisposto per essere stampato su supporto cartaceo e consegnato, successivamente, al suo destinatario[135].

[134] S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen.*, n. 1, 2014, pp. 6 e ss.
[135] M. T. ABBAGNALE, *In tema di captatore informatico*, in *Arch. pen.*, n. 2, 2016, pp. 2 e ss.

La scelta di ritenere legittimo il decreto del pubblico ministero di acquisizione, in copia, di tale documentazione informatica è basata sulla circostanza che il provvedimento ha riguardato l'estrapolazione di dati e non un flusso di comunicazioni contenute a priori nel *personal computer* ed è stata successivamente ripresa da un'ulteriore pronuncia, nel c.d. "caso Bisignani"[136]. Con le sentenze "Virruso" e "Bisignani" la Suprema Corte ha quindi affermato che le prove acquisite per il tramite di un captatore informatico rientrassero nella disciplina delle prove atipiche, sottraendole quindi alla normativa prevista dagli artt. 266 e ss. c.p.p. Tuttavia, con altra decisione del 2015[137], i giudici di legittimità sono ritornati sul punto affermando, al contrario di quanto detto in precedenza, che gli elementi probatori acquisiti tramite l'utilizzo dello strumento del captatore informatico siano da annoverare all'interno della disciplina delle intercettazioni ambientali e che, di conseguenza, esse devono avvenire nei luoghi ben circoscritti ed individuati *ab origine* e non in qualunque luogo il soggetto possa trovarsi. Tale posizione ha destato non pochi dubbi in quanto sembrava "pacifico" ritenere l'orientamento precedentemente assunto dalla Corte di Cassazione come quello prevalente. Il momento per poter sciogliere tale dubbio interpretativo non ha tardato a presentarsi e le Sezioni Unite sono state chiamate a pronunciarsi sulla specifica indicazione, nel decreto di autorizzazione, dei luoghi ove deve essere effettuata l'intercettazione, in mancanza del quale tale decreto sarebbe colpito da illegittimità e, di conseguenza, i risultati probatori da inutilizzabilità. Occorre ricordare tuttavia che, sullo stesso tema, si era pronunciata anche la Corte Europea dei Diritti dell'Uomo[138], esigendo il requisito della prevedibilità delle misure segrete di sorveglianza, come le

[136] Cass. sez. VI, 27 novembre 2012, Bisignani, in *Mass. Uff.*, n. 254865.
[137] Cass. sez. VI, 26 maggio 2015, Musumeci, in *Guida dir.*, n. 41, 2015, p. 83.
[138] C. eur, 10 febbraio 2009, Iordachi c. Moldavia, in *Cass. pen.*, 2009, p. 4021.

intercettazioni di comunicazioni[139].

La *quaestio* sollevata si fondava sull'illegittimità di un'ordinanza cautelare da parte del Tribunale di Palermo (per associazione a delinquere di stampo mafioso ed estorsione) basata su intercettazioni effettuate mediante l'utilizzo di un virus *trojan*[140]. I motivi di doglianza della difesa si riferiscono a due ambiti: da una parte al decreto emanato dal p.m. che avrebbe reso attuabile l'operazione intercettiva anche nella dimora privata senza specificare l'attualità dell'azione criminale svoltasi in quel luogo; dall'altra esse evidenziano come l'eccessiva genericità del provvedimento in esame abbia reso possibile un accesso alle comunicazioni in qualsiasi luogo la persona si trovasse. A sostegno di tali argomentazioni difensive era stato richiamato un passo della sentenza "Musumeci" secondo la quale «l'intercettazione da remoto delle conversazioni tra presenti – con l'attivazione, tramite il c.d. "agente intrusore informatico" del microfono di un apparecchio telefonico *smartphone* – può ritenersi legittima solo se il relativo decreto autorizzativo individui con precisione i luoghi in cui eseguire tale attività captativa». La stessa Cassazione VI penale, assegnataria di tale ricorso, ha ritenuto di chiedere il parere delle Sezioni Unite sul tema, esponendo in particolare tre dubbi interpretativi, tramite la seguente ordinanza[141]: «La sesta Sezione della Corte di Cassazione ha deciso di rimettere la seguente questione alle Sezioni Unite:

- se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la captazione;

---

[139] In questo senso, L. FILIPPI, *Il captatore informatico: l'intercettazione ubicumque al vaglio delle Sezioni Unite*, in *Arch. pen.*, 2016, n. 1.
[140] G. CORRIAS LUCENTE, *La nuova frontiera delle intercettazioni. I Troyan Horse e le libertà fondamentali. L'appello delle Sezioni Unite*, in *Law and Media Working Paper Series*, n.10/2016, pp. 3 e ss.
[141] Cass. sez. VI, (ord.) 6 aprile 2016, Scurato, in *Arch. pen.*, al sito http://www.archiviopenale.it/.

- se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengono in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, c.p.p.;

- se invece il decreto possa comunque prescindere da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata».

E' utile citare anche i passaggi salienti della memoria depositata per l'occasione dalla Procura generale presso la Corte di Cassazione, vista l'autorevolezza della fonte e la qualità delle argomentazioni riportate[142]. La prima considerazione è puramente metagiuridica, in quanto il PG constata la particolare velocità dei progressi tecnologici in tema di captazione e, in parallelo, di quelli volti all'elusione della captazione, traendo da ciò il convincimento che l'impiego di tali virus informatici, più che al potenziamento dell'apparato intercettivo, serva più a recuperare l'efficacia perduta o compromessa delle tecniche tradizionalmente adottate. In secondo luogo, durante la disamina delle caratteristiche tecniche del virus *trojan*, la memoria del PG giunge alla conclusione che, se è vero da un lato che questo mezzo consente una molteplicità di funzioni, è vero allo stesso tempo che questa stessa molteplicità consente, alla legge e al diritto, di apporre dei limiti tecnici preventivi al suo utilizzo. Il passaggio successivo riguarda la legittimità dell'uso di tale strumento nei procedimenti per delitti di criminalità organizzata, sottolineando in particolare che, da un lato è sbagliato qualsiasi ragionamento che, assumendo gli ambienti determinati come parametri ineludibili di riferimento, neghi legittimazione ad intercettazioni tra presenti che possano prescindere dai parametri medesimi, dall'altro la sentenza n.

[142] V. GIGLIO, *I virus informatici per scopi intercettivi nei procedimenti di criminalità organizzata: mezzi di cura o agenti patogeni?*, in Internet al sito https://www.filodiritto.com/.

27100/2015, "Musumeci", ha omesso di considerare la disciplina derogatoria stabilita dall'art. 13 del Decreto Legge 152/1991. Queste pecche motivazionali, a parere del PG, hanno portato la sentenza citata a discostarsi dalla consolidata giurisprudenza precedente che aveva richiesto l'indicazione specifica a priori dei luoghi dell'attività intercettiva solo per le intercettazioni disposte per i procedimenti ordinari. Dopo questo punto, il PG esamina i problemi, peculiari, posti in essere dall'utilizzo del captatore informatico, essendo comunque dell'avviso che le norme vigenti consentano senza ombra di dubbio e senza alcuna eccezione le intercettazioni foniche a mezzo di virus informatico nei procedimenti che si occupano di criminalità organizzata. Presupposto logico di tale ragionamento è che il legislatore, con la disciplina emanata nel 1991, abbia effettuato un adeguato bilanciamento degli interessi in campo, sacrificando "quanto basta" le garanzie costituzionalmente assicurate ad ogni individuo, a fronte della repressione dell'azione criminosa. Nel punto successivo il PG ha escluso categoricamente che lo strumento di indagine qui esaminato possa confliggere in qualsiasi modo con i precetti costituzionali stabiliti agli artt. 14 e 15 Cost, in quanto per il primo valgono i principi affermati dalla Consulta nella sentenza n. 135/2002[143], secondo i quali è esclusa l'esistenza di un divieto costituzionale assoluto alla captazione di immagini in luoghi di privata dimora, mentre per il secondo, il precetto in esso contenuto risulta soddisfatto con l'emissione di un atto motivato dall'autorità giudiziaria che sia rispondente alla normativa vigente. Allo stesso modo, a parere del PG, non sussiste nessuna violazione dell'articolo 8 CEDU, richiamando in particolare la sentenza emessa il 4 dicembre 2015 dalla Corte EDU nel caso *Zakharov* c. Russia[144], la quale contiene una sorta di decalogo dei requisiti essenziali per rendere conformi all'articolo 8 le intercettazioni.

[143] C. cost., 24 aprile 2002, n. 135, in *Giur. cost.,* 2002, pp. 1062 e ss.
[144] C. eur., 4 dicembre 2015, Zakharov c. Russia, n. 47143/06.

Dal canto loro le Sezioni unite, a brevissima distanza di tempo, precisamente il 28 aprile 2016, si sono pronunciate sulla questione. Rigettando il ricorso dell'indagato, esse hanno confermato la corrente interpretativa inaugurata dalla Sezione VI della Cassazione, la Sezione rimettente, a discapito di quanto affermato precedentemente nel 2015 nella sentenza "Musumeci". Così facendo i giudici di legittimità, intervenendo sul contrasto interpretativo fra due orientamenti sviluppatosi in seno alla stessa Sezione VI e di cui sopra ampiamente discusso, avallano ufficialmente l'ingresso, all'interno del nostro ordinamento, dei captatori informatici "polivalenti" come strumenti di indagine penale, in particolare per le indagini relative ai procedimenti per delitti di criminalità organizzata[145].

## 1.1 – Le motivazioni della Corte

Tramite la sentenza pronunciata il 28 aprile 2016, le Sezioni Unite hanno quindi posto un punto fermo, aprendo all'impiego dello strumento del captatore informatico per la realizzazione di intercettazioni tra presenti nei soli procedimenti per i delitti di criminalità organizzata, trovando applicazione in questi casi la disciplina derogatoria dettata dall'articolo 13 del decreto legge n. 152 del 1991, il quale, derogando ai principi dettati dall'art. 266, comma 2, c.p.p., consente la captazione nei luoghi di privata dimora, senza necessità di indicazione preventiva di tali luoghi e senza il necessario requisito dello svolgersi ivi di un'attività criminosa[146]. Le

[145] G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni fra presenti*, in Internet al sito http://www.penalecontemporaneo.it/.
[146] In questo senso vedasi, A. CAMON, *Cavalli di troia in Cassazione*, nota a sent. Cass. sez. un., 28 aprile 2016, Scurato, n. 26889, in *Arch. nuova proc. pen.,* 2017, pp. 76 e ss; nota di A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, pp. 2274-2288; nota di G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzie di riservatezza, esigenze di sicurezza collettiva e di funzionalità del*

Sezioni Unite, approfondendo e allo stesso tempo correggendo alcuni spunti tratti dall'ordinanza di rimessione, adottano quindi un'interpretazione equilibrata, che salvaguarda la possibilità di utilizzare uno strumento di investigazione particolarmente efficace. Il ragionamento seguito dai giudici di legittimità si articola in diverse fasi, volte ad argomentare nel modo più completo possibile la soluzione adottata. All'inizio le Sezioni Unite, dopo aver descritto lo strumento informatico e le proposte di legge ad esso collegate, intraprendono una disamina accurata e correlata strettamente al diritto positivo in modo da poter colmare le lacune della sentenza "Musumeci". In primo luogo precisano opportunamente che il termine "intercettazione ambientale" non esiste nell'ordinamento vigente, nel quale l'esclusivo riferimento è quello relativo alle "intercettazioni fra presenti", slegando quindi con questo assunto il luogo dal mezzo di prova. Successivamente passano ad analizzare la disciplina codicistica, in particolare l'art. 266 del codice di procedura penale. Affermano, innanzitutto, che il primo comma del sopra citato articolo esclude la necessità che il decreto autorizzativo emanato dal p.m. indichi preventivamente i luoghi dove l'intercettazione dovrà prendere piede. A conclusione opposta, tuttavia, le Sezioni Unite giungono nel mentre analizzano il secondo comma dell'art. 266. La Corte perviene, quindi, ad escludere che la norma citata consenta l'utilizzo dei virus *trojan* per le intercettazioni, con quattro passaggi argomentativi che si possono così sintetizzare:

a) è condizione imprescindibile per le intercettazioni in luoghi di privata dimora il fatto che sia presente il concreto sospetto che ivi si stia svolgendo attività criminosa;

---

*sistema delle prove digitali*, in *Il diritto dell'informazione e dell'informatica*, 2016, p. 88; nota di P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.,* 2016, fasc. 5, p. 21.

b) sono imprevedibili e, di conseguenza, non possono essere indicati preventivamente nel decreto autorizzativo i luoghi di privata dimora che l'intercettato avrà a frequentare;

c) premesso che è impossibile materialmente sospendere la captazione al momento dell'ingresso dell'interessato in private dimore, anche qualora lo fosse, sarebbe «impedito il controllo del Giudice al momento dell'autorizzazione»;

d) i captatori informatici, secondo le Sezioni Unite, comportano quindi il rischio elevato di una molteplicità di intercettazioni in luoghi di privata dimora contrario al principio di proporzionalità.

A conferma di quanto sopra esposto, le Sezioni Unite affermano che non sono ammissibili i captatori informatici per le intercettazioni regolate dall'art. 266, c.p.p., visto l'insormontabile ostacolo posto dai luoghi di privata dimora.

Per quanto riguarda invece i procedimenti per i reati di criminalità organizzata, la sentenza "Scurato" giunge tuttavia ad un diverso risultato, evocando una norma, tralasciata dalla sentenza "Musumeci": l'articolo 13 del decreto legge 152/1991. Il ragionamento quindi viene diversificato sul rilievo che la disciplina applicabile risulta essere diversa a seconda che si proceda nell'ambito di procedimento penale per i reati sopra citati o per i c.d. "reati comuni". Secondo le Sezioni Unite infatti, nel momento in cui si proceda ad operazioni di intercettazioni "tra presenti" da svolgersi nei luoghi di privata dimora, per reati di criminalità organizzata, non occorre la preventiva individuazione e indicazione dei luoghi in cui la captazione dovrà essere successivamente espletata, in quanto, stando al tenore della norma sopra richiamata (art. 13 d.l. 152/1991), non è necessario che sussista la condizione del fondato sospetto che nei luoghi di captazione stia avvenendo l'attività criminosa. Da questo assunto, la Corte fa derivare

il principio secondo il quale è legittimo procedere, anche nei luoghi di privata dimora di cui all'art. 614 c.p., ad intercettazioni "tra presenti" a mezzo di captatore informatico installato su un dispositivo portatile, nell'ambito dell'attività investigativa portata avanti nei procedimenti relativi a delitti di criminalità organizzata, a prescindere quindi dalla preventiva individuazione e indicazione nel decreto autorizzativo dei luoghi in cui la captazione dovrà avvenire[147]. E' opportuno ricordare che lo stesso Cordero, nel 1990, ossia prima della riforma del 1991, aveva criticato aspramente la condizione ostativa presente nell'art. 266, comma 2, c.p.p., arrivando a definirla come «un limite discutibile», affermando inoltre che «oltre date soglie il garantismo diventa feticcio, utile alle culture ed economie del delitto. Sarebbe ragionevole che nei casi più gravi l'autorizzazione fosse concessa sugli stessi presupposti definiti dall'art. 267 (ossia i gravi indizi di reato e l'indispensabilità del mezzo dell'intercettazione)[148]». La pronuncia si fa carico, nei passaggi conclusivi, della giustificazione costituzionale della disciplina ricavata dalla stessa. La Corte afferma infatti che «Le minacce che derivano alla società e ai singoli dalle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di notevoli risorse finanziarie – e oggi, anche dalla crescente diffusione ed articolazione su scala mondiale delle organizzazioni terroristiche le cui azioni sono finalizzate ad attentare alla vita ed alle libertà delle persone ed alla sicurezza collettiva – richiedono una forte risposta dello Stato con tutti i mezzi che la moderna tecnologia offre – e la vigente legislazione, nonché i principi costituzionali consentono – per adeguare l'efficacia investigativa alla evoluzione tecnologica dei mezzi

[147] G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico"*, in *Guida al diritto*, n. 34-35, 13 agosto 2016, pp. 76 e ss.
[148] F. CORDERO, *Codice di procedura penale commentato*, Torino, 1990, p. 302.

adoperati dai criminali»[149].

## 1.2 – Principali obiezioni

Gli interrogativi in merito alla pronuncia delle Sezioni Unite rimangono molteplici. In primo luogo, la portata dello strumento del captatore informatico va ben aldilà di ciò che usualmente si può raccogliere mediante le intercettazioni tradizionalmente intese. Il captatore può infatti, al contempo, effettuare un'intercettazione ambientale, una telematica, effettuare una geolocalizzazione, riprese video, immagazzinare una grande quantità di dati, immagini e video tratti dall'ambiente circostante e che possono, potenzialmente, coinvolgere anche soggetti estranei. In secondo luogo, è stato rilevato un punto critico rispetto ai soggetti che effettuano e forniscono tali *spyware*. Quando una procura autorizza una captazione si rivolge a ditte specializzate, come osservato nel capitolo precedente, le quali provvedono a rendere operative le intercettazioni. Non esistono tuttavia, al giorno d'oggi, regole atte a garantire l'affidabilità delle ditte in questione, non potendo quindi conoscere quali requisiti debbano esse avere in modo da poter essere ingaggiate e tantomeno attraverso quali modalità avvenga poi di fatto la captazione da parte delle ditte specializzate e se esista qualcuno legittimato, all'interno delle ditte stesse, ad osservare che le indicazioni della Procura richiedente tali operazioni intercettive siano osservate

[149] Sulla sentenza si veda anche A. GAITO e S. FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, II, p. 309; A. CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni Unite*, in *Arch. pen.*, 2016, II, p. 331; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen.*, 2016, II, p. 348; V. PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen.*, 2016, II, p. 354.

rigorosamente[150].

Un altro dubbio riguarda un profilo puramente operativo delle operazioni svolte con l'utilizzo dei captatori informatici. La Corte assume una posizione netta nell'escludere che esista la possibilità di un'intercettazione su un apparecchio portatile mediante virus informatico nel caso in cui si proceda per reati comuni per l'impossibilità di una preventiva indicazione, all'interno del decreto autorizzativo, dei luoghi privati ove l'apparecchio potrebbe essere utilizzato, in modo da consentire la previa verifica che in tali luoghi si stia svolgendo l'attività criminosa. Nella realtà tuttavia, possono esservi situazioni in cui tale possibilità di individuazione sia effettivamente plausibile: si pensi all'ipotesi in cui l'apparecchio portatile da sottoporre a controllo (ipotesi tipica del *personal computer*) in realtà rimanga di fatto sempre allocato presso un determinato luogo, assolvendo in quel luogo alle sue specifiche funzioni per l'utilizzatore. In questa ipotesi, nulla sembrerebbe escludere la possibilità di procedere all'intercettazione, sempre che nel luogo di specifico utilizzo permanga il motivato sospetto di svolgimento di una possibile attività criminosa[151].

Il punto più critico tuttavia, risulta essere un altro. Si deve infatti sottolineare l'ampiezza interpretativa che le Sezioni Unite hanno dato alla nozione di "criminalità organizzata" rilevante per far subentrare la disciplina derogatoria di cui all'articolo 13 del decreto legge n. 152 del 1991. In proposito, la Corte adotta una interpretazione estensiva, affermando che per i reati di criminalità organizzata devono intendersi non solo quelli elencati nell'articolo 51, commi 3-*bis* e 3-*quater*, del codice di procedura penale, ma anche quelli comunemente facenti capo a un'associazione per delinquere *ex* art. 416 del codice penale, correlata alle

[150] Così osservato da G. ZICCARDI, *Parlamento europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Arch. pen.*, 2017, n. 1.
[151] Così osservato da G. AMATO, *Reati di criminalità*, op. cit., p. 5.

attività più disparate, con esclusione del mero concorso di persone. In concreto quindi spetterà al p.m., per fisiologia ordinamentale, individuare volta per volta le fattispecie di reato che ritiene più affini al fatto sottostante, statuendo quindi che è una sola parte, seppur pubblica ed al servizio di finalità pubbliche, a determinare le condizioni che consentono l'applicazione della misura intercettiva in questione. Basterà quindi, a titolo esemplificativo, che un Pubblico Ministero iscriva nel registro delle notizie di reato un delitto ordinario aggravato *ex* articolo 7 del decreto legge 152/1991 ovvero compreso nel programma criminoso di un'associazione a delinquere, per far scattare l'utilizzo del virus *trojan*. Risulta quindi evidente che il ricorso all'intercettazione tramite captatore informatico divenga (o possa divenire), da ipotesi eccezionale, un'ipotesi alquanto metodica. Il solo limite posto a tale possibile condotta risulta quindi essere la notevole serietà professionale da parte della polizia giudiziaria e della magistratura, in modo da evitare una dilatazione delle ipotesi investigative al solo fine di poter disporre del captatore informatico in quelle determinate indagini.

Occorre inoltre chiedersi cosa potrebbe succedere se, in una fase successiva alle indagini, venga accertato che la qualificazione delle fattispecie operata inizialmente sia errata. In altre parole, la dottrina si domanda, nel momento in cui sia accertato a posteriori che il delitto in questione non rientri nel novero di quelli connessi alla criminalità organizzata, quali sarebbero le conseguenze nel caso delle risultanze probatorie captate a mezzo di captatore informatico tramite un decreto autorizzativo che non indica luoghi specifici e non consente quindi di verificare la sussistenza del fondato motivo di ritenere che ivi si stia svolgendo attività criminosa. Stando agli orientamenti giurisprudenziali e dottrinali esistenti ad oggi, si possono intravedere due possibili soluzioni: la prima è quella dell'inutilizzabilità, la seconda è una sorta di *self restraint* da parte dei Pubblici Ministeri i quali dovrebbero sempre rinunciare ad

avvalersi dei virus *trojan* quando intendono procedere con intercettazioni relative a procedimenti ordinari. Quanto alla prima ipotesi, la giurisprudenza ha elaborato negli anni un indirizzo quasi granitico sul tema, basato su una pronuncia delle Sezioni Unite, la quale nega l'esistenza di qualunque forma di inutilizzabilità derivata[152]. In questo caso quindi, anche se una certa captazione fosse dichiarata inutilizzabile, la sanzione connessa non potrebbe essere la preclusione dell'utilizzo della stessa come *notitia criminis* e quindi, ad esempio, come legittimo elemento alla base di una nuova richiesta di intercettazioni o di nuove attività investigative. La seconda opzione invece connette la sua efficacia in concreto alla discrezionalità dei Pubblici Ministeri i quali, in assenza di espliciti divieti normativi o di eventuali linee guida interne all'ufficio giudiziario in cui prestano servizio, potrebbero operare in maniera diametralmente opposta[153]. Rimane quindi il dubbio relativo a ciò che le parti e il giudice dovrebbero farne di elementi conoscitivi che continuerebbero a far parte del materia procedimentale o del fascicolo del dibattimento, chiedendosi quindi se essi possano legittimamente ignorarlo e non farne alcun uso o se siano tenuti a considerare quegli elementi attribuendogli un significato, quale che esso sia[154].

---

[152] Cass. sez. un., 27 marzo 1996, Sala, in *Foro it.*, 1996, II, p. 473.

[153] Si segnalano, a tal proposito, le linee guida in tema di intercettazioni adottate dalle procure di Roma, Napoli, Torino, Firenze, Bari, Macerata, Foggia, Nuoro, Caltanissetta, Campobasso, Siracusa, Catanzaro, Cosenza, Lamezia Terme, Arezzo, Grosseto, Livorno, Sulmona e Lecce, le quali sottolineano «l'esistenza di una peculiare, meritevole e crescente attenzione da parte dei Procuratori della Repubblica in ordine al tema del trattamento dei dati tratti da intercettazioni», così come riportato in *CSM, Settima commissione, ordine del giorno n. 2742, 28 luglio 2016*. Seppure esse facciano riferimento per lo più alle risultanze delle intercettazioni, si deve sottolineare una crescente attenzione al tema delle intercettazioni da parte delle Procure.

[154] In questo senso A. BALSAMO, *Le intercettazioni mediante virus informatico*, op. cit. p. 2274b; V. GIGLIO, *I virus informatici per scopi*, op. cit., p. 6.

# 2 – La funzione di garanzia del decreto di autorizzazione

Come osservato nel paragrafo precedente, sebbene la decisione delle Sezioni Unite limiti la possibilità dell'utilizzo del captatore informatico ai soli reati facenti capo alla nozione di criminalità organizzata, le critiche sono state molto aspre e decise. Una in particolare, mossa da alcuni docenti dell'Università di Torino e intitolata «Denuncia dei rischi connessi all'installazione occulta di virus informatici su *smartphone* e *tablet* per finalità di indagine penale»[155], traendo spunto dall'affermata legittimità del mezzo di ricerca della prova, seppure a determinate condizioni, auspica un profondo intervento da parte del legislatore in modo da disciplinare e regolare la materia con disposizioni specifiche, realizzando in tal modo un bilanciamento degli interessi e dei principi convenzionali e costituzionali coinvolti. E' stato anche rilevato che deve essere effettuata una distinzione tra l'uso di tale strumento per scopi puramente intercettivi e il suo impiego per poter perquisire a distanza gli archivi di *computer*, *tablet* e *smartphone*[156]. Riguardo quest'ultimo aspetto è stato osservato e sottolineato che l'ipotesi in questione non rientrerebbe nemmeno nel raggio di azione degli artt. 14 e 15 Cost., rendendo quindi necessaria non una semplice disciplina normativa ma, bensì, l'affermazione di un nuovo ed inedito diritto fondamentale all'uso libero e riservato delle tecnologie informatiche. Le c.d. perquisizioni *on-line* infatti non consistono in un accesso fisico al domicilio dell'indagato, non minacciando quindi una

[155] La denuncia è disponibile in Internet al sito http://www.giurisprudenzapenale.com/2016/07/29/denuncia-dei-rischi-connessi-allinstallazione-occulta-virus-informatici-smartphone-tablet-finalita-indagine-penale-universita-torino/.

[156] R. ORLANDI, Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici, in Internet al sito http://www.archiviopenale.it/.

violazione dell'art. 14 Cost. tramite un accesso fisico presso i luoghi domiciliari. D'altro canto, ispezionare i *files* contenuti in un *hard-disk* di un dispositivo è un'attività ben diversa dal captare un flusso di comunicazioni minacciando la libertà e la segretezza delle comunicazioni così come difese dall'art. 15 Cost. In questa prospettiva è stato suggerito di adottare il modello elaborato dalla Corte costituzionale tedesca, la quale con una famosa pronuncia del 2008[157], ha enucleato un nuovo diritto fondamentale dell'individuo, quello «all'uso riservato e confidenziale delle tecnologie informatiche».

Per quanto riguarda invece il primo profilo evidenziato, cioè quello relativo all'utilizzo del captatore informatico per scopi puramente intercettivi, vista la base giurisprudenziale presente e, alla luce della sopra citata pronuncia delle Sezioni Unite, sembra non porsi la necessità di un intervento del legislatore in materia. Riconoscendo infatti la peculiare forza intrusiva dello strumento informatico, le Sezioni Unite affermano che «la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso». Ecco quindi come assume un ruolo chiave il decreto di autorizzazione emanato a fronte di operazioni di intercettazioni, ruolo centrale che richiede il bilanciamento tra diritti costituzionali confliggenti, individuali e collettivi, riproponendo un problema già evidenziato dai

[157] Si tratta della sentenza del Bundesverfassungsgericht 27 febbraio 2008, in Riv. trim. dir. pen. econ., 3, 2009, 679 e ss., con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*, con la quale è stata riconosciuta l'inadeguatezza dei diritti a tutela delle libertà di domicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, ed è stato inaugurato un nuovo diritto costituzionale riconducibile alla c.d. "autodeterminazione informativa" e "sicurezza informatica", da intendersi anche come integrità e riservatezza dei dati e delle informazioni trattate da sistemi informatici, fondato sulla dignità umana dell'individuo e dell'utente "informatico".

giudici di legittimità[158]. Pur dovendo la motivazione essere alquanto sobria e, di conseguenza, potendo consistere in quella «minima necessaria a chiarire le ragioni del provvedimento»[159], la motivazione del provvedimento autorizzativo deve tuttavia spiegare come il mezzo di ricerca della prova «è assolutamente indispensabile ai fini della prosecuzione delle indagini» rispetto ad una specifica ipotesi delittuosa[160]. In altre parole, il giudice, per giustificare l'atto investigativo, non può tralasciare di indicare il criterio che funge da collegamento tra l'indagine in corso e la persona sottoposta ad intercettazioni, sottolineando ancora una volta in primo luogo quanto dettato in merito all'obbligo di motivazione dagli artt. 15 Cost. e 267, comma 1, c.p.p., e, in seconda battuta, quanto già affermato precedentemente dai giudici di legittimità[161]. In quest'ottica

---

[158] A tal proposito vedasi, Cass. sez. VI, 20 ottobre 2009 (dep. 31 dicembre 2009), Bassi, n. 50072, in *Giur. It.* 2010, 12, 2649, «la imprescindibile funzione del giudice, cui è demandato lo scrutinio dei presupposti di attivabilità delle intercettazioni, è quella di affermare in ogni momento il rispetto della legalità del procedimento e non certo quella di prestarsi a "facili aggiramenti" delle norme di legge per compiacere alle richieste del pubblico ministero o di chicchessia».

[159] Tra le altre, Cass. sez. V, 20 aprile 2004, Scardamaglia, n. 24229, in *Guida al diritto* 2004, 26, p. 76, secondo la quale risulta sufficiente che il giudice indichi i dati da lui ritenuti decisivi e non è necessario operare uno specifico esame critico dell'intero contesto sottoposto al suo esame. Il giudice, tuttavia, deve compiere autonoma valutazione delle richieste degli organi investigativi e non limitarsi ad espressioni che costituiscano perifrasi del contenuto delle norme che disciplinano l'assunzione del mezzo probatorio (Cass. sez. VI, 22 dicembre 1998, n. 4057, in *Cass. pen.* 2000, p. 3353).

[160] Cass. sez. VI, 26 febbraio 2010, Morabito, n. 10902, in *C.E.D. Cass.*, n. 246688, secondo cui «il presupposto dei gravi indizi di reato va inteso non in senso probatorio, ossia come valutazione del fondamento dell'accusa, ma come vaglio di particolare serietà delle ipotesi delittuose configurate, le quali non devono risultare meramente ipotetiche, essendo al contrario richiesta una sommaria ricognizione degli elementi dai quali sia dato desumere la seria probabilità dell'avvenuta consumazione di un reato». Allo stesso modo, tra le altre, Cass. sez. II, 1 marzo 2005, n. 10881, in *Guida al diritto* 2005, 16, p. 82; Cass. sez. un., 17 novembre 2004, n. 45189, in *Riv. pen.* 2005, p. 1018.

[161] Cass. pen., Sez. VI, 12 febbraio 2009, n. 12722, in *Giur. It.* 2010, 5, 1186. La vicenda riguardava la declaratoria di inutilizzabilità per mancanza di motivazione di alcuni decreti di intercettazioni redatti con una motivazione *per relationem* alla richiesta del PM, senza che fosse dato conto delle ragioni per cui erano sottoposte ad intercettazioni conversazioni private. Secondo la dottrina, in particolare V. GREVI, *Sul necessario collegamento tra utenze telefoniche e*

diventa di nuovo essenziale la professionalità e l'esperienza del Pubblico ministero e, soprattutto, del giudicante: esso infatti deve aver ben chiaro che l'autorizzazione all'intercettazione non impone una prognosi di colpevolezza in capo al soggetto indagato e, d'altra parte, deve poter compiere un vaglio approfondito sulle reali esigenze investigative e su quanto il mezzo di ricerca della prova possa influire, in modo negativo e positivo, sul soggetto sottoposto ad intercettazioni e sull'andamento delle investigazioni.

## 2.1 – Requisiti del decreto di autorizzazione

Il presupposto dell'attività investigativa nell'ambito della quale può trovare luogo una richiesta di intercettazione telefonica è costituito, senza alcun dubbio, dall'apprensione di una notizia di reato. Tale premessa risulta necessaria nel momento in cui si considera che l'intercettazione è un mezzo di ricerca della prova rispetto a reati che risultano già accertati, e non può, di conseguenza, trasformarsi in un mezzo per individuare reati non ancora giunti a conoscenza dell'autorità giudiziaria al fine di poterne prevenire la realizzazione, seppur con le limitate eccezioni previste da leggi speciali. Da ciò derivano due conseguenze fondamentali:

a) la richiesta di intercettazione non può che trovare il suo fondamento in una notizia di reato avanzata dalla polizia giudiziaria, ovvero da un privato cittadino, al Pubblico Ministero;

b) la richiesta può essere senza dubbio contestuale alla prima

---

*indagini in corso nel decreto autorizzativo delle intercettazioni*, in *Cass. pen.* 2009, 9, p. 3344, con questa decisione la Corte ha lanciato «un messaggio di tipo pedagogico agli organi applicatori di fronte al rischio, non soltanto teorico, di una eccessiva disinvoltura nel ricorso allo strumento delle intercettazioni».

comunicazione della notizia di reato, ma non potrà essere ontologicamente precedente alla stessa; l'indicazione del reato per cui si procede ad intercettazione deve essere, di fatto, corroborata dall'indicazione dei gravi (o sufficienti) indizi, necessari per la prosecuzione delle attività investigative, i quali da soli giustificano la richiesta di autorizzazione (o di convalida) al Giudice per le indagini preliminari (GIP).

La stessa Cassazione, interrogata sul tema, ha affermato che tali mezzi di ricerca della prova vengono disposti nella fase iniziale delle indagini, nel momento in cui gli elementi in possesso degli agenti indaganti sono limitati e lo strumento viene utilizzato proprio al fine di acquisire quanti più elementi possibili[162]. Gli unici dubbi interpretativi sono sorti in tema di indagini riferite al tema della criminalità organizzata ed in particolare ad i reati associativi, come quelli previsti dagli artt. 416 e 416-*bis* c.p., ovvero dall'art. 74 d.p.r. 9 ottobre 1990 n. 309. I dubbi sono tuttavia più apparenti che reali in quanto il reato associativo è fondato su un'attività organizzata in modo continuativo, destinata poi alla realizzazione di un numero indeterminato di reati. Se si parte dall'assunto che questo è lo schema "caratterizzante" i reati di tipo associativo, allora si potrà facilmente dedurre che l'intercettazione risulta pienamente disposta legittimamente nella fase di accertamento di tali reati, indeterminati nel numero[163]. Sempre a sostegno di questo orientamento, la Corte di cassazione si è espressa con un'ulteriore pronuncia[164], stavolta intervenendo sul punto le Sezioni Unite e chiarendo che, necessariamente prima dell'inizio delle operazioni riguardanti intercettazioni telefoniche, il Pubblico Ministero deve motivare, o integrare, con apposito decreto, la

[162] In questo senso, Cass. sez. V, 29 marzo 2000, Terracciano, in *C.E.D. Cass.*, n. 215731.
[163] In questo senso, C. PARODI, *Le intercettazioni*, op. cit., p. 79.
[164] Cass. sez. un., 29 novembre 2005, Campennì, n. 2737/06, in *Cass. mass.*, rv. 232605.

motivazione già resa, in ordine ai presupposti di urgenza o di inidoneità degli apparati intercettivi presenti nelle Procure. Il passaggio interessante risulta essere quello in cui la motivazione, a parere delle Sezioni Unite, non può che precedere l'atto da compiere, essendo impossibile per il Pubblico Ministero integrare il provvedimento successivamente, in quanto esso perderebbe la sua capacità di controllo a priori, divenendo una sorta di controllo successivo[165].

Per quanto riguarda la disciplina contenuta nel codice, le disposizioni concernenti i presupposti e le forme dei provvedimenti dispositivi delle operazioni di intercettazione sono contenute negli artt. 267 e 268 del codice di procedura penale. Il primo articolo sopra citato, intitolato «Presupposti e forme del provvedimento», al primo comma stabilisce che il Pubblico Ministero deve richiedere al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni di cui all'art. 266 c.p.p. e specifica che, detta autorizzazione, è data con decreto motivato quando vi sono gravi indizi di reato ed inoltre l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini. Al secondo comma invece, si stabilisce che nei casi di urgenza, quando vi è il fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il Pubblico Ministero dispone l'intercettazione con decreto motivato, il quale va comunicato immediatamente e in ogni caso non oltre le ventiquattro ore al giudice delle indagini preliminari. Il secondo articolo invece, il 268 c.p.p., disciplina l'esecuzione delle operazioni passo dopo passo. La disciplina derogatoria di cui al comma 2, art. 267 c.p.p., per cui bastano i sufficienti indizi di reato, è quella disciplinata per i delitti relativi alla criminalità organizzata o di minaccia per mezzo del telefono, ovvero in relazione ai procedimenti per i delitti previsti dal libro II, titolo XII, capo III, sezione I, del codice penale, ed infine in merito ai procedimenti per i

[165] A. GAITO, *L'integrazione successiva dei decreti di intercettazioni telefoniche non motivati*, in *Dir. pen. proc.*, 2004, p. 929.

delitti previsti dall'art. 3 della legge 20 febbraio 1958, n. 75 e per i casi menzionati dall'art. 13, comma 1, legge 12 luglio 1991, n. 203. Tutti i sopra richiamati presupposti sin dal momento della emissione del decreto autorizzativo[166]. In sintesi quindi: l'articolo 267 c.p.p. richiede che il decreto autorizzativo sia adottato dal GIP, ovvero dal Pubblico Ministero nei casi di urgenza, il quale lo sottopone entro ventiquattro ore al GIP affinché quest'ultimo possa convalidarlo nelle quarantotto ore successive, a pena di inutilizzabilità dei risultati delle operazioni intercettive. La particolare invasività del mezzo di ricerca della prova ha infatti "obbligato" il legislatore a prevedere l'intervento del giudice per le indagini preliminari, in funzione di garanzia e di controllo, allo scopo di autorizzare l'atto (o di convalidarlo, nell'ipotesi di cui al comma 2, art. 267 c.p.p.).

Per quanto attiene al caso contemplato dal comma 2, art. 267 c.p.p., intercettazioni denominate *ex abrupto* e riguardante la possibilità del Pubblico Ministero di emanare un decreto motivato diretto al GIP nei casi particolari disciplinati dall'articolo sopra citato, esso ha sollevato non poche perplessità, specialmente per quanto riguarda il rapporto fra il Pubblico Ministero e l'organo giudicante, il GIP. Se da un lato infatti è chiaro che il sistema codicistico abbia inteso individuare nell'organo dell'accusa il *dominus* dell'attività intercettiva, con riguardo non solamente alla richiesta, ma bensì anche all'attività esecutiva, alle modalità e all' utilizzo dei risultati raccolti, dall'altro lato è stato previsto un controllo di natura autorizzativa da parte dell'organo giudicante. Tuttavia, come osservato in dottrina[167], il Pubblico Ministero, ossia l'organo richiedente e non l'organo autorizzante, rappresenta «l'effettivo titolare del potere, integrando, invece, il *placet* di quest'ultimo, soltanto un presupposto al suo materiale esercizio». Di altrettanta importanza risulta essere la problematica relativa agli elementi che il Pubblico Ministero potrà – ovvero

[166] In questo senso, Cass. sez. V, 11 luglio 1995, Coluccia e altri, n. 8925, in *Giur. it.*, 1996, II, p. 576 con nota di F. DINACCI.
[167] P. BRUNO, *Intercettazioni di comunicazioni o conversazioni*, op. cit., p. 188.

dovrà – allegare alla richiesta di intercettazioni, risultando prospettabili tre ipotesi:

a) il Pubblico Ministero trasmette tutti gli atti di indagine compiuti sino al momento della richiesta;

b) il Pubblico Ministero trasmette unicamente gli atti di indagine che ritiene siano in grado di supportare la sua richiesta;

c) il Pubblico Ministero deve anche trasmettere evidenti o plausibili prove a discarico.

All'inizio si potrebbe protendere per la soluzione prospettata al punto *sub (a)*[168] alla quale non ostano ragioni di sicurezza delle indagini ma piuttosto ragioni collegate alla disciplina vigente: se infatti fosse trasmesso integralmente il fascicolo al GIP, esso sarebbe direttamente coinvolto nella conduzione delle indagini, in aperto contrasto dunque con il ruolo e le funzioni assegnatogli dal legislatore[169]. La soluzione prospettata invece al punto *sub (b)*[170] risulta difficilmente sostenibile se si prendono in considerazione due fattori: in primo luogo, non sembra ragionevole prospettare una sorta di strategia del segreto tra il Pubblico Ministero e il GIP, soprattutto alla luce del fatto che non c'è nessun pericolo di una *discovery* anticipata a favore della persona indagata; in secondo luogo, risulta di difficile comprensione quale possa essere l'effettivo grado di verifica esercitabile in concreto dall'organo giudicante nel momento in cui la richiesta, in concreto, presenta solamente il titolo del reato, l'esistenza degli indizi e la necessità di ottenere l'autorizzazione alle operazioni di intercettazione. In definitiva, non sembra possibile deviare dalla terza

[168] In questo senso, L. FILIPPI, *Due temi da distinguere nel dibattito sulle intercettazioni*, in *DPP*, 1993, p. 103.
[169] M. FERRAIOLI, *La funzione di «controllo» del giudice per le indagini preliminari*, in *ASalerno*, 1993, p. 88.
[170] C. TAORMINA, *Diritto processuale penale*, vol. I, Giappichelli Editore, Torino, 1995, p. 327.

ipotesi di cui al punto *sub (c)*, la cui conseguenza è quella secondo cui il Pubblico Ministero abbia l'obbligo di trasmettere al GIP anche evidenti o plausibili prove a discarico dell'indagato, anche qualora egli le ritenga inattendibili, in quanto il legislatore non pone su di lui il compito di vagliare la consistenza degli indizi. Questa soluzione tuttavia prospetta una sorta di affidamento al buon senso ed alla professionalità dei Pubblici Ministeri, in quanto l'obbligo sopra descritto poggerebbe solamente su doveri deontologici dei magistrati e non su una esplicita, e di conseguenza ben più salda, previsione normativa.

In ultima istanza, può essere utile richiamare anche quanto osservato dalla Corte europea in tema di requisiti essenziali per ritenere che una regolamentazione delle intercettazioni sia compatibile con la supremazia del diritto necessaria in ogni società democratica e, di conseguenza, indispensabile a garantire una protezione adeguata contro il pericolo di atti lesivi del diritto alla *privacy*. In particolare, in una nota pronuncia[171], la Corte puntualizza i seguenti aspetti imprescindibili nella disciplina delle intercettazioni: la definizione delle categorie di persone assoggettabili ad intercettazioni; la natura dei reati che vi possono dare luogo; la fissazione di un termine massimo per la durata delle intercettazioni; le modalità di redazione dei verbali relativi alle comunicazioni captate; le precauzioni riguardanti la trasmissione, intatta ed integrale, delle registrazioni effettuate, in modo da permettere un controllo ad opera del giudice e della difesa; le circostanze in cui si possa ovvero si debba provvedere alla cancellazione o alla distruzione delle bobine.

## 2.2 – I presupposti dell'intercettazione

Secondo quanto stabilito dall'articolo 267 del codice di procedura penale i

[171] C. eur, 10 aprile 2007, Panarisi c. Italia, n.46794/99, in *CP* 2007, p. 3941.

presupposti relative alle operazioni di intercettazioni sono rappresentati dai «gravi indizi di reato» per poter ammettere l'intercettazione e dall'«assoluta indispensabilità» dell'intercettazione «ai fini della prosecuzione delle indagini».

Il secondo presupposto risulta di semplice disamina in quanto esso significa che la prova non può essere acquisita con mezzi diversi dalle intercettazioni e, al tempo stesso, presuppone che le indagini preliminari siano avviate, escludendo pertanto che l'intercettazione possa essere autorizzata quale primo atto di indagine[172]. L'accertamento della presenza o meno di tale indispensabilità è questione rimessa alla valutazione esclusiva del giudice di merito, la cui decisione può essere censurata, in sede di legittimità, unicamente sotto il profilo della manifesta illogicità della motivazione[173]. Questo peculiare presupposto svolge inoltre una funzione essenziale, ossia quella di spostare in avanti l'operazione intercettiva: in altri termini, visto che essa deve essere assolutamente indispensabile ai fini della corretta prosecuzione delle indagini, non è consentito quindi disporla all'inizio dell'attività investigativa, in quanto occorre che l'autorità procedente si trovi già in possesso di altri elementi probatori dai quali poter desumere i gravi indizi di reato. Infine il legislatore non esige che il Pubblico Ministero, al momento della richiesta, e il GIP, in sede di autorizzazione, effettuino un giudizio prognostico sui possibili ovvero probabili esiti positivi dell'intercettazione[174], ma al contrario egli esige solamente che, al momento della disposizione dell'intercettazione, manchino alternative di eguale efficacia.

Per quanto riguarda invece il presupposto attinente ai «gravi indizi di reato» la situazione risulta più complessa. La disciplina vigente può

[172] In questo senso, L. FILIPPI, *L'intercettazione di comunicazioni*, op. cit., p. 72.
[173] Cass. sez. VI, 22 dicembre 2003, Scremin, in *CP* 2005, p. 3926.
[174] Posizione sostenuta da A. V. SEGHETTI, *Intercettazioni telefoniche illegittime per motivazione insufficiente e nullità della custodia cautelare*, *GI*, II, 1992, p. 133.

sembrare meno garantista rispetto alla precedente, la quale richiedeva «indizi seri e concreti, da indicarsi specificamente nel decreto» ovvero «la effettiva necessità ai fini di acquisizione di prove non altrimenti conseguibili» (così all'art. 266-*ter* c.p.p. successivamente abrogato), ma in realtà risulta più rigorosa in quanto le due condizioni, non più separate nel dettato della norma, devono coesistere allo stesso tempo[175]. In primo luogo c'è da notare che il riferimento operato dal codice è attinente al reato e non alla colpevolezza (di cui all'art. 273 c.p.p.), per cui si può affermare agevolmente che le operazioni di intercettazione possono esser disposte legittimamente, oltre che nei procedimenti a carico di ignoti, poiché in quei casi non avrebbe senso parlare di gravi indizi di colpevolezza in quanto non è ancora specificata la persona a cui il reato è attribuito, anche nei procedimenti contro una persona sì nota ma non ancora avente gravi indizi di colpevolezza[176]. Allo stesso modo, la dizione normativa consente di sottoporre ad intercettazione e quindi di limitare il diritto di segretezza di ogni forma di comunicazione sancito dall'art. 15 Cost. anche un soggetto che non sia indagato, ad esempio una parte lesa[177]. In altre parole, per poter procedere ad intercettazione non è affatto necessario che sussistano a carico dei soggetti le cui conversazione dovranno essere captate dei gravi indizi[178]; inoltre gli indizi non sembra debbano avere le peculiarità richieste, nell'ambito specifico della valutazione della prova, dall'art. 192, comma 2, c.p.p., in quanto essi devono essere gravi, ma non anche precisi e concordanti[179]. In

[175] In questo senso, R. D'AJELLO, *Le intercettazioni di conversazioni,* op. cit., p. 110.
[176] Cass. sez. I, 11 agosto 2000, Nicchio ed altri, n. 4979, in *C.E.D. Cass.*, n. 216747.
[177] Cass. sez. I, 16 gennaio 1995, Catti ed altri, n. 1079, in *Giust. pen.*, 1996, III, p. 226.
[178] In questo senso Cass. sez. VI, 22 luglio 1999, Patricelli, n. 9428, *ivi*, p. 188; Cass. sez. V, 4 novembre 2003, Hani, n. 44718, in *Guida al Diritto*, 2004, 8, p. 82.
[179] Di parere contrario si segnala A. NAPPI, *Guida al codice di procedura penale*, Giuffrè, Milano, 1997, p. 154.

particolare, riguardo a quest'ultimo aspetto evidenziato, la conclusione appare logica in quanto se l'art. 267, comma 1, c.p.p., si modellasse su quanto stabilito dall'art. 192, comma 2, c.p.p., allora si dovrebbe concludere che una prova storica, quale può essere ad esempio una testimonianza, non potrebbe mai legittimare un'intercettazione, il che risulta palesemente assurdo. Le due norme si pongono quindi su due piani diversi: l'art. 192 del codice di procedura penale indica «i criteri di valutazione della prova logica indiziaria, necessaria e sufficiente per affermare la responsabilità dell'imputato»[180] mentre l'art. 267 c.p.p. afferma solamente che gli elementi in mano al Pubblico Ministero fanno ritenere altamente probabile la commissione di uno dei reati derubricati all'art. 266 c.p.p. o all'art. 266-*bis* c.p.p. Sembra inoltre ipotizzabile che, sebbene l'art. 267 c.p.p. parli propriamente di «indizi» al plurale, anche un solo indizio possa essere sufficiente a supportare la richiesta di autorizzazione, in quanto ciò che conta non è il loro numero ma la loro intrinseca forza persuasiva[181]. Un altro dubbio di fondamentale importanza è quello relativo alla possibilità secondo la quale una o più delle ipotesi di reato a cui si riferiscono gli indizi siano escluse dall'elencazione di cui agli artt. 266 e 266-*bis* c.p.p. Proprio in quanto l'accertamento è ancora *in fieri* e l'imputazione è solamente ancora un'ipotesi, può accadere che gli indizi (o l'indizio), anche qualora siano gravi, siano collegati a più fattispecie di reato. In casi del genere è venuta in soccorso del legislatore la giurisprudenza, la quale non ha esitato a ritenere ammissibile l'autorizzazione purché essa sia stata concessa relativamente ad uno dei reati tassativamente previsti dal legislatore[182]. Inoltre gli stessi giudici di legittimità hanno affermato, con una pronuncia successiva[183], che l'indicazione espressa dal Pubblico Ministero circa il titolo del reato nella

[180] Cass. sez. III, 23 febbraio 1998, Derzsiova, in *RP*, 1998, p. 816.
[181] In questo senso, C. TAORMINA, *Diritto processuale penale*, op. cit., p. 326.
[182] Cass. sez. I, 12 marzo 1990, Bicici, in *GP*, 1991, III, p. 424.
[183] Cass. sez. II, 21 aprile 1997, Viveri, in *ANPP*, 1998, p. 296.

sua richiesta di autorizzazione ha un carattere puramente generico e non vincolante e, di conseguenza, il giudice per le indagini preliminari può indicare successivamente il reato che è ascrivibile sulla base degli atti trasmessigli dal Pubblico Ministero e che consente quindi di avvalersi del mezzo di ricerca della prova relativo all'intercettazione.

## 2.3 – Le modalità di esecuzione delle operazioni

Dopo aver esaminato i requisiti necessari del decreto di autorizzazione per le operazioni di intercettazioni è necessario esaminare le modalità pratiche di esecuzione di tali operazioni. In primo luogo si possono distinguere due tipi di procedimenti: quello ordinario e quello *ex abrupto*.

Il primo consiste nella richiesta, da parte del Pubblico Ministero, al giudice per le indagini preliminari, di autorizzarlo a disporre le operazioni di cui all'art. 266 c.p.p., facendo si che il GIP provveda quindi con decreto motivato, sia nel caso accolga sia nel caso in cui respinga la richiesta. E' necessario sottolineare che il decreto di diniego, così come anche il decreto che concede l'autorizzazione[184] alle operazioni emanato dal GIP, non è soggetto ad alcuna impugnazione[185], in quanto essa non è né prevista né ricavabile dal sistema, stante il principio di tassatività delle impugnazioni di cui all'art. 568 c.p.p.[186]. Vige inoltre l'obbligo di motivazione, così come imposto a pena di inutilizzabilità dall'art. 271,

[184] Esso è tuttavia soggetto ad un sindacato che si concretizza in un giudizio di utilizzabilità – inutilizzabilità dei risultati probatori acquisiti.
[185] V. CAMPILONGO, *L'obbligo di motivazione in tema di intercettazioni di conversazioni o comunicazioni: questioni interpretative e problemi applicativi,* in *CP* 2005, p. 3196.
[186] In questo senso vedasi Cass. sez. I, 22 settembre 1992, Zazza, in *ANPP*, 1993, p. 333; Cass. sez. I, 11 dicembre 1989, Baglio, in *GP*, 1990, III, p. 583.

comma 1, c.p.p., anche se la Suprema Corte ha specificato che, stante il fatto che le intercettazioni vengono di norma effettuate in un momento del procedimento caratterizzato dalla limitatezza degli elementi indiziari a disposizione del Pubblico Ministero, sia sufficiente la motivazione del decreto autorizzativo che, pur se concisa e ridotta agli elementi essenziali, consenta alle parti e al GIP di valutare la ritualità delle intercettazioni disposte[187]. Diventa sufficiente, dunque, la motivazione «minima indispensabile a chiarire le ragioni del provvedimento, a garantire il rispetto dei presupposti che lo legittimano in relazione alla natura di ognuno di essi e l'avvenuta osservanza delle disposizioni previste negli art. 267 e 268 commi 1 e 3 c.p.p.[188] ». In aggiunta a quanto appena detto, la Cassazione ha ulteriormente specificato che è consentita al GIP la motivazione *per relationem* alla richiesta del Pubblico Ministero «purché siano chiarite le ragioni del provvedimento e sia conosciuta o conoscibile la motivazione a cui si fa rinvio[189]». Risulta utile specificare che la dottrina ha sempre guardato con sospetto a tale attività del GIP in quanto essa ritiene che tale pratica riduca l'impegno del decidente, con il rischio, non del tutto astratto, di farne una sorta di «meccanico ripetitore di deliberati altrui»[190]. Questo panorama abbastanza frastagliato ha provocato l'intervento, necessario, delle Sezioni Unite[191], secondo le quali la motivazione *per relationem* è legittima quando: «1) faccia riferimento, recettizio o di semplice rinvio, a un legittimo atto del procedimento, la cui motivazione risulti congrua rispetto all'esigenza di giustificazione propria

[187] Cass. sez. V, 15 febbraio 2000, Terracciano, n. 784, cit., 2001, 568, p. 931.
[188] Cass. sez. VI, 11 maggio 1999, Belocchi, n. 8645, in *Cass. pen.*, 2000, p. 3353.
[189] Cass. sez. V, 13 maggio 2003, Pagano ed altri, n. 25522, in *Guida al diritto*, 2003, 40, p. 64.
[190] In questo senso P. BALDUCCI, *Le garanzie*, op. cit., pp. 128 e ss.; P. POMANTI, *C. pen.*, 2000, pp. 697 e ss.; E. AMODIO, *Motivazione della sentenza penale*, in *Enc. dir.*, XXVII, pp. 199 e ss.; D. SIRACUSANO, *R. it. dir. proc. pen.*, 58, pp. 387 e ss.; nel senso contrario invece, A. CRISTIANI, *Profili evolutivi*, in *Studi Vassalli*, II, pp. 434 e ss.
[191] Cass. sez. un., 21 giugno 2000, Primavera ed altri, in *A. n. proc. pen.*, 2000, p. 650.

del provvedimento di destinazione; 2) fornisca la dimostrazione che il giudice ha preso cognizione del contenuto sostanziale delle ragioni del provvedimento di riferimento e le abbia meditate e ritenute coerenti con la sua decisione; 3) l'atto di riferimento, quando non venga allegato o trascritto nel provvedimento da motivare, sia conosciuto dall'interessato o almeno ostensibile, quanto meno al momento in cui si renda attuale l'esercizio della facoltà di valutazione, di critica ed, eventualmente, di gravame e, conseguentemente, di controllo dell'organo della valutazione o dell'impugnazione».

Per quanto riguarda invece il secondo procedimento, ossia quello relativo alle intercettazioni decretate dal Pubblico Ministero (c.d. intercettazioni *ex abrupto*), come è stato ricordato nel paragrafo precedente, esso rappresenta un caso particolare. Ai sensi dell'art. 267, comma 2, c.p.p., nei «casi di urgenza» quando vi è «fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini», il Pubblico Ministero dispone l'intercettazione con decreto motivato, che va comunicato immediatamente ovvero non oltre le ventiquattro ore, al GIP, il quale, a sua volta, decide sulla possibile convalida o sul possibile diniego, di nuovo con decreto motivato, entro e non oltre quarantotto ore dal provvedimento emanato dal Pubblico Ministero. Questa particolare previsione normativa è stata oggetto di due diverse critiche: da un lato se ne è messa in dubbio la stessa legittimità in quanto la carta costituzionale imporrebbe che qualsiasi atto deputato a comporre il conflitto fra le ragioni dell'autorità e quelle della libertà fosse riservato ad un organo imparziale, ossia ad un giudice[192]; dall'altro lato, si contesta l'opportunità dell'istituto in quanto un autentico *periculum in mora* sarebbe difficilmente concretizzabile e, in ogni caso, esso sarebbe suscettibile di un facile rimedio attraverso una veloce decisione da parte del GIP. Infine, sia che ci

[192] In questo senso A. DIDDI, *Giust. pen.*, 1992, III, p. 58; L. FILIPPI, *Intercettazioni telefoniche, diritto processuale penale*, in *Enc. dir.*, Agg., VI, p. 573; G. GARUTI, *D. pen. proc.,*2005, pp. 1458 e ss.

si trovi nel primo caso prospettato, ossia il procedimento ordinario, che in quello in cui il decreto autorizzativo viene disposto direttamente dal Pubblico Ministero, per quanto attiene alla durata delle operazioni di intercettazione, l'art. 267, comma 3, c.p.p., stabilisce chiaramente che esse non possono durare più di quindici giorni, salvo successiva proroga disposta dal giudice sempre attraverso lo strumento del decreto motivato, per periodi successivi di quindici giorni e sempre qualora fossero ancora permanenti i presupposti indicati nel comma 1 dell'articolo in questione.

Inoltre, in entrambe le ipotesi sopra disaminate, alle operazioni di intercettazione si procede, a pena di inutilizzabilità secondo quanto disposto dall'art. 271, comma 1, c.p.p., con decreto del Pubblico Ministero, il quale indica le modalità e la durata delle operazioni. A tali operazioni quindi procede, personalmente, il Pubblico Ministero, il quale tuttavia, come avviene ordinariamente per via dei molteplici impegni istituzionali, si avvale di un ufficiale della polizia giudiziaria (art. 267, comma 4, c.p.p.). L'operazione di registrazione consiste dunque nell'immissione dei dati captati in una memoria informatica centralizzata[193], preferendo, così come stabilito nel codice di procedura penale, l'utilizzo degli impianti installati presso le procure, evitando tuttavia l'equivoco, puramente tecnico, per cui si pensa che la vera e propria captazione sia da svolgere presso le procure, mentre essa in realtà avviene, per ragioni esclusivamente tecniche, soltanto presso l'operatore telefonico mentre la conversazione, dirottata verso le sedi delle procure, deve essere lì registrata[194]. Malgrado l'art. 268, comma 3, c.p.p., la dottrina nota come ormai il ricorso ad impianti esterni sia diventato quasi regolare[195], e, soprattutto in merito alle intercettazioni ambientali, lo

[193] Per ulteriori approfondimenti sul punto vedasi A. PAOLONI e D. ZAVATTARO, *Intercettazioni telefoniche ed ambientali. Metodi, limiti e sviluppi nella trascrizione e verbalizzazione*, Centro Scientifico Editore, 2007, pp. 84 e ss.
[194] Cass. sez. un., 26 giugno 2008, Carli, in *Cass. pen.*, 2009, p. 30.
[195] A. BARGI, *Intercettazioni di comunicazioni e conversazioni*, op. cit., p. 800.

sviluppo di tale prassi ha portato la stessa dottrina a dividersi sul tema. Da un lato c'è chi afferma che tale prassi non sia possibile[196] facendo leva sul tenore letterale della norma di cui all'art. 267, comma 3, c.p.p.; dall'altro lato c'è chi risponde che è, di regola, difficile intercettare colloqui fra persone presenti utilizzando solamente le apparecchiature in dote alle procure, in quanto è necessario, solitamente, posizionare in prossimità del luogo in cui il dialogo si svolge, uno strumento di captazione che poi invierà il segnale ad una stazione ricevente posta nelle vicinanze. Quest'ultima posizione ritiene inoltre che il comma 3 fosse stato scritto in merito esclusivamente alle intercettazioni telefoniche, giustificando così l'utilizzo delle sole apparecchiature presenti nelle procure[197]. La tesi favorevole ad applicare l'art. 268, comma 3, c.p.p., a tutti i tipi di intercettazione è stata tuttavia recepita successivamente dalla Suprema Corte, in una vicenda nella quale l'intercettazione ambientale era stata eseguita tramite un telefono cellulare posizionato all'interno dell'autovettura sotto controllo dell'autorità investigante[198]. Si ritiene legittima pertanto la tecnica del c.d. ascolto remotizzato (*roaming*), in base alla quale l'intercettazione, mediante un "rimbalzo" del segnale dal luogo di captazione agli uffici della procura della Repubblica con una differenza temporale di pochi secondi, avviene tecnicamente presso gli uffici delle procure stesse[199].

Riguardo poi alle risultanze delle operazioni di intercettazione, a pena di inutilizzabilità, sono registrate le comunicazioni e le conversazioni intercettate e di tali operazioni viene redatto apposito verbale, così come

---

[196] G. GATTI, *Il controllo del gip*, in *Quad. C.s.m.*, 1995, n. 81, pp. 219 e ss. e p. 232.
[197] In questo senso vedasi E. BERTUGLIA e P. BRUNO, *Le intercettazioni nel nuovo codice di procedura penale*, in *Riv. guardia di fin.*, 1990, p. 1330;
[198] Cass. sez. un., 31 ottobre 2001, Policastro ed altri, in *Giust. pen.*, 2002, III, p. 625.
[199] Cass. sez. VI, 19 febbraio 2008, Carli, in *GD*, *dossier mensile* 2008, 6, p. 73. Sullo stesso tema, dopo rimessione alle Sezioni Unite, Cass. sez. un., 26 6 2008, Carli, cit., p. 30.

stabilito dall'art. 268, comma 1, c.p.p., il quale deve avere il contenuto indicato dall'art. 136 c.p.p., deve essere sottoscritto a norma dell'art. 137 c.p.p. e deve riportare, questa volta non a pena di inutilizzabilità, la trascrizione, anche in maniera sommaria, del contenuto delle comunicazioni intercettate. Vengono anche comunemente definiti "brogliacci di ascolto", i quali però si specifica che non hanno alcuna rilevanza probatoria in quanto essa è riconosciuta dalla legge solo ai documenti fonici e verbali[200]. Si deve comunque ricordare che, come stabilito anche dalla Suprema Corte[201], in tema di intercettazione di conversazioni o comunicazioni telefoniche, la prova è costituita dalla registrazione, per cui è irrilevante, ai fini dell' utilizzabilità, la possibile mancata trascrizione delle registrazioni nelle forme della perizia, poiché la prova è costituita dalle cassette o bobine contenenti le registrazioni. Per quanto riguarda invece i nastri contenenti le registrazioni, essi vengono racchiusi in apposite custodie numerate e sigillate, sono collocati successivamente in un involucro sul quale viene indicato il numero delle bobine contenute, il numero del dispositivo controllato, i nomi, ogni volta in cui risulti possibile, delle persone le cui conversazioni sono state captate ed il numero che, con riferimento alla registrazione consentita, risulta dal registro delle intercettazioni di cui sopra, *ex* art. 267, comma 5, c.p.p.

Infine, dopo la conclusione delle operazioni di intercettazione, l'art. 267, comma 4, c.p.p., afferma che la polizia giudiziaria deve trasmettere immediatamente al Pubblico Ministero i verbali e le registrazioni delle comunicazioni intercettate. Infatti quanto trasmesso deve essere depositato entro cinque giorni in segreteria, assieme ai decreti che hanno disposto, autorizzato o prorogato tale intercettazione, giungendo quindi al momento della *discovery* dei risultati delle intercettazioni, in quanto dal deposito, esse non sono più coperte dal segreto, come afferma l'art. 329,

[200] Cass. sez. VI, 7 aprile 1995, Celone, in *ANPP*, 1996, p. 156.
[201] Cass. sez. I, 19 febbraio 2002, Panella, n. 13104, in *Guida al diritto*, 2002, 22, p. 82.

comma 1, c.p.p. Sempre in merito al deposito, l'avviso di tale atto deve essere dato al difensore e non alla parte personalmente, così come stabilito dalla Suprema Corte[202]. L'unico problema riguardante il deposito di cui bisogna far menzione è quello relativo alla situazione in cui il Pubblico Ministero ritenga che dall'intercettazione non emergano elementi rilevanti per la pubblica accusa. Secondo una prassi consolidata, in passato, il Pubblico Ministero ometteva il deposito *ex* art. 268, comma 4, c.p.p., chiedendo quindi l'autorizzazione all'archiviazione della *notizia criminis* e la distruzione dei nastri e verbali delle relative intercettazione al fine di alleggerire gli obblighi di conservazione in capo alle segreterie[203]. La dottrina tuttavia ritiene che tale deposito vada effettuato ugualmente, in modo tale da permettere alla persona sottoposta alle indagini di effettuare una valutazione personale della possibile rilevanza o meno delle intercettazioni effettuate[204].

Ultima nota di rilievo, quella relativa al comma 7 dell'art. 268 c.p.p., nel quale con la legge n. 547 del 23 dicembre 1993, è stata inserita un'interpolazione che permette di estendere la disciplina originaria della trascrizione delle intercettazioni anche alle comunicazioni informatiche, in modo da adattarsi al nuovo art. 266-*bis* del codice di procedura penale. Grazie a questa operazione infatti, si dovrebbe poter permettere, o almeno rendere più agevole, sia alle parti che al giudice, di poter comprendere il contenuto delle intercettazioni informatiche eseguite, le quali, in generale, sono apprezzabili solamente dagli addetti ai lavori.

---

[202] Cass. sez. VI, 14 novembre 2006, Protopapa, in *Cass. pen.*, 2008, p. 2532.
[203] Così C. RIVIEZZO, *La trascrizione delle intercettazioni telefoniche*, in *GG* 1994, 20, p. 22; A. SPATARO, *Le intercettazioni telefoniche: problemi operativi e processuali*, in *Quaderni del c.s.m.* 1994, 69, p. 144.
[204] G. FUMU, *Intercettazioni, archiviazione e distruzione della documentazione tra norma e prassi e giurisprudenza costituzionale*, in *LP* 1995, p. 491.

## 2.4 – La possibile necessità di molteplici decreti di autorizzazione per un unico captatore

Come visto nel paragrafo precedente, il decreto di autorizzazione funge da elemento di garanzia fra le libertà dei soggetti sottoposti ad intercettazione e la necessità di reprimere ovvero scoprire i reati. Questo mezzo ha trovato perfetta corrispondenza nella disciplina delle intercettazioni di comunicazioni o telefoniche ed anche nelle intercettazioni ambientali, tuttavia si possono intravedere dei seri dubbi nel momento in cui si prendono in considerazione le intercettazioni effettuate a mezzo di captatore informatico. Come è stato già spiegato in precedenza, le intercettazioni che sfruttano le potenzialità del virus *trojan* sono anche dette "itineranti", poiché una volta installate sul dispositivo prescelto, sono in grado di seguire il proprietario di tale dispositivo ovunque egli si rechi, sia esso un luogo di privata dimora o un luogo pubblico[205]. Tale captazione si definisce anche dinamica, in quanto oltre a seguire l'intercettato, il tipo di intercettazione può variare a seconda del diverso dispositivo "infettato". Come ricordato nei capitoli precedenti, tali virus possono cercare tra i *file* presenti sul computer o sui dispositivi ad esso collegati, captare tutto il traffico di dati in arrivo ed in uscita, attivare, in maniera del tutto autonoma, il microfono e la *webcam*, fare copia di tutti i *file* presenti sull'*hard-disk*, visualizzare infine in remoto tutto ciò che viene visualizzato sullo schermo del dispositivo (*screenshot*) o sulla tastiera dello stesso

[205] Cfr. *Memoria per la Camera di Consiglio delle Sezioni Unite della Procura Generale presso la Corte di Cassazione* del 28 aprile 2016, in Internet al sito www.dirittopenalecontemporaneo.it.

(*keylogger*)[206]. In questo ampio panorama che descrive le molteplici potenzialità del captatore informatico, si deve andare ad inserire necessariamente il decreto di autorizzazione alle operazioni di intercettazione. Il problema fondamentale è il seguente: per quanto riguarda le funzionalità collegate alla fotocamera ed al microfono, esse possono essere considerate come intercettazioni ambientali, ma per le altre il discorso diviene più complesso in quanto il *download* di *file* da parte dell'agente intrusore potrebbe essere considerato un sequestro probatorio[207], la geolocalizzazione del dispositivo potrebbe implicare una sorta di pedinamento, mentre per altre funzioni esercitate dal captatore, come quella di *keylogger* o di *upload* di *file* sul dispositivo, non si riesce nemmeno a trovare una categoria giuridica corrispondente all'interno dei mezzi di ricerca della prova. Tutto ciò porta alla conclusione che, stando al dettato della normativa vigente, potrebbero essere necessari diversi decreti di autorizzazione per il medesimo captatore informatico: quello relativo a sequestro da parte del Pubblico Ministero, quello relativo alle intercettazioni ambientali da parte del GIP, relativamente al pedinamento esso può essere avviato anche su iniziativa della polizia giudiziaria, mentre per le altre due funzioni del captatore sopra citate, mancando una categoria di riferimento all'interno della disciplina dei mezzi di ricerca della prova, sembra alquanto complesso stabilire che tipo di provvedimento di autorizzazione possa rendersi necessario. Un aiuto, seppur di carattere minimo rispetto alla profonda e dettagliata normativa auspicabile in materia, si può desumere dalla Convenzione sul *Cybercrime* di cui ci si occuperà nei capitoli successivi.

[206] G. LA CORTE, *Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata*, in *Giur. pen. web*, 2017, 6.
[207] L. CHIRIZZI, *Computer Forensic. Il reperimento della fonte di prova informatica*, Laurus Robuffo, Roma, 2006.

# Capitolo 4

# Modalità di esecuzione delle operazioni intercettive

SOMMARIO: 1 – La necessaria "neutralità tecnica" delle intercettazioni. – 2 – L'applicazione e il funzionamento del *software* spia. – 2.1 – La fase di "infezione" del *device*. – 2.2 – Ricezione e conservazione dei dati captati. – 2.3 – Fase successiva alla conclusione delle indagini. – 3 – L'utilizzo del captatore in funzione di *keylogger*. – 4 – La captazione delle *e-mail* "bozza" e di *chat* sviluppatesi non contestualmente. – 5 – La possibilità di *download* dei *file* contenuti nel *device* e di *upload* di nuovi *file*. – 6 – Il pedinamento elettronico.

## 1 – La necessaria "neutralità tecnica" delle intercettazioni

La sentenza "Scurato", ampiamente analizzata nei capitoli precedenti, rappresenta un'ottima opera di ricostruzione, da parte delle Sezioni Unite, dei presupposti necessari affinché si possano autorizzare le operazioni relative alle intercettazioni tra presenti, liberando il mezzo di ricerca della prova di cui all'art. 266 c.p.p. dalla definizione di intercettazione ambientale legata esclusivamente alle tecnologie utilizzate risalente al momento in cui la legislazione in materia di intercettazioni era stata

inserita nel nostro ordinamento. Prendendo spunto da questo aspetto, sembra che la Suprema Corte abbia abbracciato il principio di "neutralità tecnica" della disciplina positiva del mezzo di ricerca della prova, principio inoltre già affermato a livello europeo in tema di protezione dei dati personali, secondo il quale la normativa dovrebbe poter trovare applicazione a prescindere dalla tecnologia utilizzata per ottenere un determinato scopo[208]. Come ricordato poc'anzi, il principio di "neutralità tecnologica" a livello comunitario è stato ufficialmente adottato dal Regolamento sulla Privacy e dalle nuove norme in materia di protezione dei dati personali dell'Unione Europea[209], ponendosi come strumento idoneo a non ostacolare future innovazioni tecnologiche. Tale principio trova applicazione quindi anche nel contesto relativo alla disciplina delle intercettazioni telefoniche, come opportunamente ricostruito dalle Sezioni Unite. In primo luogo, è stato sottolineato dai giudici di legittimità che la necessità di indicare lo strumento esatto tramite il quale espletare le operazioni di intercettazioni non trova alcuna giustificazione nell'attuale impianto normativo il quale, tra le altre cose, all'art. 268, comma 3, c.p.p., anche rispetto alle tradizionali intercettazioni telefoniche, è ben lontano dal promulgare un elenco tassativo nel momento in cui richiede genericamente di fare uso solo «degli impianti installati nella procura della

[208] G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni fra presenti*, op. cit.

[209] In particolare: regolamento (UE) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GUUE L 119 del 4 maggio 2016; direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in GUUE L 119 del 4 maggio 2016; direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GUUE L 281 del 23 novembre 1995.

Repubblica», conferendo inoltre il potere al Pubblico Ministero, con un semplice provvedimento motivato, di poter utilizzare impianti differenti. Inoltre, il rispetto della relativa doppia riserva di legge e di giurisdizione richiesta dalla Costituzione per qualsiasi tipo di intrusione nelle libertà fondamentali poste a tutela del domicilio privato e delle comunicazioni, non richiede, secondo il dettato normativo vigente, la necessità di avere una specifica previsione legislativa per ogni tipo di strumento captativo utilizzabile. Sotto questo aspetto, è stato correttamente sottolineato dalle Sezioni Unite che la Corte costituzionale ha già riconosciuto che l'art. 14 Cost. non va inteso in senso restrittivo in relazione ai mezzi di ricerca della prova lì indicati. Inoltre, la Procura generale presso la Corte di cassazione tramite la sua memoria ha puntualizzato che, nel momento in cui si decida di appoggiare un'interpretazione di questo tipo, ossia in senso restrittivo dell'art. 14 Cost., essa porterebbe al risultato paradossale di attribuire al domicilio una tutela maggiore rispetto a quella prevista per la libertà personale prevista dall'art. 13 Cost., il quale contiene una clausola di chiusura molto ampia e riferita, questa volta senza alcun dubbio interpretativo, a «qualsiasi altra restrizione della libertà della persona»[210]. Risulta quindi impossibile sostenere logicamente che, alla categoria delle intercettazioni operate tramite i captatori informatici, possa applicarsi la categoria delle c.d. prove "incostituzionali"[211].

---

[210] Cfr. *Memoria per la Camera di Consiglio delle Sezioni Unite della Procura Generale presso la Corte di Cassazione* del 28 aprile 2016, op. cit.

[211] A favore di questa tesi, fra gli altri, vedasi A. TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. e proc.*, 2015, p. 761. Inoltre, il concetto di prova incostituzionale, riconosciuto dalla Corte costituzionale a partire dalla sentenza 6 aprile 1973, n. 34, fa riferimento alla «prova assunta con modalità lesive dei diritti fondamentali del cittadino garantiti dalla Costituzione»: sul tema vedasi V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1974, p. 341. La configurabilità di tali prove incostituzionali è stata oggetto di un vivace dibattito dottrinale. Da un lato, si sosteneva che era possibile riconoscere invalidità processuali anche al di fuori del codice di procedura penale in caso di contrasto con le garanzie costituzionali, come sostenuto da G. ILLUMINATI,

Questa presa di posizione da parte delle Sezioni Unite risulta quindi totalmente in linea con quanto espresso dall'ordinamento comunitario per mezzo della Direttiva 2016/680, la quale prende in considerazione in modo specifico le sfide poste dalla rapidità dell'evoluzione tecnologica e dalla globalizzazione, analizzando al contempo le potenzialità intrusive che esse, intrinsecamente, rappresentano contro la tutela delle informazioni più sensibili dell'individuo, con particolare riferimento, all'interno della Direttiva stessa, ad «attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali». Sotto questo profilo infatti, il legislatore europeo specifica che «al fine di evitare che si corrano gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate»[212]. La "neutralità tecnica" richiesta dalla Direttiva 2016/680 appare quindi l'approccio più consono per regolare le nuove tecnologie. Risulta tuttavia auspicabile un intervento da parte del legislatore nazionale volto ad identificare, in modo chiaro e preciso, non tanto tutte le tecnologie utilizzabili nell'ambito delle operazioni intercettive ma, piuttosto, le garanzie fondamentali che devono essere in qualsiasi caso riconosciute all'indagato e ai possibili soggetti terzi coinvolti, a prescindere quindi dallo strumento utilizzato. Tale orientamento quindi, seppur sviluppato in un contesto parzialmente diverso, sembra legittimare la presa di posizione delle Sezioni Unite sull'utilizzabilità dei *trojans* per scopi di *surveillance*, anche in assenza di una specifica previsione normativa.

L'esclusione totale di tali tecnologie dal novero dei possibili strumenti di indagine penale rappresenterebbe un'opzione che, oltre ad essere

---

*L'inutilizzabilità della prova nel processo penale*, in *Riv. it. dir. proc. pen.*, 2010, p. 521; dal lato opposto, si sosteneva l'impossibilità di riconoscere una sanzione processuale in mancanza di una specifica invalidità processuale, così come affermato da N. GALANTINI, voce *Inutilizzabilità (dir. proc. pen.)* in *Enc. Dir. Agg. I*, Milano, 1997, p. 699.

[212] Cfr. art. 18 Direttiva 2016/680.

totalmente anacronistica, non prende in considerazione il dato incontrovertibile relativo all'utilizzo di sopra citate tecnologie da parte di organizzazioni criminali e quindi lascerebbe alle forze dell'ordine la categoria "residuale" delle tradizionali tecnologie captative, tendenzialmente superate ovvero facilmente eludibili.

# 2 – L'applicazione e il funzionamento del *software* spia

In una prima fase i virus *trojan* di captazione cellulare erano destinati ad avere vita breve per due motivi molto semplici ma cruciali: in primo luogo per ragioni legate all'autonomia d'impiego poiché l'attivazione del virus sul *device*, anche se occulta, aveva immediatamente fatto notare la criticità legata all'utilizzo eccessivo della batteria del dispositivo e al conseguente surriscaldamento; in secondo luogo, parallelamente all'utilizzo vistoso della batteria, si era registrato un utilizzo spropositato del traffico dati per via delle azioni di *download* e *upload* effettuate dal *software* spia tramite controllo remoto. Tuttavia, complici sia l'evoluzione tecnologica sia vari accordi stipulati dal Ministero della Giustizia con i gestori telefonici per "mascherare" i consumi eccessivi del traffico dati dell'utente, tali problemi sono stati in parte risolti[213].

Prima di iniziare ad analizzare come funziona, nello specifico, il virus *trojan* utilizzato per scopi di intercettazione, è utile specificare quale tipo di *software* viene utilizzato a tali fini. Il captatore informatico è infatti un *rootkit*, ossia un pacchetto offensivo in grado di infettare qualsiasi tipo di

[213] M. DI STEFANO, *Il captatore informatico "Trojan": stato dell'arte e profili giuridici,* in Internet al sito https://www.ictsecuritymagazine.com/articoli/captatore-informatico-trojan-dellarte-profili-giuridici/.

*device* (*computer, tablet, smartphone*) formato da uno *spyware* e da un *trojan*. Il *rootkit* permette quindi all'utilizzatore di tale *malware* di installare il captatore all'interno del sistema operativo del dispositivo prescelto, di solito in punto "remoto" di esso, in modo da rendere difficile la sua eliminazione da parte di possibili programmi di difesa, c.d. *antivirus*. Tali *software* quindi si comportano come programmi di *backdoor*, ossia rendono possibile connettersi in modalità remota al dispositivo "infetto". Una *backdoor*, nota anche come *trapdoor*, è quindi un punto di accesso, segreto, ad un programma che consente, ovviamente solo a chi ne è a conoscenza, di poter entrare senza dover utilizzare le normali procedure di controllo dell'accesso[214]. Esistono poi diversi tipi di *rootkit* ma quelli più conosciuti, ed utilizzati, sono sostanzialmente due, ossia quelli *user-mode* e quelli *kernel-mode*. I primi sono stati disegnati per poter operare nella parte del sistema operativo che contiene tutte le applicazioni, espletando quindi la loro funzione intercettando e modificando i processi relativi alle applicazioni e sovrascrivendo la memoria che viene usata durante tali processi. Il secondo tipo di *rootkit* invece agisce ad un livello più "basso" del sistema operativo, dando così al proprietario di tale programma un maggiore raggio di azione rispetto alle potenziali operazioni attuabili all'interno del dispositivo infettato. Essi infatti, dopo l'installazione, possono prendere il controllo di una qualsiasi funzione del dispositivo direttamente al livello più privilegiato, ossia quello dell'amministratore del dispositivo. Sono quindi quelli del secondo tipo i *rootkit* più pericolosi e quelli più difficili da individuare[215].

Il mezzo più efficace per poter sfruttare tutte le potenzialità offerte dai captatori informatici è quello di sfruttare un c.d. *0-day*, ossia una vulnerabilità all'interno del sistema operativo bersaglio non conosciuta,

[214] W. STALLINGS, *Sicurezza delle reti. Applicazioni e standard*, Pearson, 2007, p. 348.
[215] S. MALENKOVICH, *Che cosa sono i rootkit?*, in Internet al sito https://blog.kaspersky.it/che-cosa-sono-i-rootkit/645/.

non nota, nemmeno agli sviluppatori del programma in questione. Molti ritengono che essa sia denominata *0-day* in quanto è sfruttata per la prima volta il giorno in cui si lancia l'attacco tramite il suo utilizzo ma, in realtà, il termine *zero-day* è dovuto ad un motivo molto più semplice: il programmatore del codice vittima dell'attacco ha zero giorni per poter correggere, in qualche modo, il prodotto dopo che questo viene attaccato sfruttando una sua vulnerabilità intrinseca[216]. E' quindi possibile affermare che una *zero-day* può essere tranquillamente considerata come una *cyber-weapon* (un'arma informatica), in quanto altamente pericolosa. Un esempio su tutti può chiarire le potenzialità di un *exploit zero-day*, ossia un attacco portato avanti sfruttando tale vulnerabilità: nel 2006 il governo degli Stati Uniti d'America, con la collaborazione dello stato di Israele, sviluppò *Stuxnet*, uno dei virus informatici più distruttivi mai realizzati. La particolarità di tale programma era quella di poter danneggiare direttamente le strutture fisiche tramite dei *driver USB* infetti. Lo scopo di questo strumento informatico era quello di danneggiare le turbine della centrale Iraniana di Natanz, sfruttando alcune vulnerabilità appunto *zero-day* del sistema operativo *Windows*[217]. Secondo alcune fonti, specialmente secondo il parere di Edward Snowden (ex dipendente della CIA), tale virus era stato creato dall'NSA e i servizi di *intelligence* israeliana, in modo da poter rallentare lo sviluppo nel campo dell'atomica da parte dell'Iran. Quello che è importante sottolineare in questa sede è che lo sfruttamento della vulnerabilità *zero-day* rese praticamente impossibile fermare il propagarsi e l'agire del virus nelle fasi iniziali: esso fu scoperto solamente in quanto si replicò al di fuori della centrale di Natanz a causa di un mero errore di programmazione. Per questi motivi, la conoscibilità di tali vulnerabilità non ha prezzo, o meglio, il prezzo viene stabilito dal

[216] A. CONTINI, *ABC della sicurezza: Zero Day*, in Internet al sito http://www.techeconomy.it/2015/11/17/abc-sicurezza-zero-day/.
[217] D. VERGARA, *Stuxnet: il virus che sconvolse il mondo*, in Internet al sito http://tech.everyeye.it/articoli/speciale-stuxnet-virus-che-sconvolse-mondo-30317.html.

"venditore" in base ad un parametro fondamentale, ossia quanto essa è recente. Più sarà recente la *zero-day* più essa potrà essere rivenduta per una cifra elevata, nell'ordine dei milioni di dollari.

## 2.1 – La fase di "infezione" del *device*

Ogni virus informatico possiede proprie peculiarità, tuttavia ogni codice virale possiede uno schema basato su quattro fasi[218] che lo stesso codice percorre durante il suo periodo di "attività":

1) l'infezione. Durante questa fase il *malware* si introduce all'interno del sistema bersaglio e, superando eventuali barriere informatiche di sicurezza, si installa sul dispositivo. Successivamente il virus va a modificare le impostazioni del sistema adattandole ad esso stesso ed alle sue necessità, prima fra le quali quella di non essere rilevato dal sistema;

2) la quiescenza. In questa fase il virus rimane silente all'interno della memoria del dispositivo, in attesa che si verifichi una determinata condizione, a seguito della quale esso si attiva;

3) la replicazione e la propagazione. Sempre al determinarsi di certi eventi oppure di certe condizioni, il *malware* si replica ed inoltre seleziona i bersagli verso i quali propagarsi, infettando in questo modo altri sistemi;

4) le azioni malevoli. In questa fase invece si riscontra la vera natura del virus, in quanto a fronte di determinate condizioni o determinati eventi, esso svolge i suoi compiti malevoli, come ad esempio la distruzione o il furto dei dati contenuti nel dispositivo. Va sottolineato inoltre che, se il sistema non è compromesso in maniera definitiva, il virus ritorna alla fase

[218] A. DE SANTIS, *I malware*, in Internet al sito http://www.disrv.unisa.it/~ads/ads/Sicurezza_su_Reti_files/Lez01_I%20Malware.pdf.

della quiescenza.

In questa sede si analizzerà in particolare la prima fase, ossia quella di infezione. La prima cosa che deve fare il virus infatti è quella di inserirsi all'interno del dispositivo bersaglio e, se dovesse rendersi necessario, indurre la vittima a seguirlo. Va da sé che il virus non può presentarsi in forma esplicita all'utente che utilizza il dispositivo bersaglio ma deve essere mascherato all'interno di programmi apparentemente legittimi ed innocui. I canali principali attraverso i quali l'infezione può avvenire sono sostanzialmente tre:

1) il trasferimento fisico. Questa modalità era molto diffusa in passato e prevede l'utilizzo di un supporto fisico di memorizzazione, quali possono essere un *CD-ROM* o un'unità *USB*, per il trasporto e il successivo inoculamento dei virus nei sistemi informatici. Tali operazioni possono essere effettivamente compiute sia dall'agente intrusore sia dall'utente in maniera inconsapevole, esattamente come avvenuto per il virus *Stuxnet*;

2) tramite la posta elettronica. In questa situazione il *malware* risulta allegato ad un messaggio di posta elettronica, convincendo l'utente del dispositivo ad aprire il messaggio ed il suo allegato, il quale può essere un *file* eseguibile o anche un documento elettronico. L'esempio più famoso di infezione tramite posta elettronica è quello del virus "Melissa", il quale ha infettato oltre ottantamila sistemi nell'arco di un brevissimo periodo ed ha causato danni per più di un miliardo di dollari;

3) tramite il *Web*. Esso risulta essere il canale di diffusione più "efficiente" e, per questo motivo, quello più utilizzato, trasmettendo il virus tramite un *download* effettuato dall'utente da una pagina *web*. In questo caso la vittima può svolgere un ruolo sia attivo che passivo: nel primo caso infatti l'utente installa il *malware* scaricando un *file* in apparenza innocente; nel secondo caso invece l'agente intrusore utilizza delle tecniche, note come

*drive-by download*, le quali permettono il *download* automatico del codice virale alla semplice apertura di una determinata pagina *web*.

Nel caso dei captatori informatici tuttavia bisogna segnalare l'utilizzo di un'altra tecnica di infezione, comunemente denominata come *social engineering*. Questa tecnica utilizza metodi di comunicazione e di persuasione al fine di ottenere o compromettere informazioni personali riguardanti individui o società, tramite un vero e proprio studio, caso per caso, del soggetto da intercettare. L'utilizzo dei *social network* quali *Facebook* o *Instagram* riesce infatti a rivelare molto sulle abitudini e sulle caratteristiche personali di un individuo e, nel caso dell'installazione di un captatore informatico su un bersaglio che fa uso di tali strumenti, possono facilitare, certe volte in maniera più lieve altre in maniera più elevata, l'operazione di infezione di un determinato dispositivo in uso al bersaglio designato. Un tipo particolare di *social engineering* è rappresentato dal c.d. *phishing*, ossia una tecnica attraverso la quale si inganna la vittima al fine di farle rivelare dei dati personali, quali codici di accesso o dati finanziari, fingendosi un ente affidabile in una comunicazione digitale. In questi casi l'agente intrusore si finge un istituto di credito, un'azienda finanziaria o simili e contatta la vittima designata chiedendole, a volte in maniera nemmeno troppo velata, di comunicargli i propri dati personali al fine di risolvere determinati problemi[219].

Una volta penetrati nel sistema tramite i canali sopra descritti, i *malware*, in modo da poter operare nel dispositivo devono necessariamente modificare le impostazioni del sistema stesso. Tecnicamente, questa operazione si traduce nell'aumento dei privilegi di sistema attribuiti al virus, in quanto nell'ambito informatico, il privilegio di sistema disciplina e

[219] Ministero della Difesa, *Riconoscere ed evitare il fenomeno del social engineering e gli attacchi phishing*, in Internet al sito http://www.difesa.it/SMD_/Staff/Reparti/II/CERT/Tips_Tricks/Pagine/Fenomeno_social_engineering_attacchi_phishing.aspx.

classifica il livello di autorizzazioni ad operare sul sistema stesso attribuite ad un determinato programma. In linea generale esistono due livelli di privilegi, quello di "amministratore" e quello di "utente" e sono differenziati a seconda che una determinata operazione compiuta sul sistema possa o meno modificare le componenti importanti del sistema[220]. Il captatore informatico, in modo da acquisire tali privilegi, sfrutta una o più vulnerabilità, nella maggior parte dei casi quelle denominate *zero-day* e discusse nel paragrafo precedente.

## 2.2 - Ricezione e conservazione dei dati captati

Una volta eseguita l'attività di inoculazione del virus *trojan* all'interno del dispositivo prescelto l'agente intrusore può, dal proprio computer, agire inviando specifiche istruzioni al dispositivo infettato, costringendolo in questo modo ad eseguire le operazioni richieste dagli investigatori. Man mano che i dati vengono captati per mezzo del virus essi vengono inviati al server ricevente, non in maniera diretta (ossia tramite un collegamento *end-to-end*) ma utilizzando un metodo differente: ogni pacchetto di dati inviato contiene infatti sia l'indirizzo *IP*[221] ricevente che quello del mittente e, in modo da occultare ad una possibile analisi del dispositivo tali trasmissioni di dati e quindi il risalimento all'indirizzo *IP* ricevente, i produttori di tali virus *trojan* fanno in modo di interporre tra il bersaglio ed

[220] M. MEZZALAMA, A. LIOY, H. METWALLEY, *Anatomia del malware*, in *Mondo digitale n. 47*, settembre 2013.

[221] L'indirizzo *IP* è un numero che identifica un determinato dispositivo collegato ad una rete telematica, paragonabile quindi ad un indirizzo stradale o ad un numero telefonico. Tramite tale indirizzo infatti, il fornitore della connettività può risalire ai dati personali di colui che ha sottoscritto il contratto di utenza dei servizi di connessione.

il *server* ricevente una serie di ulteriori *server*, denominati *proxy* e i quali svolgono la funzione di occultare il reale indirizzo *IP* del destinatario dei dati estrapolati dal dispositivo bersaglio[222].

Un importante aspetto da dover sottolineare è quello relativo al tipo di accertamento che viene effettuato tramite le operazioni condotte dal virus *trojan*. Dopo l'inoculazione del virus e in particolar modo durante la fase di attivazione e captazione, il *software* rimane in costante attività, ad esempio ricevendo telefonate, inviando *sms*, ricevendo *e-mail* o navigando su Internet, e quindi si modifica in modo continuativo. Questo processo di modificazione solleva il dubbio, dal punto di vista processuale, relativo al tipo di attività condotta attraverso il *trojan*, delineandola come un'attività di tipo non ripetibile in quanto modifica di volta in volta il luogo virtuale nel quale il *malware* viene installato[223]. E' necessario quindi considerare che, qualsiasi prelievo di dati informatici eseguito tramite le modalità sopra descritte, deve essere effettuato nel rispetto di alcuni principi propri della disciplina della *Digital Forensics*[224] ed in particolare assicurare:

a) l'immodificabilità del contenuto della memoria del dispositivo *target*;

b) la conformità dei dati acquisiti rispetto ai dati originali;

c) la corretta conservazione dei dati acquisiti.

Tali principi, insieme ad altri che verranno analizzati nei capitoli successivi, sono stati cristallizzati dall'entrata in vigore della legge 18 marzo 2008, n.

---

[222] M. ZONARO, *Il Trojan – Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in *Dibattiti/Focus – Parola alla difesa*, 2016, pp. 163 e ss.

[223] F. BOSCO e C. VACIAGO, *La nuova cyber minaccia per la privacy: tutto ciò che sappiamo sui captatori informatici*, in Internet al sito https://www.agendadigitale.eu/infrastrutture/la-nuova-cyber-arma-di-distruzione-di-massa-per-la-nostra-privacy-i-captatori-informatici/.

[224] G. VACIAGO, *Digital Evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli Editore, Torino, 2012, pp. 12 e ss.

48[225], la quale ha sancito di fatto l'introduzione dei principi fondanti della *digital forensics* all'interno del nostro ordinamento, disciplinando aspetti fondamentali relativi alla gestione di quegli elementi di prova che, per loro natura, si caratterizzano per un'estrema fragilità e volatilità. L'art. 8, comma 1, della sopra citata legge è andata a modificare, ad esempio, l'art. 244, c.p.p., in tema di «Casi e forme delle ispezioni», inserendo un riferimento esplicito ai sistemi informatici o telematici, modificando così il comma 2 dell'articolo citato in precedenza in tale modo: «… anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Le previsioni dettate dalla legge 48/2008 quindi possono essere viste come un approccio volto a raggiungere le c.d. *best practices* utilizzate pedissequamente negli ordinamenti di *common law*, ossia quell'insieme di comportamenti non necessariamente codificati ma considerati dalla comunità scientifica come il miglior modo o il modo più corretto di operare, per svolgere una qualsivoglia attività in ambito scientifico e/o tecnologico[226].

Per quanto riguarda i principi elencati poc'anzi, il primo appare quasi scontato nel dichiarare che tutte le operazioni di controllo effettuate sul dispositivo e tutti i dati da esso estrapolati non devono subire alcuna modificazione ed inoltre la memoria del dispositivo bersaglio deve rimanere integra. A tal proposito potrebbe essere utile, anche se fino ad ora non sussiste nessun obbligo legislativo in tal senso, la predisposizione di un documento in cui vengono annotate tutte le operazioni effettuate tramite il virus *trojan*, documento che dovrebbe essere inoltre non modificabile tramite l'inserimento di un nuovo evento ed ogni nuova

[225] Con la legge 18 marzo 2008, n. 48 pubblicata in *Gazzetta Ufficiale* il 2 aprile 2008, n. 80, *Serie Ordinaria*, n. 79, viene recepita e al tempo stesso viene data attuazione alla Convenzione di Budapest sulla criminalità informatica.
[226] M. TONELLOTTO, *Evidenza informatica, computer forensics e best practices*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. VIII, n. 2, maggio-agosto 2014.

operazione inserita dovrebbe essere sottoposta a firma digitale. Per quanto riguarda invece il secondo principio, esso risulta di più difficile applicazione, poiché nelle normali procedure di acquisizione di dati informatici da supporti di memoria digitali, sia che esse vengano espletate a norma dell'art. 359 c.p.p. oppure dell'art. 360 c.p.p., la procedura prevede che possa essere possibile dimostrare la corrispondenza del dato acquisito tramite un confronto con il dato originale, ossia con il dato che rimane memorizzato sul dispositivo in sequestro. Nel momento in cui viene utilizzato il virus *trojan* per la captazione di dati da un determinato dispositivo, la dimostrazione, a posteriori, della conformità del dato estrapolato rispetto a quello originale diventa difficoltosa in quanto il dispositivo non è in sequestro e quindi non è nella disponibilità degli investigatori, senza considerare inoltre che, come specificato sopra, il virus continua ad operare per tutta la durata della sua "giacenza" all'interno del dispositivo intercettato, modificando quindi in maniera continuativa il suo contenuto. Tale difficoltà potrebbe essere superata, ad esempio, prevedendo l'implementazione nel sistema ricevente di una certificazione dei contenuti acquisiti tramite firma digitale e inserendo, al contempo, l'impossibilità di una loro modifica a posteriori e la creazione di un *log-report*[227] non modificabile e certificato, per ogni dato memorizzato. Il terzo punto infine prevede che i dati siano archiviati su supporti non riscrivibili unitamente ai *report-log* relativi ad essi, ossia i report che registrano le attività svolte dal captatore informatico, sia per le fasi di controllo del captatore sia per quanto riguarda le fasi di estrapolazione e acquisizione dei dati. Dal punto di vista strettamente tecnico, sono

[227] Il *file di log*, in generale, è un file in cui sono memorizzate tutte le attività compiute da un determinato utente e permette, in sostanza, di ricostruire la sua attività all'interno del computer o sulla Rete. In questo caso è intuibile che tale file avrà il compito di ricostruire non l'attività dell'utente bensì quella compiuta dal captatore.

sostanzialmente tre i rimedi utili[228] per poter applicare i tre principi sopra descritti:

1) La copia *bit stream*, ossia il procedimento di copia del dispositivo informatico intercettato che permette di ottenere un dispositivo identico a quello originale in tutte le sue caratteristiche e funzioni, ivi comprese delle parti del dispositivo in cui possono "risiedere" i dati cancellati.

2) La procedura di *write blocker*, consistente nell'applicazione di *software* o *hardware* i quali impediscono l'erronea scrittura di dati sul dispositivo intercettato durante la fase di copia dei dati.

3) Il sistema di *hashing*, il quale consiste in un procedimento puramente informatico che prevede la generazione di un codice alfanumerico identico per l'originale e per la copia effettuata: in caso di un'alterazione, essa genera automaticamente un diverso codice *hash*, dimostrando immediatamente l'alterazione dei dati, rappresentando così una sorta di "impronta digitale" informatica.

In ultimo va segnalato un problema di natura logistica relativo ai *server* dove tali dati vengono inviati. L'allocazione fisica dei *server* è infatti presso le procure della Repubblica, tuttavia i dati sono captati tramite il mandato affidato a società terze ed estranee alle forze di polizia giudiziaria normalmente assegnatarie delle operazioni intercettive, per cui la procura risulta essere l'utente del *server* mentre la società terza figura in qualità di amministratore. Si profilano quindi diversi aspetti problematici legati al

---

[228] Tali procedimenti sono ampiamente descritti da S. ATERNO, *La prova informatica nella giurisprudenza*, Corso di formazione, Università di Catania, 3 giugno 2013, in Internet al sito http://www.dmi.unict.it/~battiato/CF1213/Aterno_Catania_prova%20digitale_%202013.pdf. Sempre sullo stesso tema, vedasi anche S. ATERNO, *Il "captatore informatico": uno strumento d'indagine tra esigenze investigative e garanzie difensive*, in Internet al sito https://www.slideshare.net/jbluesj/il-captatore-informaticouno-strumento-dindagine-tra-esigenze-investigative-e-garanzie-difensive.

possesso dei dati captati da parte di tali società: in primo luogo anche terze persone potrebbero accedere al dispositivo posto sotto intercettazione, ad esempio dipendenti o ex-dipendenti della società che effettua tale operazione ed infine, ci si deve interrogare sulla "destinazione finale" dei dati captati alla fine delle operazioni intercettive ovvero, in parole più semplici, che fine fanno i dati che vengono captati dopo la conclusione delle indagini.

## 2.3 – Fase successiva alla conclusione delle indagini

Dopo aver ottenuto le prove digitali attraverso lo strumento del captatore informatico si profila un altro aspetto fondamentale della *digital forensics*, ossia la conservazione del dato digitale. La dottrina italiana[229] e le *best practices* internazionali[230] hanno suggerito diverse modalità operative al fine di non alterare in alcun modo la prova acquisita, le quali sono state analizzate nel corso del paragrafo precedente. Per quanto riguarda il panorama legislativo italiano, il codice di procedura penale, precisamente agli artt. 259, 260 e 261, stabilisce che le cose sottoposte a sequestro siano affidate in custodia alla cancelleria o alla segreteria del Pubblico Ministero. In particolare, l'art. 259 c.p.p., al comma 2, prevede che «quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o

[229] Tra tutti G. ZICCARDI, *La procedura di analisi della fonte di prova digitale*, in *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, di L. Luparia e G. Ziccardi, Giuffrè, 2007.

[230] Tra tutte le linee guida tracciate dalla Association of Chief Police Officers e disponibili in Internet al sito http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

l'accesso da parte di terzi». In modo quindi da garantire una c.d. corretta catena di custodia, occorre documentare tutto ciò che è stato fatto con la prova originale e con le copie forensi realizzate, a partire dal momento dell'acquisizione fino ad arrivare al giorno del processo. Il primo passo risulta essere quindi la redazione di un verbale apposito in cui viene annotato: numero del caso, reparto investigativo, investigatore assegnato al caso, natura e breve descrizione del caso, supporto sul quale viene copiato il dato informatico estrapolato, numero di serie del supporto, produttore del supporto stesso. Ogniqualvolta poi il supporto viene affidato ad un nuovo investigatore, ad un perito, ad un consulente tecnico di parte oppure ad un incaricato degli uffici del Tribunale, tale operazione dovrebbe essere annotata in apposito verbale. Giuridicamente parlando quindi, la documentazione e la conservazione della prova acquisita sono imposte dal principio del contraddittorio nella formazione della prova in quanto l'evidenza digitale deve essere conservata in modo tale da permettere alla controparte di effettuare le relative indagini, perizie e valutazioni su un elemento di prova perfettamente identico a quello acquisito in sede di indagini.

Per quanto riguarda il captatore informatico nello specifico, la conclusione delle indagini fa sorgere due profili problematici da non sottovalutare: il primo è relativo alla rimozione del captatore stesso dal dispositivo sottoposto ad intercettazioni; il secondo invece è attinente alla effettiva e materiale conservazione dei dati estrapolati. Per quanto attiene al secondo profilo, come è stato già esposto nel corso del paragrafo precedente, i dati estrapolati dal captatore informatico dovrebbero essere allocati presso i *server* situati fisicamente presso le procure della Repubblica. Tuttavia, poiché tali intercettazioni vengono effettuate tramite "l'utilizzo" di ditte terze e non degli agenti della polizia giudiziaria, si corre il rischio, non di lieve entità, che i dati captati siano nella disponibilità di terze persone, quali, ad esempio, i dipendenti della società stessa. Inoltre, i *server* sono

posti solo fisicamente nelle procure, ma l'accesso a detti sistemi informatici in qualità di amministratore può essere effettuato dalle ditte proprietarie dei *server* stessi, con la possibilità quindi di ottenere e di immagazzinare i dati del soggetto sottoposto ad intercettazioni. Si può certo pensare che, una volta concluse le indagini, le ditte assegnatarie di tali operazioni intercettive eliminino tutti i dati intercettati e che quindi essi rimangano nella sola disponibilità delle procure della Repubblica, tuttavia una normativa *ad-hoc* sul tema permetterebbe sicuramente di porsi meno interrogativi sul punto, in modo tale da non permettere in alcun modo che l'attività investigativa sfugga di mano agli agenti della polizia giudiziaria. Per quanto attiene al primo profilo precedentemente esposto invece, bisogna sottolineare che il captatore, una volta installato sul dispositivo bersaglio, non può essere né facilmente identificato per ovvie ragioni ma al contempo non può esseere nemmeno facilmente rimosso, rimanendo quindi giacente all'interno del dispositivo[231]. Nonostante l'utente possa accorgersi di varie "irregolarità" durante l'utilizzo di un dispositivo (quali possono essere una particolare lentezza nella connessione ad Internet, un consumo esagerato della batteria, caratteri digitati da tastiera che compaiono dopo più secondi etc.), secondo quanto spiegato nei paragrafi precedenti, utilizzando una vulnerabilità *zero-day*, ossia non conoscibile a priori, il virus inoculato diventa molto difficile da rimuovere e, senza ombra di dubbio, molto costoso per il soggetto sottoposto ad indagini tramite intercettazioni nel caso in cui egli abbia bisogno di affidarsi ad un esperto informatico ovvero a ditte specializzate in "bonifiche informatiche".

[231] Così evidenziato da F. BOSCO e C. VACIAGO, *La nuova cyber minaccia per la privacy: tutto ciò che sappiamo sui captatori informatici*, op. cit.

# 3 – L'utilizzo del captatore in funzione di *keylogger*

Il monitoraggio occulto realizzato attraverso lo strumento del captatore può, come sottolineato precedentemente, assumere diverse forme. La prima che bisogna analizzare è quella in cui il *malware* agisce in funzione di *keylogger*, ossia un *software* che permette di creare dei *file* di *log* contenenti tutto quello che viene digitato attraverso la tastiera, sia essa fisica o virtuale, del dispositivo. Tali *file* possono essere inoltre visualizzati in tempo reale oppure acquisiti in differita, da remoto, da parte del soggetto controllore[232]. Esistono poi due diverse tipologie di *keylogger*, una in formato *hardware* ed una in formato *software*. Per quanto riguarda la prima, di solito essa consiste in un micro dispositivo elettronico dotato di cavetto, di aspetto simile ad una prolunga, che viene collegato tra il cavo della tastiera e il computer, riuscendo quindi a catturare e memorizzare in un unico *file* di testo tutte le *password* e qualsiasi altro dato digitato dall'utente sulla tastiera. La seconda tipologia invece, quella di tipo *software*, è quella che viene utilizzata dagli investigatori e consiste in un programma spia o c.d. *sniffer* (letteralmente, "annusatore"), in grado di memorizzare in un *file* di *log*, totalmente nascosto all'utente del dispositivo, le attività svolte con il dispositivo, captando tutte le digitazioni che avvengono da tastiera, registrandole e poi inviandole ad un computer remoto dal quale il soggetto controllore opera.

Per capire meglio il funzionamento di tale programma può essere utile analizzare un caso concreto. Nella fattispecie in esame, durante un'indagine relativa ad un'associazione per delinquere finalizzata allo

[232] C. CONTI e M. TORRE, *Spionaggio informatico nell'ambito dei social network,* in *Le indagini atipiche*, in collana *Leggi penali tra regole e prassi*, diretta da A. Scafati, Giappichelli Editore, 2014, p. 415.

spaccio di sostanze stupefacenti, gli investigatori hanno inserito un virus *trojan* all'interno di un Internet Point utilizzato dai soggetti sottoposti ad indagini in modo da accedere ai loro *account* di posta elettronica aperti sul *provider hotmail.com*. Attraverso il *software* di *keylogger* gli inquirenti acquisivano quindi le *password* di accesso ai sopra citati *account* e le utilizzavano per carpire elementi utili ai fini investigativi, visionando i messaggi contenuti nella posta in entrata ed in uscita, nonché le *e-mail* contenute nella cartella "bozze". Il caso è stato oggetto di decisione da parte della Suprema Corte[233] la quale ha stabilito alcuni capisaldi tramite il seguente iter logico del suo percorso argomentativo:

1) il *keylogger* risulta equiparabile ad una microspia;

2) nel caso in esame in particolare, il programma *keylogger* risulta utilizzato come una semplice microspia in quanto non ha svolto, come normalmente succede nell'utilizzo dei virus *trojan*, un'attività di monitoraggio in tempo reale dell'attività svolta sullo schermo del dispositivo, per cui la sua attività risulta essere poco rilevante[234];

3) i messaggi di posta elettronica non rientrano nel concetto di corrispondenza tutelato costituzionalmente;

4) in ogni caso, nel caso in esame, le *e-mail*, siano esse inviate o ricevute, sono state acquisite dagli agenti inquirenti utilizzando la disciplina delle intercettazioni e tramite il decreto autorizzativo emanato dal GIP, "coprendo" in tal modo l'operato della Procura;

---

[233] Cass. sez. IV, 28 giugno 2016, n. 40903/16, in *C.E.D. Cass.* n. 268228, con commento di M. SENOR, *Di trojan-microspia, e-mail che non sono corrispondenza e della colpa veniale di chi usa server stranieri*, in Internet al sito http://www.medialaws.eu/di-trojan-microspia-e-mail-che-non-sono-corrispondenza-e-della-colpa-veniale-di-chi-usa-server-straneri/.

[234] «Si è usato il programma informatico, in altri termini, 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 veniva svolta su un determinato schermo», cfr. *ibidem*.

5) per quanto riguarda invece le *e-mail* rinvenute nella cartella "bozze" all'interno degli *account* dei soggetti indagati aperti presso il *provider* americano *hotmail.com*, essa può essere ricollegata ad un'attività di indagine estranea a quella relativa all'intercettazione di flussi di comunicazioni telematiche, per cui non risulta essere necessaria l'autorizzazione da parte del GIP;

6) poiché tali documenti in formato "bozza" non rientrano nel concetto di corrispondenza costituzionalmente tutelato, non si dovrà nemmeno ricorrere al rispetto della procedura di cui all'art. 254, c.p.p.;

7) infine, non può trovare applicazione neppure l'art. 254-*bis*, c.p.p., poiché, pur trattandosi nel caso in esame di dati informatici, essi non sono da considerare detenuti dal fornitore del servizio di posta elettronica sui suoi *server* situati all'estero, bensì dal singolo utente che detiene le *password* di accesso a tali *account*.

Relativamente a tale pronuncia, sono state numerose le critiche[235] in particolare su due aspetti evidenziati dalla Suprema Corte. In primo luogo, la comparazione tra il captatore informatico in funzione di *keylogger* ed una semplice e normale microspia. La capacità intrusiva dei captatori informatici infatti sono ben note e di certo non sono paragonabili a quelle di una microspia utilizzata per le intercettazioni ambientali o telefoniche. In secondo luogo invece, non può dirsi che le garanzie difensive siano da considerare rispettate solo perché è presente, agli atti, un decreto di autorizzazione da parte del GIP che copre qualsiasi attività di indagine svolta dagli inquirenti, a differenza di quanto disciplinato espressamente nel codice di procedura penale per quanto riguarda i mezzi di ricerca della prova. Nel caso in esame infatti, risulta palese che, tramite l'inoculazione

[235] Vedasi, ad esempio, L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in Internet al sito http://www.penalecontemporaneo.it/upload/GIORDANO_2017a.pdf.

e l'utilizzo del captatore informatico all'interno dei computer dell'Internet Point, si sia svolta un'operazione inizialmente di perquisizione, di tipo elettronico, la quale ha condotto all'acquisizione delle *password*, quindi ad un sequestro, il tutto "travestito" da intercettazione al fine di poter indagare senza dover necessariamente avvisare l'indagato, realizzando quindi una lesione dei diritti dell'indagato e al contempo, venendo meno il requisito necessario di un decreto autorizzativo apposito. Sembra quindi che, al fine di non violare i principi espressi nella pronuncia "Scurato" in tema di captatori informatici, sia stato ammesso l'utilizzo del captatore informatico in formato di *keylogger*, paragonandolo ad una merca cimice, in modo da poter preservare l'acquisizione di prove le quali avrebbero potuto, altrimenti, essere dichiarate inutilizzabili. Ritornano infine i dubbi espressi nei paragrafi precedenti riguardanti l'inquadramento giuridico, in termini rigorosi, del captatore informatico, nonché, di conseguenza, la possibile necessità dell'emanazione di diversi decreti autorizzativi per le operazioni svolte tramite il captatore.

# 4 – La captazione delle *e-mail* "bozza" e di *chat* sviluppatesi non contestualmente

La decisione della Suprema Corte esposta nel paragrafo precedente induce a riflettere quindi anche sulla captazione delle *e-mail* pervenute al destinatario ovvero inviate dal medesimo ed archiviate nella casella di posta elettronica, con la possibilità inoltre di comparare tale operazione anche alle *chat* sviluppatesi non contestualmente tra il soggetto sottoposto ad indagini e soggetti terzi. Secondo la sopra citata pronuncia quindi, in modo che sia integrata la disciplina sulle intercettazioni, non occorre il requisito dell'attualità della comunicazione rispetto al processo

acquisitivo posto in essere dagli inquirenti, essendo quindi sufficiente il dato storico dell'inoltro del messaggio, anche qualora esso sia precedente al decreto autorizzativo emesso per tale intercettazione. Su questo punto in particolare la sentenza della Cassazione prende spunto da un indirizzo giurisprudenziale elaborato in merito ad un procedimento relativo alle *chat* di *Blackberry*. Secondo tale indirizzo era infatti risultata legittima l'acquisizione di tali conversazioni mediante intercettazioni ai sensi dell'art. 266, c.p.p., in quanto esse rappresentano un flusso di comunicazioni, anche se non contestuali[236]. Sembra quindi che il superamento del presupposto necessario della captazione in tempo reale dei dati acquisiti tramite intercettazione vada a minare uno dei principi fondamentali di tale disciplina, ossia quello secondo il quale le intercettazioni sono un mezzo di ricerca della prova rivolto "al futuro" e non al passato come stabilito nella sopra menzionata pronuncia. Per quanto riguarda poi le *chat* sviluppatesi invece contestualmente, si segnala un altro orientamento elaborato dalla la giurisprudenza[237], il quale afferma che la polizia giudiziaria può utilizzare anche i dati segnalati sul *display* di un telefono cellulare seppur in assenza di autorizzazione da parte del GIP, in quanto tali elementi non sono assimilabili al contenuto di conversazioni o comunicazioni telefoniche, per cui gli organi investigativi potrebbero rilevare in tempo reale il messaggio pervenuto sul cellullare e, in modo molto semplice, trascrivere il tutto nel verbale di annotazione, senza incorrere in alcuna violazione[238].

Analizzando invece il regime per l'acquisizione delle *e-mail*, la dottrina

---

[236] Cass. sez. III, 10 novembre 2015, n. 50452, in *C.E.D. Cass.*, n. 265615; Cass. sez. IV, 8 aprile 2016, n. 16670, in *C.E.D. Cass.*, n. 266983.

[237] Cass. sez. IV, 8 maggio 2003, Lanzetta, in *Cass. pen.*, 2006, p. 536, con nota di S. RENZETTI, *Acquisizione dei dati segnalati sul display del cellulare: il rischio di una violazione dell'art. 15 Cost.*

[238] Contrariamente a tale impostazione vedasi C. SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui*, in *Le indagini atipiche*, op. cit., p. 41.

afferma che i messaggi già letti vanno trattati come «lettere già aperte, dissigillate, *id est* documenti informativi coperti dalla riservatezza che garantisce le informazioni di carattere personale[239]», per cui bisognerebbe applicare la disciplina in materia di sequestro di corrispondenza così come dettata dagli artt. 254, comma 2, e 353, c.p.p. Secondo la prevalente dottrina inoltre, il criterio di base da utilizzare è quello che si riscontra nel «requisito di natura temporale costituito, per così dire, dall' "attualità" della comunicazione rispetto all'atto acquisitivo[240]», sottolineando quindi, di fatto, il problema relativo alle *e-mail* in formato "bozza". Parte della dottrina[241] obietta che, nel momento in cui il soggetto che riceve il contenuto *e-mail* acquisendo di conseguenza l'elemento di conoscenza intrinseco ad esso, viene meno la natura stessa di corrispondenza attiva, per cui da quel momento si può reputare perfezionata la fattispecie complessa del flusso comunicativo e, di conseguenza, applicare l'art. 266-*bis*, c.p.p.. D'altro canto invece, secondo la decisione della Suprema Corte, l'acquisizione delle *e-mail* in formato "bozza" viene giustificato tramite la disciplina relativa al sequestro. La pronuncia infatti definisce una "bozza" come un documento non assimilabile alla corrispondenza, poiché il messaggio, essendo appunto una mera "bozza", non risulta spedito al destinatario. La detenzione inoltre, risulta essere effettuata dall'utente e non dal proprietario del *server* dove è ospitato l'*account* del soggetto, in quanto l'utente è l'unico depositario delle *password* per poter accedere al suo *account* e prendere visione dei dati ivi contenuti[242]. L'iter

[239] R. ORLANDI, *Questioni in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 134.
[240] Testualmente, F. ZACCHE', *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. e giust.*, 2013, p. 108.
[241] E. M. MANCUSO, *L'acquisizione di contenuti e-mail*, in *Le indagini atipiche*, op. cit., p. 70.
[242] Con riferimento alla sentenza in esame si veda M. S. DE NOZZA, *E-mail parcheggiate all'estero, similitudine con il cloud computing: La parola della Cassazione*, in *Sic. e giust.*, 2016, 4, p. 51, il quale sottolinea che, tramite il punto sopra affermato dalla Corte di Cassazione, si possa escludere la necessità di una rogatoria internazionale per poter richiedere l'accesso a tali *e-mail*.

logico seguito dai giudici di legittimità sembra quindi valorizzare il criterio dell'inoltro ossia l'invio del messaggio e non la contestualità della captazione rispetto alla conversazione da parte di chi invia a chi riceve distinguerebbe il confine tra l'applicazione della disciplina delle intercettazioni e quella del sequestro. In altre parole, poiché le *e-mail* erano "parcheggiate" nella cartella "bozze" senza risultare essere inoltrate, allora il sequestro era l'alternativa possibile ed utilizzabile.

Diverso infine risulta essere il procedimento per un'effettiva utilizzabilità dei risultati probatori a seconda che si sia all'interno della disciplina del sequestro o che invece venga applicata quella delineata dall'art. 266-*bis* del codice di procedura penale. Nel primo caso, si richiede l'adozione di metodiche di *legal imaging* volte a rendere conformi all'originale eventuali copie dei dati acquisiti, oltre che immodificabili, controllabili e replicabili. L'adozione di tali tecniche permette quindi l'utilizzabilità dei risultati dell'attività di copia dei contenuti *e-mail*, salvo poi permettere, in sede di contraddittorio dibattimentale, una verifica di affidabilità del metodo acquisitivo utilizzato. Per quanto riguarda invece i risultati frutto dell'attività di captazione della corrispondenza *e-mail* disposta a norma dell'art. 266-*bis*, c.p.p., poiché esse sono «entità formate "nel" e "per" il procedimento, in virtù delle operazioni di duplicazione dei flussi informatici confluiti sul *server* della procura[243]», esse potranno entrare nel compendio decisorio a seguito solamente delle operazioni di deposito e stralcio, tuttavia essendo necessario procedersi alla trascrizione e stampa così come stabilito dall'art. 268, comma 7, c.p.p., «osservando le forme, i modi e le garanzie previste per l'espletamento delle perizie».

[243] Così descritte da F. ZACCHE', *L'acquisizione della posta*, op. cit. p. 110.

# 5 – La possibilità di *download* dei *file* contenuti nel *device* e di *upload* di nuovi *file*

Come è stato specificato nei paragrafi precedenti, esiste una differenza tra le attività di *on line search* e *on line surveillance*, a seconda del tipo di funzione che l'agente intrusore, in generale quindi gli organi di investigazione, desidera che il captatore informatico compia. La possibilità di *download* dei *file* contenuti nel dispositivo bersaglio si pone all'interno della prima categoria, in quanto il virus *trojan* agisce come un vero e proprio "copiatore". Esso viene inoculato all'interno del dispositivo sottoposto ad intercettazioni e, in maniera occulta, estrapola dati ed informazioni che, una volta "copiati", vengono trasmessi ad intervalli di tempo regolari oppure prestabiliti agli organi investigativi, utilizzando un indirizzo *IP* prestabilito, in modalità nascosta e protetta. Per queste ragioni si potrebbe parlare più di "copiatore informatico" piuttosto che di captatore informatico[244]. Il fine di questa tecnica è quello di cercare ed acquisire per il procedimento documenti e dati utili per l'accertamento del fatto. Tale fine è disciplinato specificamente dal codice di procedura penale nella parte relativa agli atti di perquisizione, al sequestro e alla richiesta di consegna, i quali, nel momento in cui vengono eseguiti su sistemi informatici o telematici, devono essere compiuti secondo le nuove modalità previste dalla legge 18 marzo 2008, n. 48[245]. Le ispezioni, le

[244] M. TORRE, *Mezzi di ricerca della prova informatica e garanzie difensive: dagli accertamenti investigativi al virus di Stato – 15 luglio 2015*, in *Le indagini atipiche – Perquisizioni on line e captatore informatico nel diritto vivente*, in Internet al sito http://www.fondazioneforensefirenze.it/uploads/fff/files/2015/2015.II/2015.07.15%20Mezzi%20ricerca%20prova%20informatica/Slides%20Dott_%20Marco%20Torre.pdf.

[245] P. TONINI, *Manuale di procedura penale*, XII ed., Giuffrè, Milano, 2011, pp. 370 e ss. in cui si spiega che il legislatore, con la legge di cui sopra, ha previsto, relativamente ai mezzi di ricerca del documento informatico, una serie di «garanzie fondamentali, che dovrebbero essere attuate in ognuno dei mezzi di

perquisizioni e i sequestri relativi a sistemi informatici quindi non possono essere eseguite con una modalità qualunque, poiché il codice di procedura penale, nello specifico agli artt. 244, comma 2, 247, comma 1-*bis*, 259, comma 2, richiede espressamente l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali acquisiti o ad impedirne l'alterazione, nel momento dell'acquisizione o successivamente. In tal modo viene giustificata l'inoculazione di un programma informatico, in particolare del captatore informatico, al fine di eseguire la perquisizione informatica e copiare tutti i dati e i documenti presenti nel dispositivo bersaglio. Tuttavia, per quanto riguarda il primo aspetto analizzato in questo paragrafo, ossia il *download* dei *file* presenti nel *device* oggetto di intercettazione, si pongono dei dubbi di natura giuridica. In primo luogo, ispezioni, perquisizioni e sequestri sono per loro natura attività palesi, invece lo strumento investigativo del captatore informatico è occulto, in quanto il soggetto indagato non è a conoscenza della sua presenza all'interno del dispositivo a lui in uso[246]. In secondo luogo, l'ispezione e la perquisizione si concludono nel tempo necessario a verificare la presenza ovvero l'assenza delle possibili fonti di prova nel luogo o sulla persona indicata all'interno del decreto autorizzativo e, in caso, di apprenderle. Per quanto riguarda invece il captatore informatico, è stato già sottolineato che questo requisito è del tutto assente in tale strumento investigativo, in quanto esso rimane sul dispositivo "infettato" per un tempo indeterminato. Per tale motivo non può rientrare all'interno del concetto di perquisizione il programma spia inoltrato e lasciato all'interno del computer di un soggetto indagato ad oltranza, al fine di copiare

---

ricerca». Tali garanzie risultano essere: l'impossibilità di alterare il dato informatico originale; l'impossibilità di un'alterazione successiva; la necessità di formare una copia che assicuri la conformità del dato acquisito rispetto a quello originale; la presenza di sigilli informatici su tutti i documenti acquisiti; l'impossibilità di un'alterazione perfino della copia effettuata in un momento successivo.

[246] M. TROGU, *Sorveglianza e "perquisizione" on-line su materiale informatico*, in *Le indagini atipiche*, op. cit., pp. 444 e ss.

qualsivoglia dato e sequestrare indistintamente tutti i *file* e i dati elaborati[247]. In ultimo, va sottolineato che, nonostante la giurisprudenza prevalente affermi che il decreto che autorizza la perquisizione non debba necessariamente contenere l'indicazione esatta e precisa di tutte le cose pertinenti al corpo del reato che dovranno essere apprese, rimane tuttavia in piedi il principio secondo il quale all'esito della perquisizione l'autorità procedente potrà legittimamente sottoporre a sequestro unicamente le cose utili all'accertamento dei fatti e non, come nel caso dei dati carpiti dal captatore informatico, qualsiasi oggetto rinvenuto sul posto. Sembra quindi che, per quanto attiene all'aspetto relativo al *download* dei *file* contenuti sul dispositivo, ci si trovi di fronte ad un'attività di ricerca della prova che viola il diritto alla riservatezza dei soggetti indagati[248].

Per quanto riguarda l'aspetto relativo alla possibilità di *upload* di *file* sul dispositivo sottoposto ad intercettazioni, esso risulta essere un aspetto molto problematico relativamente alla natura dei captatori informatici. Il rischio in cui si può incorrere, senza la necessità di evocare teorie complottiste, è quello della c.d. *Evidence Planting*, ossia del piazzamento di prove[249]. I dubbi relativi a questa effettiva potenzialità del captatore informatico sono venuti a galla dopo lo scandalo che ha colpito la società Hacking Team[250]. In particolare, l'utilizzo del captatore informatico, allo

[247] Allo stesso modo, ad esempio, un decreto di perquisizione o di sequestro domiciliare non potrà mai autorizzare la presenza di un agente di polizia giudiziaria delegato all'esecuzione per giorni interi anche dopo aver cercato infruttuosamente le cose indicate nel decreto sopra citato.

[248] Così sostenuto da S. MARCOLINI, *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, di F. Ruggeri e L. Picotti, Giappichelli Editore, Torino, 2011, pp. 339 e ss.

[249] Si pensi, ad esempio, alla possibilità da parte di chi controlla il captatore informatico inoculato all'interno del dispositivo in uso ad un soggetto terzo, di "piazzare" delle foto di carattere pedopornografico al suo interno e dei possibili effetti che tale condotta può avere.

[250] M. FLORA, *Hacking Team: di cosa dovete DAVVERO avere paura*, in Internet al sito http://mgpf.it/2015/07/09/hackingteam-di-cosa-dovete-davvero-aver-

stato attuale, non sembra offrire sufficienti garanzie per quanto riguarda il controllo di eventuali abusi dello stesso strumento da parte di qualsivoglia soggetto. Considerando quindi la delicatezza e l'intrusività di questo tipo di indagini condotte mediante l'utilizzo del captatore informatico, sarebbe desiderabile, soprattutto considerando che tali intercettazioni vengono gestite non dalla polizia giudiziaria stessa ma da ditte esterne, ad esempio, una contemporanea attività di intercettazione telematica con rimando in tempo reale ai computer della polizia giudiziaria, la quale potrebbe assumere un carattere di monitoraggio di quelli che sono gli utilizzi del captatore informatico all'interno del dispositivo "infettato", preservando così il soggetto indagato da eventuali *upload* di nuovi programmi o documenti, siano essi anche realizzati involontariamente[251].

# 6 – Il pedinamento elettronico

L'ultima attività tipica del captatore informatico è quella della geolocalizzazione, ossia la possibilità di monitoraggio dei movimenti dell'individuo sottoposto ad indagini, tramite l'attivazione del sistema GPS, *Global Positioning System*. Sostanzialmente quindi, tramite meccanismi di localizzazione satellitare, si possono tracciare gli spostamenti di un veicolo o di una persona "a distanza"[252]. Il vuoto normativo creato dall'assenza appunto di una previsione normativa *ad hoc* è stato riempito dalla giurisprudenza di legittimità, la quale tende a caratterizzare tale attività

---

paura.html; e ancora, M. SCHIAFFINO, *Virus, manipolazione e false prove: tutti i rischi dei Trojan usati dallo Stato*, in Internet al sito http://www.ilfattoquotidiano.it/2016/06/07/virus-manipolazione-e-false-prove-tutti-i-rischi-dei-trojan-usati-dallo-stato/2801363/.

[251] L. MONTEVERDE, *Le nuove "frontiere" delle intercettazioni*, in *Arch. pen.*, 2014, n. 3, p. 11.

[252] M. STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova atipica*, in *Dir. pen. proc.*, 2011, p. 213.

svolta dal captatore come un mero pedinamento[253], riuscendo in tal modo a separare il suo utilizzo dal rispetto della c.d. doppia garanzia, ossia l'autorizzazione a detto uso da parte del giudice nei casi e nei modi previsti esclusivamente dalla legge, al contrario di quanto sostenuto da parte della dottrina[254]. Bisogna inoltre capire la effettiva e corretta qualificazione giuridica di tale modalità investigativa, in quanto non espressamente disciplinata. In primo luogo è stato sostenuto che l'attività di rilevamento satellitare potesse essere assimilata ad un'ispezione personale[255], ipotesi scartata in quanto non compatibile con quanto stabilito dal codice di procedura penale in merito alle ispezioni, siano esse reali o personali. Non può inoltre integrare un accertamento urgente sui luoghi, sulle cose e sulle persone così come disciplinato dall'art. 354 c.p.p., in quanto tale attività è svolta con il fine di conservare tracce o cose pertinenti al reato, fine quindi diverso da quello relativo alla localizzazione. Il monitoraggio GPS non risulta nemmeno inseribile nella categoria degli accertamenti, rilievi segnaletici, descrittivi o fotografici ed

[253] Cfr., tra le altre, Cass. sez. V, 30 ottobre 2010, in *Dir. pen. proc.*, 2010, n. 1464; Cass. sez. I, 28 maggio 2008, in *C.E.D. Cass.*, n. 240092; Cass. sez. I, 10 gennaio 2012, n. 14529, inedita; Cass. sez. V, 10 marzo 2010, n. 9667, in *Dir. pen. proc.*, 2010, p. 1464; Cass. sez. IV, 29 gennaio 2007, n. 8871, in *Cass. pen.*, 2008, p. 1137; Cass. sez. V, 27 febbraio 2002, Bresciani, in *Foro it.*, 2002, II, c. 635.

[254] L. G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare G.P.S.*, in *Giur. It.*, 2003, pp. 2372 e ss; L. FILIPPI, *Il GPS è una prova incostituzionale. Domanda provocatoria ma non troppo dopo la sentenza Jones della Corte Suprema USA*, in *Arch. pen.*, 2012, p. 309. Da sottolineare inoltre che il sistema GPS è stato oggetto di una nota pronuncia, richiamata poco fa, da parte della Corte Suprema degli Stati Uniti (cfr. Corte Suprema USA, 23 gennaio 2012, *U.S. vs Jones*), la quale ha stabilito che nessun mezzo limitativo dei "beni" di un individuo può essere effettuato laddove manca un "mandato" emesso da un giudice competente, laddove ovviamente esistano le condizioni che possano giustificare tale atto. Da segnalare invece la posizione opposta espressa dalla Corte europea dei diritti dell'uomo (cfr. CEDU, sez. V, 2 settembre 2010, *Utza c. Germania*), la quale ha considerato l'utilizzo della tecnologia GPS come utile ai fini delle indagini in procedimenti contro la criminalità e quindi utilizzabile in tali sedi, giustificando tale decisione sulla base che in Germania esiste un'effettiva normativa che regolamenta l'utilizzo del sistema GPS.

[255] Così sostenuto da L. CARLI, *Le indagini preliminari nel sistema processuale penale*, Giuffrè, Milano, 2005, p. 333.

alle altre operazioni tecniche così come disciplinate dall'art. 359, c.p.p., per le quali sono necessarie specifiche competenze. In ultimo, nonostante il codice non presenti una definizione di intercettazione, non risulta tuttavia ascrivibile a tale categoria il sistema di localizzazione satellitare, in quanto non va a captare clandestinamente il contenuto di una comunicazione riservata di due o più persone, nonostante è stato osservato[256] che, nel momento in cui la captazione del flusso venga ottenuta utilizzando i dati di un ricevitore GPS in dotazione e di proprietà del soggetto sottoposto ad indagine, tramite un telefono cellulare o uno *smartphone*, tale attività rappresenterebbe una vera e propria intercettazione digitale a tutti gli effetti, con l'applicazione della relativa disciplina. Tale ultima teoria risulta, in linea generale, applicabile anche ai captatori informatici nel momento in cui essi vengano inoculati all'interno di un *device* portatile, quali *smartphone* o *tablet*, tuttavia la dottrina e la giurisprudenza tendono a classificare tale attività di indagine come un atto investigativo atipico, quale è il pedinamento, ed in particolare, poiché la localizzazione avviene per via satellitare, si tende a classificare tale attività come "pedinamento elettronico", ovvero una *species* tecnologica del *genus* del pedinamento[257].

Rimane da sciogliere il nodo relativo all'utilizzabilità probatoria degli atti di indagine acquisiti tramite GPS, in particolar modo analizzando la natura ripetibile o irripetibile di tale atto di indagine, come è stato fatto anche per le altre funzioni relative al captatore informatico analizzate nei paragrafi precedenti. In linea generale, le sole attività investigative che sono classificabili come irripetibili sono quelle che non possono essere a conoscenza del giudice per mezzo dell'assunzione della testimonianza

[256] D. GENTILE, *Tracking satellitare mediante gps: attività tipica di indagine o intercettazione di dati?*, in *Dir. pen. proc.*, 2010, p. 12.
[257] In questo senso T. BENE, *Il pedinamento elettronico: truismi e problemi spinosi*, in *Le indagini atipiche*, op. cit., pp. 350 e ss; in senso contrario, vedasi A. CAMON, *L'acquisizione dei dati sul traffico telefonico*, in *Dir. pen. proc.*, 2005, p. 634.

ovvero le attività che perderebbero la loro genuinità per via della narrazione dibattimentale. In questo senso, sembra potersi ritenere che, anche grazie al dettato dell'art. 431 c.p.p. e la menzione ai «verbali» degli atti non ripetibili, le forme meno dettagliate di documentazione dell'attività di spostamento del soggetto indagato tramite localizzazione satellitare, come le annotazioni della polizia giudiziaria e le relazioni di servizio, siano atti ripetibili[258]. La peculiarità infatti relativa ai dati di localizzazione incorporati nei supporti informatici allegati è quella di indicare, di regola, il giorno, il mese e l'anno del rilevamento satellitare, oltre che il tracciato degli spostamenti effettuati dal soggetto, andando così ad integrare, assieme alla mera annotazione effettuata dalla polizia giudiziaria, le caratteristiche tipiche degli atti ripetibili. La stessa Corte di Cassazione ha negato la natura irripetibile dei supporti informatici che contengono i dati sugli spostamenti di un veicolo controllato[259], affermando al contempo che è esclusa tuttavia la possibilità di acquisire le connesse relazioni di servizio, in quanto i risultati provenienti dall'attività di localizzazione possono essere conoscibili dal giudice esclusivamente attraverso la testimonianza della polizia giudiziaria, la quale ha eseguito materialmente l'operazione, così come accade per l'attività investigativa relativa al pedinamento ordinario. Per quest'ultimo motivo la Suprema Corte ha esteso la disciplina offerta per i pedinamenti ordinari, ammettendo quindi la testimonianza della polizia giudiziaria che ha condotto effettivamente l'operazione di localizzazione in modo da acquisire in modo legittimo la "prova satellitare" e garantendo al tempo stesso delle modalità processuali che garantiscono un contraddittorio equo fra le parti[260].

L'ultima particolarità di questo tipo di attività investigativa condotta

[258] Su questo tema, S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, pp. 580 e ss.
[259] Cass. sez. I, 9 marzo 2010, n. 9416, in *Cass. pen.*, 2012, p. 1062.
[260] Cass. sez. VI, 11 dicembre 2007, n. 15396, in *Cass. pen.*, 2009, 6, p. 2534.

tramite captatore informatico risulta essere quella relativa alle garanzie dettate dai diritti fondamentali. Il pedinamento elettronico può essere ascrivibile al novero delle attività della polizia giudiziaria, per cui esso risulta possibile anche in mancanza di un decreto autorizzativo emanato dal giudice ma, in particolare, può non rispettare la riserva di legge e non avvenire secondo i casi e i modi previsti dalla legge, poiché è un mezzo di prova atipico e quindi non suscettibile di regolazione a priori. Tale tecnica risulta quindi al riparo dalle garanzie offerte dall'applicazione dell'art. 14 Cost. Si ritiene poi che, in relazione ai limiti esposti dai giudici di legittimità in relazione all'art. 15 Cost., i dati captati tramite la localizzazione satellitare non incidano affatto sul diritto alla libertà ed alla segretezza delle comunicazioni poiché esso è, strutturalmente, non in grado di apprendere contenuti comunicativi[261]. Tale impostazione trova tuttavia un riscontro non pacifico per quanto riguarda il captatore informatico poiché esso è in realtà in grado di captare contenuti comunicativi e allo stesso tempo tracciare gli spostamenti del soggetto tramite la geolocalizzazione. Per questo motivo ritorna, di nuovo, in auge la necessità innanzitutto di un dettato normativo che garantisca la determinatezza all'interno del decreto di autorizzazione emanato dal giudice delle attività effettivamente da porre in essere tramite il captatore informatico, nonché, in secondo luogo, la motivazione specifica e la proporzionalità sulle modalità di impiego e svolgimento da parte dell'autorità investigativa di tali attività.

[261] A. CHELO MANCHIA, *Localizzazione tramite GPS: quali garanzie?*, in *Riv. giur. Sarda*, 2006, p. 432.

# Capitolo 5

## Il nuovo regime di utilizzabilità dei captatori: la disciplina dettata dalla legge Orlando

SOMMARIO: 1 – La sentenza "Scurato" e la presa di posizione delle Sezioni Unite. – 1.1 – L'irrilevanza del luogo ai fini della legittimità. – 1.2 – Il rischio di strumentalizzazione del reato associativo. – 2 – La normativa nazionale in tema di utilizzabilità delle intercettazioni. – 2.1 – La legge "Orlando".

## 1 – La sentenza "Scurato" e la presa di posizione delle Sezioni Unite

Rimanendo nell'ambito delle intercettazioni per mezzo di immissione di un captatore informatico, la delega al Governo contenuta nella legge "Orlando", la quale verrà analizzata nel corso di questo capitolo, su questo tema sembra rispecchiare quanto affermato dalla Suprema Corte nella decisione del 28 aprile 2016, ossia nella sentenza "Scurato" più volte richiamata nel corso di questa trattazione. Secondo quanto stabilito dai giudici di legittimità, l'intercettazione di comunicazioni tra presenti mediante l'utilizzo del captatore informatico in qualsivoglia dispositivo elettronico, è consentita nei soli casi relativi a procedimenti per criminalità organizzata, per i quali trova applicazione la disciplina derogatoria di cui all'art. 13 del d.l. n. 151 del 1991, la quale consente la captazione anche nei luoghi di privata dimora e anche nel caso in cui ivi non vi si stia

svolgendo un'attività criminosa[262]. Al di fuori di tale disciplina derogatoria, la Suprema Corte ha escluso categoricamente la possibilità di utilizzare ai fini intercettivi lo strumento del captatore informatico in quanto il dettato codicistico di cui all'art. 266, comma 2, c.p.p., secondo il quale sarebbero consentite le intercettazioni ambientali nei luoghi di privata dimora solo in presenza del fondato motivo di ritenere che ivi sia in corso un'attività criminosa, non ammette deroghe a parere della Corte[263]. La stessa Corte ha inoltre specificato che, vista la particolare intrusività del mezzo utilizzato per eseguire le operazioni intercettive, la qualificazione del fatto reato che deve essere annoverato nell'ambito della criminalità organizzata deve essere supportata da sufficienti e sicuri elementi indiziari, i quali devono risultare all'interno della motivazione del provvedimento che autorizza tali operazioni di intercettazione.

Secondo quanto detto sopra quindi, le Sezioni Unite sembrano tracciare delle linee guida utili per poter distinguere le intercettazioni ambientali effettuate mediante l'utilizzo del virus *trojan* da tutte le altre, considerando due macro-ipotesi:

1) nel primo caso, l'intercettazione di comunicazioni tra presenti, relativamente a procedimenti diversi da quelli compresi nella nozione di criminalità organizzata, viene attuata nei luoghi rientranti nel dettato codicistico di cui all'art. 614, c.p., nei quali si sta svolgendo un'attività criminosa;

2) nel secondo caso l'intercettazione di comunicazione tra presenti, sempre riguardante procedimenti diversi rispetto a quelli relativi alla criminalità organizzata, avviene in luoghi diversi da quelli citati dall'art.

[262] G. L. CORTE, *Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata*, in *Giur. pen. web*, 2017, 6, pp. 10 e ss.
[263] S. ROMANO e C. SORIO, *L'utilizzo dei c.d. trojan horses nelle indagini penali e la tutela "progressiva" della libertà e segretezza delle comunicazioni*, in *Law and Media Working Paper Series*, 2016, n. 14.

614, c.p.

Ragionando quindi su quanto delineato dalle Sezioni Unite, sembrano quindi ipotizzabili due scenari in grado di poter rispettare sia un criterio di logica e coerenza sia i principi di garanzia esposti dalla Suprema Corte: nel primo, l'intercettazione di comunicazioni mediante l'utilizzo del captatore informatico risulterebbe legittima, in procedimenti diversi a quelli relativi a reati di criminalità organizzata, nei luoghi domiciliari disciplinati dall'art. 614, c.p., e nei quali si stia svolgendo un'attività criminosa, nel caso detti luoghi fossero preventivamente indicati e motivati nel provvedimento di richiesta dell'intercettazione stessa; nel secondo scenario invece, un'intercettazione dello stesso tipo, ossia mediante l'utilizzo di un virus *trojan*, risulterebbe altrettanto legittima ove essa fosse disposta, sempre in procedimenti non attinenti a reati di criminalità organizzata, per dei luoghi non disciplinati dall'art. 614, c.p., e indicati in termini anche generici all'interno della richiesta di autorizzazione[264].

## 1.1 – L'irrilevanza dell'indicazione del luogo ai fini della legittimità

Un ulteriore aspetto evidenziato dalla Suprema Corte è quello relativo all'indicazione del luogo all'interno del decreto autorizzativo. I giudici di legittimità, nel corso del loro ragionamento riguardante la sentenza "Scurato", hanno sottolineato l'assoluta assenza di basi legali per poter sostenere che l'assenza della preventiva indicazione dei luoghi di

[264] S. ATERNO, *Il Trojan dalla A alla Z. Esigenze investigative e limitazioni della privacy: un bilanciamento necessario*, in Internet al sito http://www.dirittopenaleinformatica.it/wp-content/uploads/2017/02/ATERNO_Il-TROJAN-dalla-A-alla-Z.pdf.

svolgimento delle attività di intercettazione sia un requisito necessariamente previsto a pena di inutilizzabilità dalla legge, dalla giurisprudenza o dalla stessa Costituzione. Tale affermazione risulta quindi non "confinare" la disciplina delle intercettazioni ai soli casi in cui lo strumento tramite il quale vengono espletate dette operazioni sia "fisso", come nel casco delle microspie, ma ha il pregio di "aprire" un nuovo scenario delle indagini penali anche a strumenti, come i captatori informatici, in grado di "seguire" il soggetto sottoposto ad intercettazioni. Gli stessi giudici di legittimità tuttavia sottolineano che tale affermazione non deve portare a giustificare qualsivoglia strumento di indagine anche nei casi in cui esso possa rivelarsi lesivo del diritto alla riservatezza del domicilio. Le conclusioni prospettate dalla Suprema Corte tuttavia trovano immediata applicazione nella disciplina derogatoria di cui all'art. 13, d.l. n. 151 del 1991, la quale stabilisce chiaramente l'indifferenza in ambito spaziale per quanto riguarda le intercettazioni relative a procedimenti in ambito di criminalità organizzata[265]. Sollevare infatti il giudice e il Pubblico Ministero dall'onere di indicare preventivamente i luoghi dove dovranno svolgersi le intercettazioni contribuisce in modo essenziale a rendere più trasparente la richiesta di autorizzazione ad effettuare tali operazioni e, di conseguenza, la necessità esplicitata all'interno dell'autorizzazione stessa. Tale possibilità, ossia di poter porre in essere forme di sorveglianza più intrusive, trova appiglio anche all'interno del quadro convenzionale. Come ricordato dalle Sezioni Unite infatti, la Corte di Strasburgo ha chiaramente esplicitato i requisiti essenziali da adottare in sede di normativa nazionale in tema di intercettazioni, non citando mai fra di essi la necessità di indicazione preventiva dei luoghi dove tali operazioni verranno poste in essere[266]. Secondo la giurisprudenza della Corte europea quindi, nel

[265] A. MONTAGNA, *Intercettazioni ambientali tramite virus negli smartphone: la decisione delle Sezioni Unite*, in *Quotidiano Giuridico*, 4 luglio 2016, pp. 3-4.

[266] Il parametro topografico viene preso in considerazione dalla Corte all'interno della sentenza del 4 dicembre 2015, *Zakharov c. Russia*, n. 47143/06, in cui viene fatto riferimento generico «all'insieme dei luoghi» interessati dalle

momento in cui il soggetto destinatario di misure di sorveglianza (*surveillance*) è indicato espressamente all'interno del provvedimento che autorizza tali misure, non risulta necessario specificare anche l'ambiente in cui esse devono essere eseguite[267]. In sintesi quindi, la disciplina posta in essere dall'art. 266, c.p.p., in tema di intercettazioni ambientali, così come interpretato dalle Sezioni Unite all'interno della pronuncia in esame, fa si che non possano aversi intercettazioni ambientali all'interno dei luoghi di privata dimora di cui all'art. 614, c.p.p., salvo che ci si trovi nei casi stabiliti dalla disciplina derogatoria di cui all'art. 13, d.l. n. 151 del 1991, in relazione alla quale risultano quindi ammissibili intercettazioni tramite l'utilizzo dei captatori informatici, inoculati all'interno di dispositivi elettronici portatili, anche qualora all'interno del provvedimento autorizzativo non siano stati indicati preventivamente i luoghi in cui dette operazioni verranno effettivamente e di volta in volta poste in essere[268]. Bisogna ricordare infine che il ritenere inutile l'indicazione del luogo per reati di particolare gravità come possono essere quelli relativi alla criminalità organizzata – peraltro senza effettive basi legali per poter affermare il contrario – non equivale logicamente a ridurre i diritti e le garanzie dei soggetti sottoposti a determinate misure, poiché l'uso di tali tecnologie ai fini investigativi necessita improrogabilmente di una disciplina specifica e della previsione di adeguate garanzie per tutelare diritti e libertà fondamentali degli individui.

---

intercettazioni e non alla loro indicazione preventiva. Anche nella sentenza sopra citata tuttavia esso viene preso come riferimento solo in via secondaria ed in alternativa alla possibile identificazione del soggetto che deve essere sottoposto ad operazioni di intercettazione.

[267] Tale orientamento elaborato dalla Corte ha trovato riscontro anche in una recente pronuncia della stessa, cfr. C. eur., 23 febbraio 2016, *Capriotti c. Italia*, n. 28819/12, in *Riv. it. dir. e proc. pen.*, fasc. 2, 2016, p. 1100.

[268] E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla difesa*, 1, Pisa, 2016, p. 160.

## 1.2 – Il rischio di strumentalizzazione del reato associativo

Il motivo fondamentale per cui la Corte di Cassazione ha deciso di limitare la disciplina dei captatori informatici ai reati di criminalità organizzata è relativo alla natura intrinseca dei captatori stessi: essendo uno strumento in grado di seguire il soggetto ovunque vada poiché inoculato all'interno di un dispositivo elettronico portatile, esso finirà prima o poi con l'intercettare colloqui avvenuti all'interno di luoghi domiciliari, da qui la scelta delle Sezioni Unite di limitarne l'utilizzo ad un ambito in cui già è prevista una disciplina derogatoria rispetto alla tutela del domicilio. Tuttavia, uno dei problemi fondamentali evidenziati dalla dottrina in merito alla pronuncia "Scurato" riguarda esattamente il bilanciamento operato dalle Sezioni Unite tra l'invasività dello strumento del captatore informatico e il suo possibile utilizzo all'interno dei soli procedimenti di criminalità organizzata. Come già ricordato nel corso di questa trattazione, la dottrina non definisce con certezza la nozione di "criminalità organizzata", alle volte definendola sotto il profilo socio-criminologico, altre volte definendo tale concetto tramite i delitti previsti da elenchi normativi tassativi[269]. Le Sezioni Unite invece, sulla scorta di una precedente giurisprudenza elaborata dalla Corte medesima[270], ritengono integrata la nozione di criminalità organizzata nel momento in cui sia soddisfatto il requisito di «una stabile organizzazione programmaticamente ispirata alla commissione di più reati»[271]. In merito

[269] Per un ulteriore approfondimento sul tema vedasi A. BERNASCONI, voce *Criminalità organizzata (diritto processuale penale)*, in *Enc. dir.*, Agg. IV, Milano, 2000, pp. 501 e ss; G. LEO, *La nozione processuale di criminalità organizzata*, in *Corr. mer.*, 2005, p. 830; B. ROMANO e G. TINEBRA, *Il diritto penale della criminalità organizzata*, Giuffrè, Milano, 2013.
[270] Cass. sez. un., 25 luglio 2010, Donadio, in *C.E.D. Cass.*, n. 247994.
[271] Sul punto, vedasi anche G. GARUTI, *Osservatorio Corte di Cassazione – Sezioni Unite*, in *Dir. pen. e proc.*, n. 8, 2016, p. 1042.

a tale categoria di reati, la dottrina ha sottolineato il problema relativo al possibile abuso delle intercettazioni, sia "ordinarie" sia a mezzo di captatore informatico, fondate magari su ipotesi di reato associative ma senza magari una individuazione chiara dei delitti scopo di tali associazioni[272]. Tale problema risulta da tempo presente, soprattutto alla luce di quanto esposto precedentemente in tema di una definizione specifica della nozione di criminalità organizzata, ma potrebbe accentuarsi particolarmente con l'utilizzo dei captatori informatici a scopo intercettivo, nel momento in cui possono essere utilizzati solo nel momento in cui ci sia una configurazione del reato associativo. La giurisprudenza, in linea generale, è abbastanza incline a sterilizzare le conseguenze di una qualificazione giuridica differente da quella per cui sono state disposte le intercettazioni. Per quanto riguarda le intercettazioni telefoniche, ad esempio, si ritiene che se esse siano state disposte per uno dei reati di cui all'art. 266, c.p.p., esse siano esplicabili anche per altri reati per i quali si procede all'interno del medesimo procedimento, anche qualora per essi le intercettazioni non fossero consentite[273].

Il problema quindi che si pone è quello di una strumentalizzazione forte del reato associativo in modo da ottenere l'utilizzo, a fini intercettivi, del captatore informatico. In questo modo, richiedendo tale strumento durante la fase delle indagini, si potrebbero utilizzare le risultanze ottenute tramite le intercettazioni eseguite con il virus *trojan* al fine di realizzare un impianto probatorio per reati per i quali i captatori non potrebbero essere utilizzati legittimamente[274]. L'unica soluzione profilabile

[272] A. NAPPI, *Sull'abuso delle intercettazioni*, in *Cass. pen.*, 2009, pp. 470-471.
[273] Cass. sez. F., 23 agosto 2016, n. 35536, in *C.E.D. Cass.*, n. 267598. In senso contrario, ossia non ammettendo le intercettazioni per i reati per i quali non sussistono i presupposti di ammissibilità delle stesse, vedasi Cass. sez. II, 18 dicembre 2015, n. 1924, in *C.E.D. Cass*, n. 265989; Cass. sez. III, 25 febbraio 2010, n. 12562, in *C.E.D. Cass.*, n. 246594; Cass. sez. VI, 15 gennaio 2004, n. 4942, in *C.E.D. Cass.*, n. 229999.
[274] Il punto è stato sottolineato, in modo approfondito da G. VERDE, *Le inchieste di Napoli e le intercettazioni "esplorative"*, in *Il Mattino*, in Internet al sito

per poter scongiurare una tale eventualità, oltre che far completo affidamento sulla professionalità del Pubblico Ministero, è quella per cui l'organo investigativo non deve mai dimenticare il richiamo fatto dalla Corte di Cassazione al rigore della motivazione all'interno della richiesta di autorizzazione e del decreto autorizzativo, verificando quindi con estrema puntualità, di volta in volta, i presupposti per l'utilizzo di tale strumento investigativo.

## 2 – La normativa nazionale in tema di utilizzabilità delle intercettazioni

Nel momento in cui lo strumento del captatore informatico viene equiparato ad una forma di intercettazione e, di conseguenza, viene assoggettato alla disciplina specifica di tale materia, devono essere analizzate anche le cause di inutilizzabilità di tali risultati probatori. In generale, ai fini della valutazione sulle possibilità di utilizzo di un determinato atto, quello che conta è che tale atto non sia stato ottenuto violando un divieto di legge. Questo rilievo consente quindi di giungere ad una unificazione[275], almeno per quanto riguarda gli effetti, delle varie cause di inutilizzabilità dalla disciplina dettata dall'art. 191, c.p.p., intitolata «prove illegittimamente acquisite», la quale stabilisce, al comma 1, che «le prove acquisite in violazione di divieti stabiliti dalla legge non possono essere utilizzate». L'art. 191, c.p.p., diventa quindi una sorta di denominatore comune ovvero la norma di disciplina di riferimento[276]. Per

---

https://www.pressreader.com/italy/il-mattino-caserta/20170113/282643212244457.

[275] In questo senso, F. R. DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Giuffrè, Milano, 2008, p. 37.

[276] Da sottolineare inoltre che, l'art. 191, comma 2, c.p.p., costituisce una «norma generale di riferimento per il regime del vizio dell'inutilizzabilità», così

quanto attiene poi alla disciplina specifica delle intercettazioni, un'altra norma del codice di procedura penale risulta essere un ulteriore caposaldo per quanto riguarda i divieti d'uso delle stesse all'interno di un procedimento. L'art. 271, comma 1, c.p.p., con un rimando all'art. 191, c.p.p., stabilisce infatti che «i risultati delle intercettazioni non possono essere utilizzati qualora le stesse siano state eseguite fuori dai casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dagli artt. 267 e 268 commi 1 e 3». Tramite il disposto dell'articolo sopra menzionato è possibile quindi "dividere" le inutilizzabilità relative alle intercettazioni in quattro macro-categorie: in primo luogo quelle relative alla motivazione degli atti di autorizzazione e relativi vizi (art. 267, comma 1, c.p.p.), in secondo luogo quelle relative alle operazioni "pratiche" di intercettazione ed ai relativi vizi (art. 268, comma 3, c.p.p.), quelle annesse ai vizi relativi alla "registrazione" dei dati e alle risultanze delle intercettazioni (bobine e brogliacci) e, infine, quelle legate all'utilizzo delle intercettazioni in altri procedimenti.

In primo luogo potrebbe quindi aversi inutilizzabilità dei risultati probatori acquisiti tramite intercettazione nel momento in cui sussistano dei vizi di motivazione degli atti di autorizzazione relativi alle operazioni intercettive. La procedura ordinaria, come analizzato nel corso dei capitoli precedenti, prevede una richiesta da parte del Pubblico Ministero, convalidata successivamente tramite decreto motivato dal GIP, salvo poi i casi di urgenza in cui il Pubblico Ministero può provvedere da sé fermo restando la convalida da parte del GIP del decreto emanato dall'organo inquirente. Il punto centrale, comune a questi atti, è l'apparato motivazionale, il quale, come sostenuto da autorevole dottrina, «è costituito dall'*iter* cognitivo e valutativo seguito dal giudice in modo che se ne possano conoscere i risultati, i quali devono essere conformi alla legge; ciò in

---

come affermato da V. GREVI, in *Prove,* in G. Conso e V. Grevi, *Profili del nuovo codice di procedura penale,* Padova, 1990.

funzione della garanzia assicurata a chi ha diritto di impugnare la decisione, di esercitare il diritto di critica e, all'organo della valutazione o dell'impugnazione, di effettuare l'attività di verifica che gli compete[277]». La motivazione deve quindi contenere dei riferimenti espliciti ai «gravi indizi» del reato[278], al bisogno istruttorio e, nel momento in cui le operazioni di intercettazioni debbano essere effettuate nei luoghi domiciliari, è richiesto il fondato motivo di ritenere che ivi sia in atto una condotta criminosa[279]. Per quanto riguarda la prassi della motivazione *per relationem*, anche se essa appare fortemente lesiva del tenore letterale dell'art. 266, c.p.p., è ritenuta prassi lecita[280] nonostante un contrasto giurisprudenziale in seno alla Suprema Corte che va avanti da molti anni e che ha visto numerose pronunce contrapporsi fra di loro. In caso di doglianze relative quindi alla motivazione, in particolar modo quelle relative alla carenza della motivazione, esse devono sempre poter dimostrare un difetto di consequenzialità all'interno del ragionamento del GIP e devono, di conseguenza, essere tenute distanti, almeno sul piano concettuale, da quelle relative alla sussistenza del requisito a cui la motivazione stessa fa riferimento, in quanto la Corte potrebbe altresì rilevare come il vizio della motivazione sia in realtà solo apparente, appartenendo esso al merito della valutazione effettuata piuttosto che alla sua legittimità.

In secondo luogo si potrebbe riscontrare l'inutilizzabilità delle risultanze probatorie anche relativamente alle operazioni "pratiche" di intercettazione, in particolar modo nei casi previsti dall'art. 268, comma 3,

---

[277] L. KALB, *Intervento*, in *Le intercettazioni di conversazioni e comunicazioni – Meccanismi operativi e regole procedurali*, Giuffrè, Milano, 2009, p. 305.

[278] Tuttavia, occorre ricordare che, in tema di captatori informatici, poiché essi sono utilizzabili all'interno di procedimenti relativi alla criminalità organizzata, il requisito dei gravi indizi di reato viene "ridimensionato" a quello dei sufficienti indizi di reato.

[279] Ufficio del Massimario, Servizio Penale, *Orientamenti sulle linee interpretative della giurisprudenza e della dottrina in materia di intercettazioni*, Rel. n. 55/2005.

[280] In questo senso, M. BORGOBELLO, *L'eccezione di inutilizzabilità delle intercettazioni*, Giappichelli Editore, Torino, 2013, p. 54.

c.p.p. Al fine di evitare che l'esecuzione delle operazioni si svolga al di fuori del controllo dell'autorità giudiziaria, esse avvengono di regola, così come stabilito dall'articolo sopra richiamato, mediante l'utilizzo degli impianti installati presso le procure della Repubblica. Tuttavia lo stesso articolo fa riferimento alla possibilità, nei casi di urgenza, dell'utilizzo di impianti esterni alle procure, disposta tramite decreto del Pubblico Ministero sul quale, in questo caso, graverà l'obbligo di motivazione[281]. Attraverso la procedura d'urgenza, anche se in apparenza criticabile per via della sovrapposizione concettuale delle ipotesi di cui all'art. 267, comma 2 e 268, comma 3, c.p.p., esiste comunque un controllo del GIP nel momento in cui viene emesso il decreto di convalida. La Cassazione[282] dunque, per poter "giustificare" tale procedura da parte del Pubblico Ministero, pone su di esso una serie di specifici obblighi di motivazione: in primo luogo deve sussistere una specifica inadeguatezza degli impianti in dotazione all'ufficio della procura, per cui la motivazione si può definire corretta e congruente nel momento in cui evidenzi l'insufficienza degli impianti interni rispetto alla specifica indagine probatoria da condurre in quel determinato momento; in secondo luogo, in merito alle ragioni di eccezionale urgenza, la motivazione deve sottolineare ed evidenziare l'attualità della situazione criminosa, in modo tale da mostrare la gravità del pregiudizio che verrebbe arrecato alle indagini se non si utilizzassero impianti esterni.

Successivamente, si può riscontrare un'inutilizzabilità degli elementi acquisiti tramite intercettazioni anche relativamente ai vizi annessi alla

[281] Su questo punto è da sottolineare l'opinione di A. MANGANELLI e F. GABRIELLI, in *Investigare – Manuale pratico delle tecnologie di indagine*, Cedam, Padova, 2007, pp. 125-126, secondo cui questa prassi è in via di progressiva risoluzione in quanto sempre più uffici giudiziari si stanno dotando delle tecnologie idonee tali da conciliare il dettato normativo con le esigenze degli organi inquirenti. In particolare, si fa riferimento al c.d. "ascolto da remoto", tema fondamentale nell'ambito dell'utilizzo dei captatori informatici.
[282] Cass. sez. I, 28 aprile 2009, n. 31570, in *Guida al dir.*, 44, 68.

"registrazione" dei dati e, di conseguenza, alle prove derivanti da tali operazioni, ossia bobine e brogliacci. Col progresso tecnologico, le operazioni di captazione di conversazioni avvengono in modo diverso rispetto al passato, per cui, dopo essere state captate presso l'operatore telefonico e registrate presso la procura della Repubblica, esse vengono poi ascoltate e di tale ascolto viene redatto un verbale sintetico[283]. La recente dottrina ha ulteriormente sottolineato come l'ascolto c.d. "remotizzato" costituisca una modalità legittima di captazione delle conversazioni[284]. L'unico momento rilevante, così come evidenziato sia da parte della dottrina che da parte della giurisprudenza di legittimità, diviene quindi quello in cui, attraverso il *server* installato presso le procure della Repubblica, i dati vengono trascritti nella memoria informatica centralizzata, arrivando così a definire tale momento come "operazione"[285] ai sensi dell'art. 268, comma 3, c.p.p. Tuttavia, poiché la giurisprudenza è da tempo pacifica nello stabilire che la prova vera e propria è costituita dal supporto materiale su cui sono memorizzati i dati (le bobine, ad esempio), ciò permette di riconsiderare quanto espresso poc'anzi arrivando a stabilire che l'attività di "scaricamento" dei dati dal *server* ai supporti informatici è sì rilevante ai fini dell'art. 268, c.p.p., specialmente quando detta attività avviene utilizzando impianti esterni a quelli installati presso le procure. Per quanto riguarda invece i brogliacci, essendo essi non considerati prove in quanto risultano essere una mera trascrizione delle conversazioni ritenute rilevanti dalla polizia giudiziaria, il problema non si pone[286]. Per queste ragioni, la difesa potrà controllare i verbali delle

---

[283] E. SAVIO, *Remotizzazione dell'ascolto: dalla recente giurisprudenza al progetto Alfano*, in *Diritto penale e processo*, Ipsoa, Padova, 2010, n. 4, p. 494.
[284] E. TURCO, *Nota a sent. Cass. sez. un., 26 giugno 2008, n. 36359*, in *For. it.*, Zanichelli, Bologna, 2009, n. 2, II, p. 80.
[285] In questo senso, C. ANGELONI, *Le intercettazioni telefoniche "in remotizzato": gli aspetti esecutivi al vaglio delle Sezioni unite*, in *Giur. it.*, Ipsoa, Milano, 2009, n. 2, p. 462.
[286] Bisogna tuttavia sottolineare che, laddove vengano meno le registrazioni vere e proprie, i brogliacci potrebbero essere considerati ai fini della prova in giudizio

operazioni redatti dalla polizia giudiziaria e, in questo modo, verificare le modalità attraverso le quali gli agenti inquirenti hanno effettuato le operazioni di intercettazione. Nel momento in cui si rilevasse che non è stata fatta menzione del *server* della procura utilizzato per lo "scaricamento" dei dati, ma solamente dei supporti (cd-rom, ad esempio) su cui sono stati salvati i dati raccolti, si potrò sollevare un'eccezione di inutilizzabilità, *idem* per quanto riguarda i casi in cui sia stato utilizzato per dette operazioni un *server* installato presso la Questura oppure altre apparecchiature esterne, ipotesi che potrebbe coinvolgere direttamente l'utilizzo dei captatori informatici in quanto l'operazione intercettiva viene, di solito, delegata ad agenzie terze rispetto agli organi inquirenti.

L'ultima forma di inutilizzabilità è quella legata al divieto di utilizzo delle intercettazioni in un procedimento diverso da quello in cui esse sono state ammesse. Tale impostazione è ripresa nella prima parte del comma 1 dell'art. 270, c.p.p., la quale stabilisce il divieto di utilizzo delle intercettazioni in procedimenti diversi da quello in cui esse sono state autorizzate[287]. Di regola quindi, poiché manca il controllo preventivo da parte dell'organo giudicante, il GIP, le informazioni ottenute tramite delle intercettazioni disposte in un determinato procedimento non possono essere utilizzate nell'ambito di un procedimento diverso. Il divieto espresso nella prima parte dell'art. 270, c.p.p., non conosce quindi eccezioni, se non quella di un eventuale uso delle informazioni captate tramite intercettazioni quali *notitia criminis*. Le uniche eccezioni a tale

---

e, di conseguenza, divenire utilizzabili così come stabilito da Cass. sez. IV, 29 gennaio 2001, n. 8437, inedita.

[287] Tale articolo è stato oggetto di una disamina da parte della Corte Costituzionale la quale, con la pronuncia n. 366/1991, in *Giust. pen.*, 1992, I, pp. 35 e ss., stabilisce la necessaria motivazione dell'atto giudiziale di autorizzazione delle intercettazioni, nei modi e nei sensi previsti dalla legge, vietando quindi «l'utilizzabilità dei risultati di intercettazioni validamente disposte nell'ambito di un determinato giudizio come elementi di prova in processi diversi». Contrario a questa impostazione R. CANTONE, definendo l'art. 270 come «costituzionalmente indifferente», in *L'elaborazione giurisprudenziale sull'art. 270 c.p.p.; brevi riflessioni*, in *Cass. pen.*, 2000, p. 2046.

divieto possono riscontrarsi nella seconda parte del comma 1 dell'art. 270, c.p.p., nel momento in cui si prevede una deroga al divieto espressamente previsto, qualora le intercettazioni siano state richieste ed autorizzate per un procedimento a carico di ignoti oppure qualora le stesse siano state disposte per più reati collegati o connessi per i quali si sia proceduto, successivamente, separatamente[288]. Inoltre, sempre all'interno del comma 2 del sopra citato articolo, si può rinvenire anche la previsione secondo la quale tali risultanze probatorie sono utilizzabili in procedimenti diversi qualora esse risultano indispensabili per l'accertamento di delitti per i quali il codice prevede l'arresto in flagranza.

Un'ultima causa di inutilizzabilità, così clamorosa da essere poco riscontrata nella prassi applicativa, è quella dell'inutilizzabilità comminata per le intercettazioni eseguite per un'ipotesi criminosa estranea a quelle elencate nell'art. 266, c.p.p. Nella prassi, detta inutilizzabilità non viene quasi mai comminata poiché risulta essere molto più frequente il caso in cui viene scoperto un reato diverso da quello ipotizzato nel decreto autorizzativo. In questo caso, la dottrina si divide in due filoni: da una parte coloro che, interpretando in modo estensivo il concetto di procedimento diverso stabilito dall'art. 270, c.p.p., estendono l'inutilizzabilità ad ogni ipotesi mutata rispetto a quella originariamente ipotizzata all'interno del decreto di autorizzazione, ritenendo valide dette intercettazioni solo nel caso in cui la fattispecie "finale" implichi l'arresto in flagranza[289]; dall'altro lato vi è chi rifiuta questa impostazione, scontrandosi con il problema di stabilire cosa dovrebbe accadere alle intercettazioni autorizzate per un determinato reato ma che, all'apertura del procedimento, si ritrovino ad essere utilizzate per una fattispecie

[288] F. RUGGERI, *Divieti probatori e inutilizzabilità nella,* op. cit., pp. 111 e ss.
[289] In questo senso vedasi, su tutte, C. DI MARTINO e T. PROCACCIANTI, *Le intercettazioni telefoniche*, op. cit., pp. 217 e ss.

criminosa mutata[290].

In ultimo, va sottolineato che l'inutilizzabilità, sia essa proveniente da qualunque dei vizi sopra descritti, è rafforzata tramite l'istituto della distruzione. Esso punta in primo luogo a neutralizzare i possibili sviluppi di una prova vietata per legge[291], mentre, al contempo, l'eliminazione fisica del materiale si rileva utile alla tutela del diritto alla riservatezza. La distruzione inoltre, considerati i valori tutelati in gioco, potrà essere disposta anche d'ufficio, a differenza di quanto accade per quella regolata dall'art. 269, c.p.p. La Corte Costituzionale ha inoltre stabilito che la procedura di distruzione può seguire due vie distinte, a seconda del tipo di inosservanza che ha determinato l'inutilizzabilità delle risultanze probatorie: nel momento in cui si tratti di vizi di ordine procedurale e di comunicazioni che di per sé avrebbero potuto essere conoscibili, ma che avrebbero potuto essere captate in modo legittimo qualora fosse stato seguito l'*iter* corretto, la distruzione dovrà avvenire al cospetto delle parti; ove invece si sia ravvisata una violazione di una sfera di riserbo (ad esempio, il segreto professionale), la distruzione dovrà essere disposta per forza al di fuori del contraddittorio.

## 2.1 – La legge "Orlando"

Dopo aver analizzato i casi di inutilizzabilità dettati in tema di intercettazioni in generale, risulta necessario prendere in considerazione quanto disposto dalla nuova legge "Orlando", recentemente approvata dal Parlamento. Le direttrici su cui si muove la sopra citata legge possono essere ricondotte a tre ambiti: in primo luogo quello della giustizia

[290] Secondo F. CORDERO, *Tre studi sulle prove penali*, op. cit. p. 851, esse sarebbero utilizzabili solo nel momento in cui il fatto rimanga compreso nell'elenco delle fattispecie espresso negli artt. 266 e 266-*bis*, c.p.p..
[291] F. M. GRIFANTINI, *Inutilizzabilità*, in *Dig. pen.*, vol. VIII, Torino, 1993, p. 249.

riparativa, in secondo luogo quella della deflazione processuale e, in ultimo, quello dell'inasprimento del c.d. doppio binario[292].

Per quanto riguarda il primo ambito, si deve ricondurre ad esso non solo la nuova causa di estinzione del reato per condotte riparatorie (così come stabilito dall'art. 1, comma 1, DDL), ma anche l'inserimento all'interno dei criteri a cui il Governo dovrà attenersi in sede di riforma dell'ordinamento penitenziario di «attività di giustizia riparativa e delle relative procedure, quali momenti qualificanti del percorso di recupero sociale sia in ambito intramurario sia nell'esecuzione delle misure alternative» (così disposto dall'art. 1, comma 85, lett. f, DDL). Questo approccio tende a mettere al centro del processo penale gli individui e si basa, fondamentalmente, su una sorta di responsabilizzazione dell'agente non più nei confronti dello Stato bensì della persona offesa, distanziandosi in tal modo dal concetto di teoria retributiva della pena che caratterizza il codice penale italiano.

Per quanto riguarda il profilo della deflazione processuale, diversi sono i meccanismi previsti all'interno del provvedimento normativo tesi a sottolineare una filosofia premiale e a contenere i tempi della giustizia[293]. All'art. 1, comma 22, viene introdotta una nuova ipotesi di definizione del processo penale, in merito alla sentenza di non luogo o non doversi procedere, per incapacità irreversibile dell'imputato; all'art. 1, comma 28, viene introdotta una previsione di un termine di 10 giorni per la richiesta di incidente probatorio nei casi in cui la persona sottoposta ad indagini ne abbia fatto riserva prima del conferimento dell'incarico da parte del

---

[292] G. SPANGHER, *DDL n. 2067: sulle proposte di modifica al codice di procedura penale*, in *Giur. pen. web*, 2017, 3, in Internet al sito http://www.giurisprudenzapenale.com/wp-content/uploads/2017/03/spangher_gp_2017_3.pdf; sul punto, vedasi anche S. ZIRULIA, *Riforma Orlando: la "nuova" prescrizione e le altre modifiche al codice penale*, in Internet al sito http://www.penalecontemporaneo.it/d/5501-riforma-orlando-la-nuova-prescrizione-e-le-altre-modifiche-al-codice-penale.

[293] F. PALAZZO, *La riforma penale alza il tiro? Considerazioni sul disegno di legge A. S. 2067 e connessi*, in *Dir. pen. cont.*, *Riv. trim.*, 2016, n.1, pp. 52 e ss.

Pubblico Ministero, nei casi contemplati dall'art. 360, c.p.p., relativamente agli accertamenti tecnici non ripetibili; con l'art. 1, comma 30, viene inserito un termine di 3 mesi (i quali diventano 15 per i reati previsti dall'art. 407, comma 2, lett. a), numeri 1), 3) e 4), c.p.p.) per esercitare l'azione penale o per richiedere l'archiviazione, termine che decorre dalla scadenza del termine massimo previsto per legge per la durata delle indagini e, in ogni caso, dalla scadenza dei termini previsti dall'art. 415-*bis*, c.p.p.; all'art. 1, commi 32 e 33, viene inserito un termine di 3 mesi per fissare e decidere in merito all'udienza di archiviazione, stabilendo inoltre che, tramite il reclamo, si può ricorrere davanti al tribunale in composizione monocratica (anziché tramite il ricorso in cassazione come stabilito precedentemente), contro l'ordinanza e il decreto di archiviazione nulli; all'art. 1, comma 38, l'impugnabilità tramite il mezzo dell'appello (non tramite il ricorso per cassazione come ora) della sentenza di non luogo a procedere; all'art. 1, comma 44, viene prevista la riduzione della metà della pena in caso di condanna per una contravvenzione avvenuta tramite giudizio abbreviato (rimane la riduzione di un terzo relativamente alle condanne per i delitti); all'art. 1, comma 50, per quanto attiene le sentenze di patteggiamento, viene delimitato il ricorso per cassazione per i soli motivi attinenti all'espressione della volontà dell'imputato, al difetto di correlazione tra richiesta e sentenza, all'erronea qualificazione giuridica del fatto e all'illegalità della pena ovvero della misura di sicurezza; in ultimo, all'art. 1, comma 53, nei casi in cui si proceda per decreto, viene prevista una determinazione della pena pecuniaria, in sostituzione di quella detentiva, più bassa (75 euro al giorno a fronte dei 250 euro attualmente richiesti) e con possibilità di pagamento rateale, viene inoltre reintrodotto dall'art. 1, comma 56, il c.d. patteggiamento in appello.

Per quanto riguarda infine il rafforzamento del c.d. doppio binario, il provvedimento cardine contenuto nella legge "Orlando" è costituito dalla trasformazione da eccezione a regola della possibilità della partecipazione

a distanza, ovvero tramite videoconferenza, al dibattimento, non solo nei procedimenti penali ma anche nei giudizi civili, di quelle persone che siano state ammesse a programmi di protezione o che si trovino in stato di detenzione per i delitti previsti dall'art. 51, comma 3-*bis*, nonché dall'art. 407, comma 2, lett. a), numero 4, c.p.p..

L'elemento più interessante per i fini di questa trattazione rimane tuttavia la delega Governo attinente alla futura disciplina relativa all'utilizzo dei captatori informatici, virus *trojan*, per le intercettazioni ambientali[294], facente parte della più larga delega in tema di intercettazioni. Partendo dalla disciplina generale delle intercettazioni, la delega interviene su più ambiti[295]:

a) intervento sulle operazioni captative: nel momento in cui il Pubblico Ministero selezionerà il materiale da inviare al giudice in modo da sostenere la richiesta di misura cautelare, egli dovrà assicurare al tempo stesso la riservatezza degli atti contenenti registrazioni di conversazioni o comunicazioni informatiche ovvero telematiche che risultino essere inutilizzabili a qualunque titolo, specialmente nel caso in cui esse contengano dati sensibili non pertinenti all'accertamento di alcuna responsabilità penale o irrilevanti ai fini delle indagini; gli atti quindi non allegati alla richiesta inviata dal Pubblico Ministero dovranno essere custoditi in apposito archivio riservato, prevedendo la facoltà di ascolto ma non di copia, da parte dei difensori delle parti e del giudice; nel momento in cui viene meno il divieto di pubblicazione previsto dall'art.

[294] M. GIALUZ, A. CABIALE e J. D. TORRE, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *Dir. pen. cont.*, pp. 29 e ss., disponibile in Internet al sito http://www.penalecontemporaneo.it/upload/GIALUZCABIALEDELLATORRE_2017a.pdf.

[295] *Codice penale e di procedura: la riforma pubblicata in Gazzetta*, in Internet al sito http://www.altalex.com/documents/leggi/2017/03/15/riforma-codice-penale-e-procedura.

114, comma 1, c.p.p., i difensori potranno ottenere sia la copia degli atti sia le trascrizioni delle intercettazioni ritenute rilevanti dal giudice ovvero quelle rilasciate dal giudice dopo la conclusione delle indagini preliminari; infine, per poter instaurare una richiesta di giudizio immediato o per un deposito successivo alla conclusione delle indagini, il Pubblico Ministero dovrà chiedere lo stralcio delle conversazioni o delle comunicazioni, siano esse informatiche o telematiche, inutilizzabili per le ragioni sopra citate.

b) si prevede l'introduzione di una nuova fattispecie di reato la quale avrà il fine di punire la diffusione del contenuto di riprese audiovisive o registrazioni di conversazioni telefoniche che siano state captate in modo fraudolento e pubblicate al mero scopo di recare danno all'immagine di un individuo; tuttavia, la punibilità rimane esclusa nel momento in cui tali risultanze siano utilizzate in un procedimento amministrativo o giudiziario, ovvero quando si eserciti il diritto di difesa o il diritto di cronaca.

c) si prevede infine la semplificazione dell'utilizzo delle intercettazioni nell'ambito dei procedimenti relativi ai reati più gravi contro la pubblica amministrazione.

Per quanto riguarda invece, nello specifico, i captatori informatici, secondo il legislatore, la rosa dei reati per i quali sarebbe possibile l'utilizzo degli stessi è circoscritta alle ipotesi più gravi di delitti di criminalità organizzata[296]. L'Associazione Nazionale Magistrati, ANM, ha subito preso posizione contro tale definizione in quanto ritiene che in tal modo si "sminuisca" il mezzo di indagine e lo si renda effettivo solo per quei delitti di associazione di stampo mafioso. Dopo aver esplicitato tali prese di posizioni è tuttavia necessario delineare cosa prevede il disegno

[296] Così riferito durante la relazione introduttiva del DDL alla Camera dall'on. Ferranti, relatrice per la maggioranza, la quale, esponendo il contenuto del ddl, ha affermato che contiene: «una disciplina delle operazioni effettuate mediante immissioni di captatori informatici, il cosiddetto "Trojan", che saranno limitati ai reati più gravi di criminalità organizzata».

di legge nello specifico. All'art. 1, comma 85, lett. e) si può leggere che il Governo viene delegato a disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti, realizzate mediante l'immissione di captatori informatici in dispositivi elettronici portatili, ipotizzando che: «3) l'attivazione del dispositivo sia sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, del codice di procedura penale e, fuori da tali casi, nei luoghi di cui all'art. 614 del codice penale soltanto qualora ivi si stia svolgendo l'attività criminosa, nel rispetto dei requisiti di cui all'art. 266, comma 1, del codice di procedura penale». I reati richiamati dal tenore letterale della norma sono quindi: in primo luogo le associazioni per delinquere finalizzate a commettere i reati di riduzione in schiavitù, tratta di persone, acquisto e vendita di schiavi, prostituzione e pornografia minorile, violenza sessuale nei confronti di un minorenne, contraffazione, alterazione di marchi e brevetti, introduzione nello Stato e commercio di prodotti con segni contraffatti; in secondo luogo le associazioni di tipo mafioso, anche di natura straniera; i reati di scambio elettorale di tipo politico-mafioso; i sequestri di persona a scopo estorsivo; le associazioni a delinquere finalizzate allo spaccio di sostanze stupefacenti, al contrabbando di tabacchi lavorati esteri ed al traffico illecito di rifiuti; infine, i reati con finalità di terrorismo. A tali reati devono essere aggiunti, inoltre, quelli previsti nella seconda parte della disposizione, ossia quella che permette di usare i *trojan* nei luoghi di cui all'art. 614, codice penale, ammesso che ivi si stia svolgendo attività criminosa e nel rispetto dei requisiti stabiliti dall'art. 266, comma 1, c.p.p. Si tratta quindi, in particolare, di tutti i delitti non colposi i quali prevedono una pena superiore nel massimo a cinque anni, dei delitti contro la pubblica amministrazione, dei delitti di spaccio, dei reati relativi ad armi ed esplosivi, dei reati di contrabbando, di ingiuria, di minaccia, di usura, di molestia o disturbo agli individui per mezzo del telefono, della pornografia minorile, dell'adescamento di minorenni, della vendita e del commercio di alimenti nocivo ovvero contraffatti e, in ultimo, dello stalking. Stando

quindi a quest'elenco di reati per cui l'utilizzo del captatore risulterebbe lecito, sembra infondata la critica mossa dall'Associazione Nazionale Magistrati, in quanto il testo sembra concedere alle procure della Repubblica uno strumento di indagine di enorme portata investigativa, disciplinando inoltre un solo aspetto relativo ai captatori informatici, ossia quello attinente alla funzione intercettiva del virus *trojan*, dimenticando quindi tutte le altre funzioni che il virus può esplicitare una volta "infettato" il *device* (accesso a *file*, e-mail, *chat*, immagini, video, rubriche, *screenshot*, etc.)[297]. La legge prevede inoltre la possibilità di operare tramite il virus *trojan*, avviando di fatto la registrazione audio, anche per il «personale incaricato» dalla polizia giudiziaria, oltre che dagli stessi agenti. Questo, in altri termini, vuol dire continuare a far gestire di fatto le indagini a società private, terze rispetto agli organi investigativi, come avviene tutt'oggi[298]. Si sottolinea inoltre che il testo del disegno di legge è stato oggetto di critica, per quanto riguarda le linee guida attinenti alla futura disciplina del *trojan*, da numerose associazioni che si occupano di diritti umani e digitali[299]. Per quanto riguarda, infine, l'utilizzabilità delle risultanze probatorie captate tramite l'utilizzo dei captatori informatici, la delega specifica che i risultati di tali intercettazioni potranno essere utilizzati per fini probatori solo dei reati oggetto del provvedimento autorizzativo; se fossero captate conversazioni di soggetti terzi alle

[297] M. A. SENOR, *DDL Orlando, ecco le conseguenze giudiziarie delle intercettazioni con trojan*, in Internet al sito https://www.agendadigitale.eu/documenti/ddl-orlando-ecco-le-conseguenze-giudiziarie-delle-intercettazioni-con-trojan/.

[298] C. FREDIANI, *Ddl Orlando: più facile e frequente l'utilizzo di trojan*, in Internet al sito http://www.lastampa.it/2017/05/22/tecnologia/news/ddl-orlando-pi-facile-e-frequente-lutilizzo-di-trojan-poBLFWMRJ7IBnbUg0XtlzJ/pagina.html.

[299] Su tutte, si segnalano il rapporto diffuso di una ong britannica, *Privacy International*, e dalla Coalizione Italiana Libertà e Diritti Civili (CILD), secondo il quale l'attuale testo non soddisferebbe «gli standard di legalità, necessità e proporzionalità, né stabilisce procedure sufficienti di minimizzazione, vigilanza efficace o salvaguardia da abusi». Il rapporto è disponibile in Internet al sito https://medium.com/@privacyint/press-statement-privacy-international-and-the-italian-coalition-for-civil-liberties-and-rights-7c2a98e004c5.

indagini, esse non potranno essere in alcun modo conoscibili, divulgabili o pubblicabili; per quanto riguarda invece l'utilizzo delle risultanze probatorie ottenute tramite i captatori in procedimenti diversi, rimane ferma le deroga al loro utilizzo per i reati per cui è previsto l'arresto in flagranza, così come disposto dall'art. 380, c.p.p.

# Capitolo 6

# Profili comparatistici: la normativa europea e nordamericana

SOMMARIO: 1 – La Convenzione *Cybercrime* di Budapest. – 2 – Il Regolamento Generale sulla Protezione dei Dati (GDPR). – 3 – L'esperienza tedesca: la Corte Costituzionale e la sentenza sulle misure di sorveglianza occulta. – 4 – Il caso NSA: l'abuso dello strumento intercettivo da parte del governo statunitense.

## 1 – La Convenzione *Cybercrime* di Budapest

In ambito europeo, molti sono i provvedimenti in tema di intercettazioni, detenzione di dati personali e reati connessi alla criminalità informatica, tuttavia alcuni risultano di particolare rilievo ai fini di questa trattazione.

In primo luogo, è utile citare la c.d. direttiva *"Data Retention"*[300], promulgata come risposta agli attentati di Madrid del 2004, la quale imponeva agli operatori telefonici di memorizzare i dati di traffico per un periodo variabile da sei mesi a due anni, in modo tale da poter utilizzare tali dati in sede di indagine. Tale Direttiva ha subito incontrato l'opposizione dei governi degli Stati membri, come ad esempio In Repubblica Ceca, Germania o Romania, dove le rispettive Corti

[300] Direttiva 2006/24/CE, 15 marzo 2006, «riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE», in Internet al sito http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:IT:PDF.

costituzionali hanno dichiarato incostituzionali le leggi attuative della direttiva stessa, arrivando, in ultimo, ad essere invalidata dalla stessa Corte di Giustizia dell'Unione Europea. La vita "breve" della direttiva è stata determinata nel momento in cui la Corte ha dovuto affrontare la questione della validità inerente a tale direttiva nelle cause C-293/12 e C-594/12. La decisione della Corte di Giustizia ha affrontato quindi, per la prima volta, la questione relativa al bilanciamento fra le esigenze di repressione e di accertamento dei reati da un lato e, dall'altra parte, la tutela dei diritti fondamentali dell'individuo, limitati dalla nuova disciplina introdotta dalla direttiva. Tale decisione ha impattato, senza dubbio alcuno, sugli ordinamenti nazionali e sulle attività investigative poste in essere mediante l'acquisizione di dati e di informazioni presso i *service providers*. Analizzando i ricorsi presentati, la Corte è arrivata ad affermare l'incompatibilità della direttiva 2006/24, in quanto essa eccedeva i limiti imposti dal principio di proporzionalità alla luce degli artt. 7, 8 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea[301]. La decisione della Corte, totalmente condivisibile sia da un punto di vista argomentativo sia da un punto di vista fattuale, si scontra tuttavia con l'attuale assetto sociale ed economico nel quale, come è stato sottolineato più volte, il ricorso a strumenti investigativi al passo con il progresso tecnologico e anche alla c.d. *data retention* risultano indispensabili. Tuttavia, sebbene indispensabili, la complessità di tale materia, impone che il bilanciamento più volte richiesto fra le esigenze di tutela e quelle di repressione ed accertamento sia posto in essere sulla base di un rapporto di "complicità" e dialogo fra tre figure: gli "operatori" del diritto, la società civile e, necessariamente, gli esperti di scienze extragiuridiche, come

[301] C. eur., grande sezione, Cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e al.*, 8 aprile 2014, in Internet al sito http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62012CJ0293&from=IT.

quella informatica[302].

In secondo luogo, il Consiglio d'Europa, nel 1977, ha visto insediarsi al suo interno un comitato di esperti a cui si deve la struttura attuale della Convenzione *Cybercrime* di Budapest[303]. Tale struttura si rinviene già nella Raccomandazione n. R (95) 13 dell'11 settembre 1995[304] del Consiglio dei Ministri agli Stati membri relativa ai problemi di procedura penale legati alla tecnologia dell'informazione. Detta raccomandazione, prendendo spunto e richiamando pregresse raccomandazioni[305], raccomandava ai governi degli Stati membri, nel momento in cui avrebbero modificato le rispettive legislazioni, di ispirarsi ai principi generali di coordinamento e di adattamento chiaramente tracciati in ambito europeo, delineando quindi in modo chiaro e applicando, di conseguenza, la distinzione operata dal diritto tra la perquisizione dei sistemi informatici, il sequestro dei dati raccolti e l'intercettazione di dati che si stiano trasmettendo in tempo reale. La Convenzione è stata approvata dai Ministri degli esteri dei paesi del Consiglio d'Europa l'8 novembre del 2001, venendo aperta di conseguenza alle sottoscrizioni il 23 novembre 2001 ed entrando in vigore, ufficialmente, il 1° luglio 2004. Essa è stata ratificata attualmente da 21 Stati. Di pari passo con la Convenzione è stato anche insediato, per mezzo di un protocollo addizionale, un Comitato di esperti avente il

[302] R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "Data Retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2014, 2, pp. 178 e ss.
[303] O. MORALES GRACIA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul Cyber-Crime*, in *Il diritto penale dell'informatica*, di L. Picotti, Padova, 2000, p. 123.
[304] Raccomandazione n. R (95) 13, 11.9.1995, in *Rivista italiana di intelligence*, in Internet al sito http://gnosis.aisi.gov.it/sito%5CRivista8.nsf/servnavig/14.
[305] In particolare: Raccomandazione n. R (85) 10 relativa alle commissioni rogatorie per la sorveglianza delle telecomunicazioni; Raccomandazione n. R (81) 20 relativa all'armonizzazione delle legislazioni nazionali in ambito di esibizione di documenti e in materia di ammissibilità di replicazione di documenti e di registrazioni informatiche; Raccomandazione n. R (87) 15, relativa alla regolarizzazione dell'utilizzo di dati a carattere personale in ambito politico; Raccomandazione n. R (89) 9 in ambito di criminalità informatica.

compito di elaborare una proposta legislativa in ambito penale riguardante gli atti di razzismo e xenofobia perpetrati in rete, estendendo quindi tramite tale previsione, le previsioni contenute nella Convenzione. Tale protocollo addizionale prevede inoltre la l'irrogazione di una sanzione penale per «atti commessi con motivazioni razziste e per mezzo di un sistema informatico, in particolare la divulgazione di materiale a sfondo razzista, l'offesa pubblica per motivi razzisti nonché la negazione e la minimizzazione di genocidi», entrando ufficialmente in vigore il 1° marzo 2006[306]. Nel preambolo della Convenzione, la finalità principale evidenziata è quella di rafforzare la coesione degli Stati membri dell'Unione europea, riconoscendo come elemento essenziale la collaborazione tra di essi, arrivando quindi a definire una politica comune in campo penale al fine di proteggere la società moderna contro il *cybercrime* attraverso l'implementazione di una legislazione appropriata[307]. Si può affermare quindi che i principali obiettivi della Convenzione siano tre:

a) l'armonizzazione del diritto penale in materia di *cybercrime* e dei reati ad essa collegati;

b) il conferimento, agli organi investigativi dei singoli Stati, del potere ma soprattutto degli strumenti necessari per poter svolgere indagini sul *cybercrime* e sui reati collegati, commessi quindi per mezzo di un sistema informatico o per i quali siano disponibili prove in formato digitale;

c) l'organizzazione di un sistema internazionale di cooperazione che sia rapido ed efficace, che preveda rapporti diretti tra le autorità degli Stati aderenti alla Convenzione e che, di conseguenza, superi in maniera

[306] G. CORASANITI, *Autorizzazione alla ratifica*, in *Cybercrime, responsabilità degli enti, prova digitale*, *Commento alla legge 18 marzo 2008, n. 48*, di G. Corasaniti e G. C. Lucente, CEDAM, Milano, 2009, pp. 8 e ss.
[307] U. SIEBER, *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in *Riv. trim. di dir. pen. dell'econ.*, 1997, p. 496.

efficace le formalità burocratiche previste dai canali diplomatici tradizionali.

Per quanto riguarda invece i beni giuridici tutelati dalla Convenzione, risulta opportuno richiamare il testo dell'art. 1, il quale riporta la definizione di sistema informatico, definendolo come «qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati», mentre per quanto riguarda l'espressione relativa ai dati informatici, lo stesso articolo li definisce come «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione». La dottrina italiana, relativamente alla nozione di bene giuridico applicabile ai reati informatici, ha elaborato diverse ipotesi, alcune delle quali si richiamano ai diritti della persona, ossia all'utilizzatore o organizzatore del "sistema", altre invece che sottolineano il valore dei dati elaborati, valore quindi tutelabile dall'ordinamento italiano[308]. In questo modo, il dettato della Convenzione risulta quindi allargare in modo considerevole la nozione di sistema informatico, superando quindi la tradizionale distinzione tra *hardware* e *software*, arrivando così a comprendere, in linea con il progresso tecnologico, qualsiasi applicazione o infrastruttura che sia anche solo potenzialmente utilizzabile per fini illeciti[309].

Da un punto di vista strettamente applicativo invece, la Convenzione porta con sé la novità relativa all'applicabilità della stessa non solamente ai c.d.

[308] Vedasi, per ulteriori approfondimenti, E. GIANNANTONIO, *L'oggetto giuridico dei reati informatici*, in *Cass. pen.*, 2001, p. 2244; F. BERGHELLA e R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, p. 2329; P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, pp. 46 e ss.

[309] S. SEMINARA, *La responsabilità penale degli operatori su Internet*, in *Il diritto dell'informazione e dell'informatica*, 1998, p. 745.

*computer's crimes*, ma anche a tutte le fattispecie di reato commesse mediante l'utilizzo di un sistema informatico, prevedendo inoltre che sia applicabile anche per i reati per i quali sia necessario, o addirittura possibile, il raccoglimento di prove in formato elettronico (così previsto agli artt. 14 e 23). Per quanto riguarda invece l'ambito processuale, la Convenzione fornice diversi strumenti per rendere efficace l'azione contro il *cybercrime*. In primo luogo devono essere assicurate misure volte a garantire: la conservazione rapida ed efficace dei dati informatici (artt. 16 e 17); il mantenimento dell'integrità delle informazioni raccolte (art. 16, comma 2); la facoltà di procedere, per gli organi investigativi, alla perquisizione, al sequestro o all'accesso a sistemi, dati o supporti informatici (art. 19). Gli artt. 20 e 21 prevedono poi l'introduzione di regole uniformi all'interno degli Stati membri relativamente alle operazioni di intercettazione e di registrazione delle comunicazioni telematiche. La previsione quindi di molte misure provvisorie al fine di accelerare l'esecuzione delle attività investigative, come quelle citate sopra o ancora, ad esempio, le intercettazioni del contenuto di comunicazioni trasmesse attraverso l'uso di elaboratori elettronici così come previsto dagli artt. 33 e 34, permettono di snellire i tempi delle indagini. Tale processo di snellimento è ulteriormente accentuato dalla previsione secondo la quale ciascuno Stato, prima ancora di inoltrare una rogatoria internazionale al fine di eseguire una perquisizione, un sequestro o altri mezzi di ricerca della prova, potrà ottenere la misura, a carattere provvisorio, della conservazione rapida dei dati informatici contenuti all'interno di un sistema informatico ubicato all'estero[310].

La Convenzione è stata ratificata per mezzo della legge 18 marzo 2008, n.

[310] Tale previsione risulta particolarmente utile in tema di captatori informatici, nel momento in cui gli organi investigativi decidano di "prelevare" dal sistema informatico sottoposto ad intercettazioni, il traffico e-mail, spesso ubicato su *server* di origine estera, così come analizzato anche nel corso dei precedenti capitoli.

48, con la quale è stato approvato il disegno di legge riguardante appunto la ratifica e l'esecuzione della Convenzione. Tale legge è andata a modificare il codice di procedura penale nell'ambito relativo ai mezzi di ricerca della prova e in quello delle indagini di polizia giudiziaria, specificando particolari modalità di esecuzione di ispezioni, perquisizioni e sequestri, con l'implementazione di regole *ad-hoc* relativamente alla conservazione, all'intangibilità dei dati originali estrapolati ed alla conformità delle copie. Tali prescrizioni trovano fondamento, come già analizzato nel corso di questa trattazione, nelle tecniche di *computer forensics* e di *best practices* relativamente alla ricerca e alla conservazione delle prove digitali.

In particolare, per mezzo della Convenzione *Cybercrime* di Budapest e per poter assicurare dei mezzi efficaci di contrasto alla criminalità elettronica, è stato introdotto l'art. 266-*bis* all'interno del codice di procedura penale, in quale autorizza le intercettazioni di comunicazioni relative a sistemi informatici o telematici, per i procedimenti relativi ai reati di cui all'art. 266, c.p.p., ed in quelli in cui i reati siano stati commessi per mezzo di tecnologie informatiche o telematiche. Così facendo, la nuova previsione normativa non limita tali intercettazioni ai reati ontologicamente elettronici (ossia quelli introdotti dalla legge 23 dicembre 1993, n. 547 sui c.d. *computer's crime*), ma la estende in modo da ricomprendere nel suo alveo qualsiasi fattispecie per cui l'autore ha utilizzato un qualsiasi strumento informatico o telematico. Uno dei rilievi più importanti risulta essere quello relativo alla competenza territoriale, in quanto, secondo il dettato della Convenzione, ogni comunicazione in entrata (anche proveniente dall'estero) su un'utenza o su un sistema ubicati sul territorio nazionale ovvero anche tutti gli altri scambi di dati diretti all'estero, risultano essere assoggettati alla giurisdizione dello Stato. In questo modo, non risulta esserci nessuna violazione delle norme relative alle rogatorie internazionali nel momento in cui gli organi inquirenti dispongano

intercettazioni di comunicazioni provenienti dall'Italia e dirette all'estero, in quanto l'attività di captazione, ricezione e registrazione di tali flussi informatici risulta espletata interamente sul territorio italiano[311].

## 2 – Il Regolamento Generale sulla Protezione dei Dati (GDPR)

Rimanendo in ambito europeo, un altro provvedimento che occorre analizzare è il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, il quale deve essere esaminato soprattutto alla luce di quanto detto sopra relativamente alla direttiva c.d. *Data Retention*. Il motivo fondamentale dell'analisi di tale regolamento ai fini di questa trattazione, oltre a quello poco fa citato, è lo stretto collegamento tra l'utilizzo dei captatori informatici e il dettato dell'art. 8 della CEDU, così come richiamato anche nell'art. 1 del sopra citato regolamento e che vale la pena riportare in quanto esso afferma che «la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea, stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano[312]». Tale collegamento risulta importante, così come analizzato nei capitoli precedenti, nel momento in cui si prendono in

[311] In dottrina, L. CUOMO e R. RAZZANTE, *La nuova disciplina dei reati informatici*, Giappichelli Editore, 2009, p. 85; in giurisprudenza, cfr. Cass. sez. IV, 30 giugno 2004, n. 37646, in *Cass. pen.*, 2006, 5, p. 1837.

[312] Art. 1, Regolamento UE 2016/679, 27 aprile 2016, in Internet al sito http://eurlex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:32016R0679&from=GA.

considerazione le potenzialità intrusive molto elevate del captatore informatico e quindi la sua capacità di estrapolare dati a carattere personale. Lo strumento del regolamento è stato quindi adottato in modo da far fronte alle numerose critiche mosse contro la c.d. "Direttiva Privacy"[313], poiché in quanto direttiva, è stata attuata con differenze talvolta sostanziali, all'interno degli Stati membri, ponendo in essere quindi un'armonizzazione non in linea con quanto richiesto dalla Comunità europea. Poiché inoltre tale direttiva è stata applicata quando Internet non era ancora uno strumento così diffuso come lo è oggi, per non parlare dei *social network* o delle *app*, risultava necessario una nuova normativa che potesse far fronte a tali sfide lanciate dal progresso tecnologico. Per quanto riguarda l'Italia, in particolare, il Regolamento andrà a sostituire il "Codice della Privacy", in vigore dal 1° gennaio 2004. Per quel che concerne l'ambito applicativo, il Regolamento si applica a tutti i trattamenti che vengano effettuati da un titolare stabilito all'interno del territorio dell'Unione europea, nonché a tutti i trattamenti che abbiano ad oggetto dati a carattere personale che vengano effettuati da tutti i soggetti, sia titolari che responsabili, che abbiano sede al di fuori dell'Unione europea e riguardi l'offerta di beni e servizi ed infine, nella parte che più risulta connessa con il tema di questa trattazione, al monitoraggio di comportamenti che hanno luogo all'interno dell'Unione europea[314].

Tra le svariate novità introdotte dal Regolamento, lo strumento più innovativo risulta essere quello della c.d. *Data Breach Notification*, previsto dall'art. 33 del Regolamento, il quale prevede che nel momento in

[313] Diretttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in Internet al sito http://194.242.234.211/documents/10160/10704/Direttiva+95+46+CE.pdf.
[314] L. LIGUORI, *E' in vigore il nuovo regolamento generale sulla protezione dei dati*, in Internet al sito https://www.filodiritto.com/articoli/2016/06/-in-vigore-il-nuovo-regolamento-generale-sulla-protezione-dei-dati.html.

cui avvenga una violazione dei dati personali si renderà necessaria la comunicazione di tale violazione all'autorità di vigilanza dello Stato membro. In particolare, secondo quanto riportato dal Regolamento stesso, questa particolare violazione degli standard di sicurezza dei dati personali, può comportare «accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati». In caso una violazione di questo genere venga posta in essere ugualmente, sussiste un obbligo informativo, da parte non solamente dei fornitori di servizi di comunicazioni elettroniche ma anche da altri operatori, presso le autorità di controllo, da effettuare senza indebito ritardo, inoltre, ove possibile, tale obbligo è da adempiere entro e non oltre 72 ore dopo la conoscenza della violazione posta in essere[315].

In ultimo, viene prevista l'istituzione di una nuova figura professionale di riferimento, obbligatoria per le amministrazioni e gli enti pubblici ed anche in ambito privato in particolari casi, ossia quella del Responsabile per la protezione dei dati personali (*Data Protection Officer*), così come disposto dall'art. 37 del Regolamento. Per quanto riguarda gli aspetti essenziali di tale figura, innanzitutto essa deve possedere requisiti di autonomia ed indipendenza, a differenza di quanto accadeva per la figura prevista dall'art. 29, Codice della *Privacy*, ossia del responsabile *privacy*, il quale era soggetto al mandato fornito dal titolare dei dati personali rispetto al loro trattamento, venendo meno quindi il requisito di ampia autonomia ed indipendenza richiesto invece per la nuova figura professionale disciplinata dal Regolamento. Quanto invece ai compiti[316] che il *Data Protection Officer*

[315] F. TRAFICANTE, *Regolamento UE Privacy: Data Security e Data Breach Notification*, in Internet al sito http://www.techeconomy.it/2016/03/03/regolamento-ue-privacy-parte-1-data-security-data-breach-notification/.

[316] F. DI RESTA, *Il nuovo regolamento generale sulla protezione dei dati personali: un continente una legge, ma occorre essere preparati*, in Internet al sito http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-04-15/il-nuovo-

sarà chiamato a svolgere, nonostante il Regolamento non li esponga in modo chiaro e preciso e quindi risultino di complessa delineazione, essi si possono distinguere in:

1) sorvegliare sull'applicazione, in modo corretto, della normativa in tema di protezione dei dati, sia a livello europeo che a livello nazionale; sorvegliare sull'osservanza delle politiche interne dell'ente ed in ordine all'attribuzione delle responsabilità oltre che alla sensibilizzazione del personale che partecipa in modo diretto ai trattamenti dei dati personali e alle relative attività di controllo degli stessi;

2) fornire pareri e vigilare in merito ad una corretta esecuzione di una *Data protection impact assessment*, ovvero un Piano di Valutazione d'Impatto sui Dati Personali, previsto dall'art. 35 del Regolamento e redatto ogni qualvolta risulta esserci una mutazione nelle modalità di trattamento dei dati[317];

3) fungere da figura di contatto e di collaborazione con l'Autorità Garante per la protezione dei dati personali.

Un cenno va fatto, infine, al nuovo impianto sanzionatorio previsto dal Regolamento all'art. 83. Tale norma stabilisce infatti che, in caso di violazione di determinate disposizioni[318], le sanzioni siano alquanto

---

regolamento-generale-protezione-dati-personali-continente-legge-ma-occorre-essere-preparati-171042.php.

[317] Per un approfondimento sul tema, vedasi *Data protection impact assessment (DPIA o PIA), Piano di impatto sulla protezione dei dati (PIPD)*, in Internet al sito http://www.leggesullaprivacy.it/ita/data_protection_impact_assessment_piano_impatto_protezione_dati.asp.

[318] Tali disposizioni a cui l'art. 83 del Regolamento fa riferimento risultano essere: a) i principi base del trattamento, comprese le condizioni relative al consenso, così come disciplinati dagli artt. 5, 6, 7 e 9; b) i diritti degli interessati, a norma degli artt. da 12 a 20; b-*bis*) i trasferimenti di dati personali ad un destinatario in un paese terzo o ad una organizzazione internazionale, così come disposto dagli artt. da 40 a 44; b-*ter*) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; c) in caso di mancata osservazione di un ordine, di una limitazione provvisoria o definitiva di

elevate. In particolare si prevedono sanzioni amministrative pecuniarie fino ad un massimo di 20 milioni di euro, nel caso invece tali violazioni siano perpetrate da imprese, le sanzioni applicabili andranno fino al 4% del fatturato mondiale totale annuo del precedente esercizio, in caso esso risultasse superiore.

Nonostante tutti i "buoni propositi" e gli strumenti che il Regolamento dovrebbe introdurre, rimane tuttavia indubbio che sarà necessaria una ingente produzione normativa, a livello nazionale, che dovrà accompagnare tale Regolamento, in quanto esso sembra configurarsi come una sorta di elencazione di principi in attesa di essere definiti in maniera migliore e più lineare dalle legislazioni nazionali[319].

# 3 – L'esperienza tedesca: la Corte Costituzionale e la sentenza sulle misure di sorveglianza occulta

Il problema relativo alle intercettazioni eseguite mediante l'inoculazione di un virus informatico, ossia il captatore, è stato affrontato anche da diversi Stati membri dell'Unione europea, con risultati diversi.

In Spagna, per mezzo della legge n. 13 del 2015[320], è stata disciplinata la

---

trattamento, oppure di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

[319] M. IASELLI, *Protezione dei dati personali: il nuovo Regolamento Europeo in Gazzetta Ufficiale UE*, in Internet al sito http://www.altalex.com/documents/news/2015/12/23/accordo-raggiunto-sul-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.

[320] *Ley Organica 13/2015, de modificaciòn de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantias procesales y la regulaciòn de las medidas de investigaciòn tecnològica*, in Internet al sito

captazione e la registrazione mediante l'impiego di dispositivi elettronici, prevedendo inoltre che l'utilizzo dei captatori informatici sia delimitato alle indagini nelle quali tale mezzo di ricerca della prova risulti necessario e sussidiario agli altri mezzi di ricerca probatoria. La norma prevede, inoltre, che il decreto con cui il giudice autorizza l'utilizzo del captatore informatico specifichi le generalità degli individui nei cui confronti verranno eseguite le intercettazioni, i mezzi attraverso i quali si procederà alla captazione delle telecomunicazioni ed i luoghi in cui esse verranno espletate.

In Francia, la previsione dell'utilizzo del virus informatico in funzione di captatore è si prevista[321], ma per i delitti più gravi, tra i quali sono compresi quelli di criminalità organizzata e di terrorismo. Tale possibilità è stata recentemente introdotta, a seguito della legge 9 marzo 2004, come disciplina derogatoria in materia di criminalità organizzata. La normativa francese prevede inoltre un profondo controllo da parte del giudice, a pena di nullità, rispetto all'utilizzo di tali intercettazioni, come ad esempio la precisa indicazione del reato per il quale risulta giustificato l'utilizzo del captatore informatico, la localizzazione esatta o la descrizione del sistema informatico nonché la durata delle operazioni, senza tuttavia prevedere, come accade in Italia, il requisito della preventiva specificazione dei luoghi in cui la captazione verrà attuata[322].

Un caso importante di utilizzo di tali sistemi captativi si è avuto in Germania nel 2011, quando venne diffusa una copia dello *spyware* in uso alla Polizia federale tedesca e prodotto dalla società DigiTask, pubblicando inoltre un'analisi tecnica molto dettagliata nella quale era possibile dimostrare come tale programma, oltre a consentire la "tradizionale" intercettazione audio, fosse in grado di effettuare il *download* di *file* dal

---

https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf.

[321] Art. 706-102-1, Libro IV, Titolo XXV, *Code de procedure penal*.

[322] Per i riferimenti alla normativa francese e spagnola sopra citati, vedasi G. LA CORTE, *Il trojan: le intercettazioni*, op. cit., pp. 17-18.

computer dell'indagato e catturare immagini dallo schermo (*screenshot*). Invero, la possibilità di eseguire attività di indagine mediante programmi *backdoors* era stata introdotta in Germania nel 2006, nel *Land* del Nord Reno-Westfalia, come conseguenza di una modifica della Legge sulla protezione della Costituzione del *Land*. Tale norma risulta essere il primo caso di conferimento ad un'autorità tedesca, tramite il § 5, comma 2, n. 11 di tale legge, di un potere esplicito di accesso segreto a sistemi informatici e quindi di *Online Durchsuchung*, ossia *on line search* e *on line surveillance*[323]. Su questo tema è dovuta intervenire la Corte costituzionale federale tedesca, la quale, con la sentenza 27 febbraio 2008[324], ha dichiarato incostituzionale la disposizione sopra citata. Secondo la Corte, l'incostituzionalità di tale disposizione scaturisce dal contrasto evidente tra l'attività di *intelligence* posta in essere rispetto ad un nuovo diritto fondamentale, ossia quello che tutela il cittadino nel momento in cui egli utilizzi tecnologie di informazione e di comunicazione in rete, inteso come espressione del più generale diritto alla dignità dell'individuo-utente. La Corte affermava quindi l'esistenza di un nuovo diritto di rango costituzionale, quello alla riservatezza ed alla integrità dei sistemi informatici[325]. Gli utenti, a parere della Corte, godono quindi di una legittima aspettativa di riservatezza rispetto a dati da cui è possibile ricavare elementi sulla personalità degli utenti stessi, tracciandone quindi un vero e proprio profilo, per cui la segretezza e l'integrità di essi rappresentano dunque diritti fondamentali dell'individuo. Oltre ciò, la

[323] R. FLOR, *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del* Bundesverfassungsericht *e della* Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e data retention*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti processuali*, di L. Picotti e F. Ruggieri, Giappichelli editore, 2011, pp. 32 e ss.

[324] Cfr. Bundesverfassungsericht, 27 febbraio 2008, in *Riv. trim. dir. pen. econ.*, 2009, 3, pp. 679 e ss.

[325] Cfr. *Memoria per la Camera di Consiglio delle Sezioni Unite della Procura Generale presso la Corte di Cassazione del 28 aprile 2016. Cenni di diritto comparato sulle esperienze tedesca, spagnola e francese e sull'O. E. I. (Ordine di indagine* europeo*)*, in Internet al sito www.dirittopenalecontemporaneo.it.

Suprema corte ha ritenuto la norma in esame non conforme ai principi di chiarezza, determinatezza e proporzionalità, specificando inoltre che tali attività di indagine devono essere controbilanciate da idonee precauzioni procedurali, ossia delimitando l'utilizzo di tali strumenti ad un provvedimento del giudice che svolga un controllo necessariamente preventivo. Bisogna sottolineare tuttavia che la declaratoria di incostituzionalità non ha riguardato, pertanto, i nuovi mezzi di ricerca della prova in quanto tali, ma bensì le loro modalità di utilizzo, i presupposti ed i limiti per la loro adozione in sede di investigazioni. In altri termini, secondo la Corte, il legislatore avrebbe dovuto determinare i casi, le finalità ed i limiti della compressione del nuovo diritto fondamentale, in modo tale da rendere ben definita, in ossequio ai principi di proporzionalità, determinatezza e chiarezza, l'area di intervento riferibile ai gravi reati a tutela di importanti beni giuridici per cui l'utilizzo dei captatori informatici risulta consentito, oltre che infine prevedere la riserva dell'autorità giudiziaria sul controllo di detti requisiti caso per caso.

Il 20 aprile 2016, la Corte costituzionale tedesca si è dovuta esprimere di nuovo in merito a misure di sorveglianza occulte e relativamente alla captazione di conversazioni da remoto tramite strumenti informatici[326], dichiarando l'incostituzionalità di talune disposizioni facenti parte della legge federale denominata *Bunderskriminalamtgesetz – BKAG* – che disciplina i compiti e l'attività posta in essere dalla polizia federale tedesca, legge contenuta nella sottosezione della legge dedicata alla prevenzione e al combattimento delle minacce terroristiche internazionali[327]. La Corte ha infatti affermato, in linea con la precedente

[326] Bundersverfassungsgericht, I Senato, 20 aprile 2016 – 1 BVR 966/09, 1 BVR 1140/09, in Internet al sito https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html.

[327] *Unterabschnitt Abwehr von Gefahren des internationalen Terrorismus*, paragrafi da 20a a 20x, introdotti il 25 dicembre 2008 con efficacia dal 1° gennaio 2009, in Internet al sito

decisione del 27 febbraio 2008, che in linea generale e per fini di protezione della società contro le minacce di terrorismo internazionale, le misure di sorveglianza occulta adottate dalla polizia federale criminale risultano compatibili con i diritti fondamentali dell'individuo riconosciuti dalla Costituzione, tuttavia, la medesima Corte ha censurato le disposizioni impugnate sotto diversi aspetti, di cui due risultano fondamentali[328]:

a) in primo luogo la Corte critica il paragrafo 20g, da 1 a 3, della BKAG (*Bundeskriminalamatgesetz*), il quale prevede le disposizioni relative all'utilizzo di mezzi speciali di sorveglianza in luoghi diversi dal domicilio, come ad esempio l'osservazione, la registrazione audio-video, l'applicazione di dispositivi di localizzazione o l'uso di informatori della polizia. Secondo la Corte infatti, i poteri attribuiti alla polizia federale non sono sufficientemente delimitati dalla legge. In particolare, per l'utilizzo di simili mezzi di investigazione, anche se essi sono autorizzati dalle norme costituzionali, occorre che sia prevedibile almeno uno specifico fatto-reato o, in mancanza di esso, che il comportamento di una persona sia atto a comprovare la probabilità specifica che egli possa commettere reati di matrice terroristica in un futuro prossimo. Per il monitoraggio a lungo termine poi, o per l'ascolto di conversazioni che non siano pubbliche, ci sono casi in cui è richiesta necessariamente l'autorizzazione preventiva dell'autorità giudiziaria mentre, in altri casi, essa è richiesta solo dopo un mese dall'inizio delle operazioni intercettive. Infine, all'interno delle disposizioni censurate, nel momento in cui si consente la raccolta e l'analisi dei dati personali, allo stesso modo non è prevista alcuna misura per assicurare il rispetto dello spazio riservato, il quale caratterizza la vita

---

https://beck-online.beck.de/?vpath=bibdata/ges/BKAG/cont/BKAG.G2.G4.htm.

[328] L. GIORDANO e A. VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in Internet al sito http://www.penalecontemporaneo.it/d/4703-la-corte-costituzionale-tedesca-sulle-misure-di-sorveglianza-occulta-e-sulla-captazione-di-conversa.

privata di ogni individuo e che risulta pertanto escluso a qualsiasi ingerenza pubblica;

b) in secondo luogo, la decisione afferma che il paragrafo 20k della BKAG, per mezzo del quale è consentito l'accesso ai sistemi informatici da remoto (si citava, all'interno della sentenza, anche l'accesso al disco rigido di un computer attraverso l'utilizzo di un *trojan*), non consente la previsione di una protezione quantomeno sufficiente della vita privata. Tale critica riguarda in particolar modo il fatto che la normativa attuale prevede un controllo eseguito dal personale dell'ufficio federale della polizia penale invece di quello eseguito da parte di soggetti esterni e indipendenti.

La Corte specifica inoltre che, per quanto attiene alle operazioni di sorveglianza che si svolgono in abitazioni private, il principio di proporzionalità risulta solamente in parte soddisfatto poiché nel caso tali operazioni coinvolgano, come è possibile che succeda, terze persone estranee alle indagini, il loro diritto alla riservatezza verrebbe violato. Di conseguenza, secondo il parere della Corte, tutte le risultanze relative alle intercettazioni devono essere affidate ed analizzate ad un organismo terzo ed indipendente, facendo così in modo di eliminare qualsiasi dato o informazione non strettamente attinente alle indagini prima che il tutto venga affidato alla polizia federale[329].

Tale decisione, in conclusione, assieme a quella del 27 febbraio 2008, nonostante non sia stata adottata all'unanimità in quanto due giudici della Corte costituzionale tedesca hanno fatto registrare il loro dissenso, rappresenta senza ombra di dubbio un intervento molto significativo nel complicato rapporto che intercorre tra il rafforzamento dei mezzi investigativi al fine di reprimere e prevenire reati gravi quali quelli legati al

[329] 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.

terrorismo e, dall'altro lato, le garanzie fondamentali degli individui che risultano compresse da tali strumenti d'indagine.

# 4 – Il caso NSA: l'abuso dello strumento intercettivo da parte del governo statunitense

Dopo aver analizzato le più importanti disposizioni in tema di intercettazioni e di captatori informatici all'interno dell'Unione europea, risulta particolarmente interessante procedere all'analisi della normativa nordamericana sul tema nonché alla disamina dello scandalo c.d. *Datagate* avvenuto nel 2013 proprio per l'abuso di tali programmi intercettivi.

La disciplina americana delle intercettazioni, telefoniche, telematiche e ambientali, a livello federale, è contenuta negli artt. 2510 e ss. del *Title* 18, Parte 1, Capitolo 119, relativo alle norme di procedura penale, dello *US Code*[330]. L'articolo 2518 risulta particolarmente importante in quanto stabilisce i requisiti attraverso i quali il giudice può validamente emanare un provvedimento autorizzativo di intercettazioni, prevedendo che si debba riscontrare, in particolare:

a) il fondato sospetto che un individuo stia commettendo, abbia commesso ovvero si appresti a commettere uno dei reati indicati all'art. 2516;

b) il fondato motivo di ritenere che, attraverso l'uso delle intercettazioni,

[330] Lo *United States Annotated Code* o *U.S.C.A.* non è riferibile alla nozione utilizzata nei paesi di *civil law* di "codice", bensì rappresenta una compilazione ufficiale di tutta la legislazione federale con la relativa giurisprudenza, così come definito da F. DE FRANCHIS, *Dizionario Giuridico*, Giuffrè, Milano, 1984.

sarà possibile ottenere specifiche informazioni relativamente al reato per il quale si procede;

c) sia già occorso l'espletamento delle normali procedure investigative senza tuttavia apportare buoni risultati ovvero appare agli organi investigativi che esse porteranno risultati concreti ovvero ancora ciò potrebbe risultare pericoloso;

d) infine, deve esistere il fondato sospetto di ritenere che i luoghi in cui le captazioni avranno luogo sono utilizzati o stiano per essere utilizzati relativamente alla commissione del reato, ovvero detti luoghi siano stati concessi, intestati o normalmente utilizzati dal soggetto sottoposto ad indagini[331].

Tale disciplina si va ad "incastrare" con l'utilizzo del virus *trojan* per scopi intercettivi e, in particolar modo, occorre esaminare detto strumento alla luce della ben più nota disciplina costituzionale americana relativa al Quarto Emendamento, il quale crea un diritto ad essere liberi da «*unreasonable searches and seizures*», letteralmente quindi esso stabilisce la possibilità per gli individui di essere tutelati contro perquisizioni e sequestri irragionevoli. Nel momento in cui si deve determinare se c'è stata una violazione del Quarto Emendamento, i giudici americani non iniziano dalla disamina della condotta e se essa è stata o meno ragionevole, bensì essi esaminano in primo luogo se si può parlare di perquisizione e/o di sequestro. Analizzando perquisizione e sequestro distintamente, è possibile notare che nel primo caso, una perquisizione può violare una ragionevole aspettativa di privacy in un luogo o in riferimento ad una cosa, specificando inoltre che, al fine di avere tale

[331] F. ABRUZZO, *Intercettazioni. La normativa negli altri Paesi (Francia, GB, Germania e USA)*, in Internet al sito http://www.francoabruzzo.it/document.asp?DID=5269; M. TORTORELLA, *Intercettazioni: come funziona negli altri Paesi*, in Internet al sito http://www.panorama.it/news/in-giustizia/intercettazioni-come-funziona-negli-altri-paesi/.

aspettativa, un individuo deve essere portato a credere che una determinata area o un determinato oggetto è privato ed anche la società deve aver accettato tale credenza, in altre parole essa deve essere supportata dagli usi comuni[332]. Per quanto riguarda invece il sequestro delle proprietà di qualcuno, esso avviene, secondo la giurisprudenza americana[333], quando sia posta in essere un'interferenza effettiva negli interessi possessori dell'individuo su quella determinata proprietà. Infine, per poter essere «ragionevole», la perquisizione o il sequestro devono essere condotti dagli ufficiali di polizia attenendosi al mandato ovvero attenendosi ad una possibile eccezione ai requisiti del mandato stesso. Nell'ottica sopra delineata, lo strumento del captatore informatico assume un ruolo chiave all'interno della normativa americana, in particolar modo si è analizzata la possibilità che esso possa violare il dettato del Quarto Emendamento ed essere, di conseguenza, vietato all'interno dell'ordinamento americano. Per poter capire quindi in che modo viene disciplinato lo strumento in esame, l'iter logico impone di esaminare i due diversi concetti di *search* e *seizure*, per poi stabilire in quali modi il virus *trojan* possa essere legittimamente utilizzato[334].

Per quanto riguarda il concetto di *search*, esso costituisce un'attività di perquisizione all'interno del computer di un soggetto attraverso l'utilizzo del virus *trojan* (o di qualsivoglia altro *malware*), nel momento in cui tale soggetto abbia la ragionevole aspettativa della *privacy* relativamente ai contenuti dell'*hard-disk* del computer. La giurisprudenza americana ha infatti equiparato, in via analogica, l'*hard-disk* di un computer ad una sorta di contenitore al quale, in assenza di ulteriori circostanze di bilanciamento, va assicurata la stessa protezione che il Quarto Emendamento assicura ai contenitori chiusi o a qualsiasi altro effetto

[332] Cfr. *Katz v. United States*, 389 U.S. 347, (1967).
[333] Cfr. *Soldal v. Cook Cnty*., 506 U.S. 56, 61 (1992).
[334] S. W. BRENNER, *Fourth amendment future: remote computer searches and the use of virtual force*, in *Mississippi Law Journal*, vol. 81:5:2012.

personale chiuso di un individuo[335]. Un altro aspetto chiave è relativo alla modalità di esecuzione della perquisizione, in quanto tradizionalmente, nel momento in cui essa viene svolta in un computer posizionato in un ufficio o in un'abitazione privata, essa richiederebbe due passaggi: l'ingresso all'interno del luogo fisico dove il computer è ubicato e, in secondo luogo, l'accesso al computer stesso, ognuno dei quali deve essere ragionevole secondo il dettato del Quarto Emendamento. Inoltre, questi due "tipi" di accessi devono essere supportati, in modo da risultare legittimi, da un mandato oppure da un'eccezione applicabile ai requisiti del mandato stesso. Tuttavia, nelle perquisizioni da remoto poste in essere per mezzo del captatore informatico, l'unico accesso richiesto agli ufficiali di polizia è quello al computer del soggetto indagato e non anche al luogo dove il computer è fisicamente posto. In questo modo, si potrebbe quindi configurare la possibilità per gli organi investigativi di non necessitare di un mandato per effettuare tale perquisizione poiché non è previsto un accesso fisico al luogo dove il computer è situato[336]. In aggiunta a questo, i computer differiscono dai normali contenitori in quanto essi sono connessi ad Internet attraverso un *network*, rendendo di fatto accessibile agli investigatori tali dispositivi in quanto essi potrebbero semplicemente sfruttare il fatto che essi siano connessi *on-line*, rendendo non necessario qualsiasi tipo di ingresso meramente fisico all'interno del locale dove i dispositivi si trovano. A tal proposito, le corti americane hanno ritenuto che chi utilizza *software* di *file-sharing*, ossia rende disponibili i contenuti del proprio dispositivo *on-line*, non ha diritto ad una aspettativa di *privacy* relativamente ai *file* destinatari dello *sharing*, in quanto non è uso comune credere che tale aspettativa sia oggettivamente ragionevole[337]. Tramite quanto specificato riguardo all'attività di *search* così come definita e disciplinata dal Quarto Emendamento, è possibile desumere che l'utilizzo

[335] Cfr. *United States v. Barth*, 26 F. Supp. 2d 929, 9367-37 (W.D. Tex. 1998).
[336] Cfr. *United States v. Martinez-Fuerte*, 428 U.S. 543, 561 (1976).
[337] Cfr. *United States v. Ganoe*, 538 F. 3d 1117, 1127 (9th Cir. 2008).

legittimo del virus *trojan* per ottenere dati contenuti sul computer di un soggetto sottoposto ad indagini, vada ad inserirsi all'interno delle perquisizioni di cui alla norma in esame, rendendo quindi necessaria la presenza di un mandato oppure di un'applicabile eccezione ai requisiti del mandato.

In merito al concetto di *seizure* invece, il sequestro di una proprietà altrui avviene nel momento in cui le condotte degli organi di polizia interferiscono significativamente con gli interessi del proprietario sul possesso e sull'utilizzo di quella determinata proprietà. In quest'ambito si potrebbe quindi collocare il virus *trojan* in funzione di "copiatore", ossia di estrapolatore di dati da un dispositivo tramite *download*. Nei casi di sequestri tradizionali di una proprietà fisica, gli organi di polizia non permettono al proprietario di accedere a detta proprietà per un periodo di tempo limitato (c.d *temporary detention*) oppure in modo permanente. In entrambi i casi comunque, risulta esserci un vincolo di indisponibilità sulla proprietà e quindi un'effettiva interferenza così come richiesto dalla normativa statunitense mentre, nel momento in cui si prende in considerazione l'attività di "copiatura" dei *file* contenuti in un dato dispositivo, essa non rappresenta assolutamente alcuna interferenza nel possesso e nell'utilizzo di quei dati da parte del proprietario[338]. Nonostante ciò, la giurisprudenza americana ha affermato che, nonostante tale attività di copia non rappresenti una deprivazione fondamentale del diritto del proprietario all'utilizzo dei suoi dati, esso ne riceve comunque una interferenza significativa[339].

Per questi due motivi sopra analizzati, il mandato che autorizza l'utilizzo del virus *trojan* deve essere supportato dalla probabile eventualità ovvero da fatti e circostanze sufficienti a far ritenere ad un uomo ragionevole che

[338] S. W. BRENNER, *Copying as Search and Seizure*, in Internet al sito http://cyb3rcrim3.blogspot.it/2009/10/copying-as-search-and-seizure.html.
[339] Cfr. *State v. Schwartz*, 21 P. 3d 1128, 1131, 1135 (Or. Ct. App. 2001).

possibili evidenze probatorie saranno ritrovare nel computer che dovrà essere sottoposto a perquisizione e/o sequestro. A questo proposito, si deve segnalare che la polizia americana si può servire, in modo da stabilire il nesso della probabile eventualità, di informazioni confidenziali o anche di informazioni ottenute da altre fonti giudicate attendibili[340]. Il mandato deve inoltre descrivere con particolare eloquenza il posto da perquisire e le cose da sequestrare, intendendo per il primo (il posto) il computer del soggetto sottoposto ad indagini mentre, per le cose da cercare, esse consistono nei dati informatici. In merito a questo secondo aspetto, il mandato dovrebbe quindi specificare con particolare chiarezza i dati da copiare e sequestrare, tuttavia, essendo difficile stabilire a priori quali *file* gli organi investigativi dovranno copiare, si ritiene plausibile dover specificare nel mandato solo il tipo di dati che gli organi di polizia sono autorizzati a cercare ed acquisire, ad esempio si potrebbe specificare che gli agenti sono autorizzati a copiare solo prove inerenti alla pedopornografia o ancora prove attinenti alla spaccio di sostanze stupefacenti e via discorrendo[341]. Per quanto riguarda invece l'esecuzione del mandato, sembra scontato che per via dell'attività posta in essere tramite virus *trojan* da remoto, gli ufficiali di polizia non si presenteranno alla porta del soggetto indagato bussando e dichiarando le proprie intenzioni, nonostante questo sia un requisito stabilito dal Quarto Emendamento e dalla Suprema Corte degli Stati Uniti stessa[342]. Inoltre, sempre in tema di esecuzione del mandato, l'emendamento sopra citato non specifica il periodo di tempo entro il quale il mandato deve essere eseguito, tuttavia esso è disciplinato a livello federale tramite statuti o regolamenti delle corti. In particolare, secondo la *Rule 41 of the Federal Rules of Criminal Procedure*, i mandati che autorizzano la copia di

[340] Cfr. *United States v. Gitarts*, 341 F. App'x 935 (4th Cir. 2009).
[341] Cfr. *United States v. Welch* 291 F. App'x 193, 205 (10th Cir. 2008); inoltre, *United States v. Stabile*, 633 F. 3d 219, 237-39 (3d Cir. 2011).
[342] Cfr. *Wilson v. Arkansas*, 514 U.S. 927, 930 (1995).

informazioni immagazzinate elettronicamente sono eseguiti solamente nel momento in cui le informazioni sono effettivamente copiate, assumendo quindi che l'esecuzione del mandato sia un evento singolo ed unitario. Tuttavia si pone il problema relativo alla possibilità per i virus *trojan* di rimanere "dormienti" all'interno del dispositivo infettato oppure di "lavorare" autonomamente senza nessun *input* esterno da parte del soggetto controllore del virus, realizzando di fatto un'intercettazione *ubiquitous* e sempre attiva[343]. Per evitare tale situazione, gli statuti e i regolamenti delle corti potrebbero ovvero dovrebbero prevedere che il virus *trojan* venga eliminato dal dispositivo bersaglio una volta che l'attività di perquisizione o di sequestro autorizzata sia stata conclusa, oppure ancora prevedere che gli ufficiali di polizia disattivino il programma in modo da evitare che esso continui le attività di cui sopra sul computer infettato. Nonostante tutte queste accortezze tuttavia, lo scandalo più grande relativo all'utilizzo di tali *software* per scopi non esattamente legali ha colpito proprio gli Stati Uniti, evidenziando quindi ulteriori criticità sulla materia in esame.

Lo scandalo a cui si fa riferimento è quello denominato *Datagate*, originato dalle rivelazioni di un ex-dipendente della CIA, Edward Snowden, il quale iniziò, nel 2013, a collaborare con alcuni giornalisti britannici e statunitensi fornendo loro documenti relativi ad un programma di sorveglianza di massa, chiamato *PRISM*. L'operatività di tale programma era assicurata dalle previsioni normative previste dalla sezione 702 del *Foreign Inteligence Surveillance Act* (FISA), emanato nel 1978 e modificato dopo gli accadimenti dell'11 settembre 2001 da altri provvedimenti normativi, come ad esempio lo *USA Patriot Act*. Detta previsione normativa regola le modalità e le procedure per operazioni di sorveglianza elettronica e fisica,

[343] W. ABEL e B. SCHAFER, *The German "Federal Trojan" – Challenges Between law and Technology*, in Internet al sito http://www.teutas.it/societa-informazione/prova-elettronica/634-the-german-federal-trojan-challenges-.

nonché per la raccolta di informazioni provenienti da fonti di *intelligence* straniere. Bisogna sottolineare tuttavia che è la stessa sezione 702 a proibire alla NSA di intercettare i residenti sul suolo americano, tuttavia, poiché le intercettazioni "incidentali" di cittadini americani sono concesse dalla norma in esame, ciò ha permesso alla NSA di immagazzinare informazione anche relativamente ad individui residenti degli Stati Uniti e aventi contatti con persone residenti oltreoceano[344]. A tale provvedimento normativo è collegata una Corte federale fondata nel 1978, denominata Corte FISA, la quale ha il compito di autorizzare e sorvegliare sulle procedure di sorveglianza elettronica. Tale Corte è stata accusata di aver ampliato oltremodo i poteri conferiti alla NSA, l'agenzia di sicurezza nazionale americana (*National Security Agency*), in materia di sorveglianza di massa. Non è infatti un caso che il documento che ha dato il via allo scandalo *Datagate* sia stato proprio un mandato della sopra citata Corte tramite il quale si imponeva alla compagnia americana *Verizon* di fornire alla NSA un *dossier* quotidiano riguardante tutto il traffico telefonico gestito dalla compagnia[345]. La NSA aveva quindi messo in piedi, secondo le rivelazioni di Snowden, un programma di sorveglianza non solo nazionale ma addirittura su scala mondiale, basandosi sull'utilizzo di vari programmi in grado di intercettare il traffico Internet o telefonico di utenti di ogni parte del mondo, servendosi inoltre della collaborazione di altri cinque Paesi, il Regno Unito, l'Australia, il Canada e la Nuova Zelanda, i quali, assieme agli Stati Uniti, fanno parte del c.d. accordo UKUSA, accordo il cui fine è quello di raccogliere informazioni attraverso attività di *intelligence* relativa alla captazione e all'analisi di segnali emessi sia dalle macchine, come i segnali elettronici, sia dalle persone, come i

[344] G. GROSS, *The NSA's foreign surveillance: 5 things to know.*, in *PCWorld*, Aprile 2017, vol. 35, cap. 4, pp. 37-41.
[345] G. GREENWALD, *NSA collecting phone records of millions of Verizon customers daily*, in Internet al sito https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

segnali radio. Uno dei programmi maggiormente utilizzati da parte della NSA era *PRISM*[346], il quale era in grado di intercettare la maggior parte del traffico Internet mondiale e di immagazzinarlo per poterlo rendere disponibile alla NSA. I dati ottenibili comprendevano quindi email, *chat*, *chat* vocali nonché *videochat*, video, foto, conversazioni avvenute tramite tecnologia *VoIP* (ad esempio tramite il programma *Skype*), trasferimento di qualsiasi tipo di *file*, notifiche di accesso e tutti i dettagli relativi ai *social* frequentati dagli utenti intercettati. Il tutto avveniva con la collaborazione dei maggiori *service provider*, aziende quindi del calibro di *Google*, *Facebook*, *Microsoft*, *Skype*, *Apple*, *Yahoo*, *AOL* e ad altre. A tale scandalo si sono susseguite reazioni di sdegno da parte degli interessati dalle intercettazioni, in particolar modo gli enti governativi, ma la NSA ha sempre difeso, per tramite del suo capo Keith Alexander, il suo operato, definendolo utile in quanto avrebbe permesso di sventare almeno 50 attentati terroristici aiutando addirittura a prevenire un altro 11 settembre sul territorio statunitense[347].

Per concludere, è utile far riferimento ad una sentenza emanata dal giudice federale Richard J. Leon[348], nel Distretto di Columbia. Leon definisce tale programma di sorveglianza come quasi "orwelliano" e pronuncia la prima sentenza contro l'Agenzia per la sicurezza nazionale

---

[346] B. GELLMAN e L. POITRAS, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, in Internet al sito https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.13c174ba2470.

[347] E. NAKASHIMA, *NSA chief defends collecting American's data*, in Internet al sito https://www.washingtonpost.com/world/national-security/nsa-chief-defends-collecting-americans-data/2013/09/25/5db2583c-25f1-11e3-b75d-5b7f66349852_story.html?utm_term=.8b60d80cad2a.

[348] M. VINCENZI, *Il giudice federale alla NSA: raccolta dati va fermata. "E' contro la Costituzione".*, in Internet al sito http://www.repubblica.it/esteri/2013/12/16/news/il_giudice_federale_alla_nsa_raccolta_dati_va_fermata_e_contro_la_costituzione-73788260/.

statunitense, affermando, nelle 68 pagine della sentenza in esame, «non riesco ad immaginare un'invasione più indiscriminata ed arbitraria di quanto è avvenuto sino ad ora. Raccogliere e archiviare milioni di dati riguardanti praticamente tutti i cittadini è una palese violazione della nostra Costituzione», specificando inoltre che il motivo fondante della difesa, ossia la necessità di tale azione a difesa della sicurezza nazionale, non risulta verificato in quanto non sussistono prove evidenti che tale attività governativa abbia effettivamente sventato minacce alla sicurezza nazionale[349].

Lo scandalo *Datagate* ha quindi evidenziato le criticità relative all'utilizzo di tali *software* in modi illegittimi e, in alcuni casi, illeciti. Tali criticità sono state analizzate, nel corso di questa trattazione, anche in merito alla disciplina applicabile a livello italiano, evidenziando numerosi elementi di similitudine fra le lacune della normativa italiana e quella estera, alle quali sembrano mancare quelle garanzie fondamentali volte a tutelare gli interessi, molto spessi garantiti costituzionalmente, degli individui, spesso sacrificati sull'altare della repressione dell'azione criminale o, nei casi più gravi, per interessi puramente politici o governativi che nulla hanno a che vedere con le minacce terroristiche o la sicurezza nazionale e che fungono quindi da "parafulmine" per utilizzi illeciti dei virus *trojan*.

[349] Per contro, si può riscontrare una decisione del giudice William Pauley, della Corte distrettuale di Manhattan, con la quale si giustifica invece tale attività di sorveglianza, arrivando a definire il programma *PRISM* come un «valido strumento nella lotta al terrorismo che funziona solamente nel momento in cui raccoglie e conserva tutto». La sentenza è riportata, in lingua inglese, in Internet al sito https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf.

# Bibliografia


ABBAGNALE M. T., *In tema di captatore informatico*, in *Arch. pen.*, n. 2, 2016, pp. 2 e ss.

ABEL W. e SCHAFER B., *The German "Federal Trojan" – Challenges Between law and Technology*, in Internet al sito http://www.teutas.it/societa-informazione/prova-elettronica/634-the-german-federal-trojan-challenges-.

ABRUZZO F., *Intercettazioni. La normativa negli altri Paesi (Francia, GB, Germania e USA)*, in Internet al sito http://www.francoabruzzo.it/document.asp?DID=5269.

AMATO G., *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico"*, in *Guida al diritto*, n. 34-35, 13 agosto 2016, pp. 76 e ss.

AMODIO E., *Motivazione della sentenza penale*, in *Enc. dir.*, XXVII, pp. 199 e ss.

AMORTH A., *La costituzione italiana*, Giuffrè, Milano, 1948, p. 62.

ANGELONI C., *Le intercettazioni telefoniche "in remotizzato": gli aspetti esecutivi al vaglio delle Sezioni unite*, in *Giur. it.*, Ipsoa, Milano, 2009, n. 2, p. 462.

ATERNO S., *Il "captatore informatico": uno strumento d'indagine tra esigenze investigative e garanzie difensive*, in Internet al sito https://www.slideshare.net/jbluesj/il-captatore-informaticouno-strumento-dindagine-tra-esigenze-investigative-e-garanzie-difensive.

ATERNO S., *Il Trojan dalla A alla Z. Esigenze investigative e limitazioni della privacy: un bilanciamento necessario*, in Internet al sito http://www.dirittopenaleinformatica.it/wp-content/uploads/2017/02/ATERNO_Il-TROJAN-dalla-A-alla-Z.pdf.

ATERNO S., *La prova informatica nella giurisprudenza*, Corso di formazione, Università di Catania, 3 giugno 2013, in Internet al sito http://www.dmi.unict.it/~battiato/CF1213/Aterno_Catania_prova%20digitale_%202013.pdf.

BALDUCCI P., *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria,* in *Studi di diritto processuale* raccolti da Giovanni Conso, Giuffrè Editore, 2002, pp. 9 e ss.

BALSAMO A., *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea. The "on line surveillance" between Italian criminal trial and European Court of Human Rights*, in *Cass. pen.,* fasc. 5, 2016, p. 2274b.

BARGI A. e FURFARO S., *Le intercettazioni di conversazioni e* comunicazioni, in *La prova penale*, di A. Gaito, in *Trattati brevi*, vol. II, *Le dinamiche probatorie e gli strumenti per l'accertamento giudiziale*, UTET GIURIDICA, 2010, pp. 109 e ss.

BARILE P. e CHELI E., *Corrispondenza (Libertà di)*, in *Enciclopedia del diritto*, vol. X, Giuffrè, Milano, 1962, p. 749.

BARTOLE S., BIN R., CRISAFULLI V. e PALADIN L., *Commentario breve alla Costituzione*, in *Breviaria Iuris*, di G. Cian e A. Trabucchi, seconda edizione, CEDAM, 2008, p. 124.

BENE T., *Il pedinamento elettronico: truismi e problemi spinosi*, in *Le indagini atipiche*, op. cit., pp. 350 e ss.

BERGHELLA F. e BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, p. 2329.

BERNASCONI A., voce *Criminalità organizzata (diritto processuale penale)*, in *Enc. dir.*, Agg. IV, Milano, 2000, pp. 501 e ss.

BERTUGLIA E. e BRUNO P., *Le intercettazioni nel nuovo codice di procedura penale*, in *Riv. guardia di fin.*, 1990, p. 1330.

BORGOBELLO M., *L'eccezione di inutilizzabilità delle intercettazioni*, Giappichelli Editore, Torino, 2013, p. 54.

BOSCO F. e VACIAGO C., *La nuova cyber minaccia per la privacy: tutto ciò che sappiamo sui captatori informatici*, in Internet al sito https://www.agendadigitale.eu/infrastrutture/la-nuova-cyber-arma-di-distruzione-di-massa-per-la-nostra-privacy-i-captatori-informatici/.

BRENNER S. W., *Copying as Search and Seizure*, in Internet al sito http://cyb3rcrim3.blogspot.it/2009/10/copying-as-search-and-seizure.html.

BRENNER S. W., *Fourth amendment future: remote computer searches and the use of virtual force*, in *Mississippi Law Journal*, vol. 81:5:2012.

BRUNO P., *Intercettazioni di comunicazioni o conversazioni*, in *Dig. Disc. Pen.,* 1993, vol. VII, pp. 178 e ss.

BUONOMO G., *Metodologia e disciplina delle indagini informatiche*, in R. Borruso, G. Buonomo, G. Corasaniti e G. D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pp. 135 e ss.

CAJANI F., *L'odissea del captatore informatico,* in *Cass. pen., 2016,* n. 4143.

CAMON A., *Cavalli di troia in Cassazione*, nota a sent. Cass. sez. un., 28 aprile 2016, Scurato, n. 26889, in *Arch. nuova proc. pen.,* 2017, pp. 76 e ss.

CAMON A., *L'acquisizione dei dati sul traffico telefonico*, in *Dir. pen. proc.*, 2005, p. 634.

CAMON A., *Le intercettazioni nel processo penale*, Milano, 1996, p. 11.

CAMPILONGO V., *L'obbligo di motivazione in tema di intercettazioni di conversazioni o comunicazioni: questioni interpretative e problemi applicativi,* in *CP* 2005, p. 3196.

CANTONE R., *L'elaborazione giurisprudenziale sull'art. 270 c.p.p.; brevi riflessioni*, in *Cass. pen.*, 2000, p. 2046.

CAPRIOLI F., *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, *Riv. it. dir. e proc. pen.*, 1991, p. 155.

CARETTI P. e DE SIERVO U., *Istituzioni di diritto pubblico*, VIII ed., Giappichelli, Torino, 2006, p. 602.

CARLI L., *Le indagini preliminari nel sistema processuale penale*, Giuffrè, Milano, 2005, p. 333.

CHELO MANCHIA A., *Localizzazione tramite GPS: quali garanzie?*, in *Riv. giur. Sarda*, 2006, p. 432.

CHIRIZZI L., *Computer Forensic. Il reperimento della fonte di prova informatica*, Laurus Robuffo, Roma, 2006.

CISTERNA A., *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni Unite*, in *Arch. pen.*, 2016, II, p. 331.

*Codice penale e di procedura: la riforma pubblicata in Gazzetta*, in Internet al sito http://www.altalex.com/documents/leggi/2017/03/15/riforma-codice-penale-e-procedura.

COLAIOCCO S., *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen.*, n. 1, 2014, pp. 6 e ss.

CONSO G., *La criminalità organizzata nel linguaggio legislativo*, in *Giust. pen.,* 1992, vol. III, pp. 385 e ss.

CONTI C. e TORRE M., *Spionaggio informatico nell'ambito dei social network,* in *Le indagini atipiche*, in collana *Leggi penali tra regole e prassi*, diretta da A. Scafati, Giappichelli Editore, 2014, p. 415.

CONTI C., *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.,* 2011, pp. 3653 e ss.

CONTINI A., *ABC della sicurezza: Zero Day*, in Internet al sito http://www.techeconomy.it/2015/11/17/abc-sicurezza-zero-day/.

CORASANITI G., *Autorizzazione alla ratifica*, in *Cybercrime, responsabilità degli enti, prova digitale*, *Commento alla legge 18 marzo 2008, n. 48*, di G. Corasaniti e G. C. Lucente, CEDAM, Milano, 2009, pp. 8 e ss.

CORASANITI G., *Le intercettazioni "ubiquitarie" e digitali tra garanzie di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in *Il diritto dell'informazione e dell'informatica*, 2016, p. 88.

CORDERO F., *Codice di procedura penale commentato*, Torino, 1990, p. 302.

CORDERO F., *Tre studi sulle prove penali,* Giuffrè, 1963, p. 164.

CORRIAS LUCENTE G., *La nuova frontiera delle intercettazioni. I Troyan Horse e le libertà fondamentali. L'appello delle Sezioni Unite*, in *Law and Media Working Paper Series*, n.10/2016, pp. 3 e ss.

CORTE G. L., *Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata*, in *Giur. pen. web*, 2017, 6, pp. 10 e ss.

CRISTIANI A., *Profili evolutivi*, in *Studi Vassalli*, II, pp. 434 e ss.

CUOMO L. e RAZZANTE R., *La nuova disciplina dei reati informatici*, Giappichelli Editore, 2009, p. 85.

DALIA A. e FERRAIOLI M., *Manuale di diritto processuale penale,* Padova, 2003, p. 511.

DE FRANCHIS F., *Dizionario Giuridico*, Giuffrè, Milano, 1984.

DE LEO F., *Pubblico Ministero*, in *Codice di procedura penale. Rassegna di giurisprudenza e dottrina*, di G. Lattanzi e E. Lupo, vol. I, Giuffrè, 2008, p. 493.

DE NOZZA M. S., *E-mail parcheggiate all'estero, similitudine con il cloud computing: La parola della Cassazione*, in *Sic. e giust.*, 2016, 4, p. 51.

DE SANTIS A., *I malware*, in Internet al sito http://www.disrv.unisa.it/~ads/ads/Sicurezza_su_Reti_files/Lez01_I%20Malware.pdf.

DELL'ANDRO R., *Colloqui registrati ad uso probatorio*, in *R. it. d. proc. pen.* 84, pp. 118 e ss.

DI CAMILLO F., *L'ambito di operatività della nozione normativa di "criminalità organizzata"*, in Internet al sito http://www.altalex.com/documents/news/2005/12/12/l-ambito-di-operativita-della-nozione-normativa-di-criminalita-organizzata.

DI MARTINO C. e PROCACCIANTI T., *Le intercettazioni telefoniche*, in *Enciclopedia*, di P. Cendon, CEDAM, 2001, pp. 38 e ss.

DI RESTA F., *Il nuovo regolamento generale sulla protezione dei dati personali: un continente una legge, ma occorre essere preparati*, in Internet al sito http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-04-15/il-nuovo-regolamento-generale-protezione-dati-personali-continente-legge-ma-occorre-essere-preparati-171042.php.

DI STASI G., *La tutela costituzionale della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione,* in *Riv. amm. R.I.,* 1994, p. 1129.

DI STASIO C., *La lotta multilivello al terrorismo internazionale: garanzia di sicurezza versus tutela dei diritti fondamentali*, Giuffrè, 2010, pp. 233 e ss.

DI STEFANO M., *Il captatore informatico "Trojan": stato dell'arte e profili giuridici,* in Internet al sito

https://www.ictsecuritymagazine.com/articoli/captatore-informatico-trojan-dellarte-profili-giuridici/.

DINACCI F. R., *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Giuffrè, Milano, 2008, p. 37.

FELICIONI P., *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziali e prospettive di riforma*, in *Proc. pen. e giust.*, n. 5, 2016, p. 124.

FERRAIOLI M., *La funzione di «controllo» del giudice per le indagini preliminari*, in *ASalerno*, 1993, p. 88.

FERRUA P., *Studi sul processo penale*, vol. III, Torino, 1997, p. 121.

FIANDACA G., *Criminalità organizzata e controllo penale*, in *Indice pen.,* 1991, pp. 5 e ss.

FILIPPI L., *Due temi da distinguere nel dibattito sulle intercettazioni*, in *DPP*, 1993, p. 103.

FILIPPI L., *Il captatore informatico: l'intercettazione ubicumque al vaglio delle Sezioni Unite*, in *Arch. pen.*, 2016, n. 1.

FILIPPI L., *Il GPS è una prova incostituzionale. Domanda provocatoria ma non troppo dopo la sentenza Jones della Corte Suprema USA*, in *Arch. pen.*, 2012, p. 309.

FILIPPI L., *L'intercettazione di comunicazioni*, Giuffrè, Milano, 1997, p. 81.

FILIPPI L., *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen.*, 2016, II, p. 348.

FLOR R., *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "Data Retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2014, 2, pp. 178 e ss.

FLOR R., *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del* Bundesverfassungsericht *e della* Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e data retention*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti processuali*, di L. Picotti e F. Ruggieri, Giappichelli editore, 2011, pp. 32 e ss.

FLORA M., *Hacking Team: di cosa dovete DAVVERO avere paura*, in Internet al sito http://mgpf.it/2015/07/09/hackingteam-di-cosa-dovete-davvero-aver-paura.html.

FREDIANI C., *Ddl Orlando: più facile e frequente l'utilizzo di trojan*, in Internet al sito http://www.lastampa.it/2017/05/22/tecnologia/news/ddl-orlando-pi-facile-e-frequente-lutilizzo-di-trojan-poBLFWMRJ7IBnbUg0XtlzJ/pagina.html.

FREDIANI C., *Intercettazioni col trojan, ecco la proposta di legge*, in Internet al sito http://www.lastampa.it/2017/01/31/italia/cronache/intercettazioni-col-trojan-ecco-la-proposta-di-legge-MP8BJ2PB0jCwMt84ofRSlM/pagina.html.

FUMU G., *Intercettazioni, archiviazione e distruzione della documentazione tra norma e prassi e giurisprudenza costituzionale*, in *LP* 1995, p. 491.

FUMU G., *Sub. art. 266-bis*, in *Commentario Chiavario*, ed. III agg., 1997, p. 131.

G. BORRELLI, *Dei delitti in particolare*, in *Codice penale. Rassegna di giurisprudenza e dottrina*, di G. Lattanzi e E. Lupo, vol. 9, Giuffrè, 2008, pp. 137-138.

GAITO A. e FURFARO S., *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, II, p. 309.

GAITO A., *L'integrazione successiva dei decreti di intercettazioni telefoniche non motivati*, in *Dir. pen. proc.*, 2004, p. 929.

GALANTINI N., voce *Inutilizzabilità (dir. proc. pen.)* in *Enc. Dir. Agg. I*, Milano, 1997, p. 699.

GALBIATI R., *Autorità garanti – Profili processuali*, in *Foro it.,* 1998, IV, c. 43.

GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, pp. 46 e ss.

GARUTI G., *Osservatorio Corte di Cassazione – Sezioni Unite*, in *Dir. pen. e proc.*, n. 8, 2016, p. 1042.

GATTI G., *Il controllo del gip*, in *Quad. C.s.m.*, 1995, n. 81, pp. 219 e ss. e p. 232.

GELLMAN B. e POITRAS L., *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, in Internet al sito https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.13c174ba2470.

GENTILE D., *Tracking satellitare mediante gps: attività tipica di indagine o intercettazione di dati?*, in *Dir. pen. proc.*, 2010, p. 12.

GHIRARDINI A. e FAGGIOLI G., *Computer forensics*, Apogeo, Milano, 2007, p. 45.

GIALUZ M., CABIALE A. e TORRE J. D., *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *Dir. pen. cont.*, pp. 29 e ss., disponibile in Internet al sito http://www.penalecontemporaneo.it/upload/GIALUZCABIALEDELLATORRE_2017a.pdf.

GIANNANTONIO E., *L'oggetto giuridico dei reati informatici*, in *Cass. pen.*, 2001, p. 2244.

GIARDA A., *Sub artt. 266-267*, in *Codice di procedura penale. Commentario* a cura di A. Giarda, vol. II, IPSOA, Milano, pp. 11-19.

GIGLIO V., *I virus informatici per scopi intercettivi nei procedimenti di criminalità organizzata: mezzi di cura o agenti patogeni?*, in Internet al sito https://www.filodiritto.com/.

GIORDANO L. e VENEGONI A., *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in Internet al sito http://www.penalecontemporaneo.it/d/4703-la-corte-costituzionale-tedesca-sulle-misure-di-sorveglianza-occulta-e-sulla-captazione-di-conversa.

GIORDANO L., *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in Internet al sito http://www.penalecontemporaneo.it/d/5267-dopo-le-sezioni-unite-sul-captatore-informatico-avanzano-nuove-questioni-ritorna-il-tema-della-funz.

GIORDANO L., *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in Internet al sito http://www.penalecontemporaneo.it/upload/GIORDANO_2017a.pdf.

GOSSO P. G., Voce *Intercettazioni telefoniche*, in *Enciclopedia del diritto*, vol. XXI, 1971, pp. 890 e ss.

GREENWALD G., *NSA collecting phone records of millions of Verizon customers daily*, in Internet al sito https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

GREVI V., *Appunti in tema di intercettazioni telefoniche operate dalla polizia giudiziaria*, in *Riv. it. dir. e proc. pen.*, 1967, p. 733

GREVI V., *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1974, p. 341.

GREVI V., *Intercettazioni telefoniche e principi costituzionali*, in *Riv. it. dir. e proc. pen.*, 1971, p. 1079.

GREVI V., *Prove,* in G. Conso e V. Grevi, *Profili del nuovo codice di procedura penale,* Padova, 1990.

GREVI V., *Sul necessario collegamento tra utenze telefoniche e indagini in corso nel decreto autorizzativo delle intercettazioni*, in *Cass. pen.* 2009, 9, p. 3344.

GRIFANTINI F. M., *Inutilizzabilità*, in *Dig. pen.*, vol. VIII, Torino, 1993, p. 249.

GROSS G., *The NSA's foreign surveillance: 5 things to know.*, in *PCWorld*, Aprile 2017, vol. 35, cap. 4, pp. 37-41.

IASELLI M., *Nuove tecnologie per nuove tecniche investigative, ma a rischio privacy*. *Dalle indagini sul caso D'Antona un esempio da seguire*, in *DGius,* 2003, 43, pp. 91 e ss.

IASELLI M., *Protezione dei dati personali: il nuovo Regolamento Europeo in Gazzetta Ufficiale UE*, in Internet al sito http://www.altalex.com/documents/news/2015/12/23/accordo-raggiunto-sul-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.

ILLUMINATI G., *L'inutilizzabilità della prova nel processo penale*, in *Riv. it. dir. proc. pen.*, 2010, p. 521.

ILLUMINATI G., *La disciplina processuale delle intercettazioni*, Giuffrè, 1983, pp. 37 e ss.

KALB L., *Intervento*, in *Le intercettazioni di conversazioni e comunicazioni – Meccanismi operativi e regole procedurali*, Giuffrè, Milano, 2009, p. 305.

KEANE WOODS A., *Dark Clouds Over the Internet*, in Internet al sito https://www.nytimes.com/2015/12/01/opinion/dark-clouds-over-the-internet.html?_r=0.

KUSHNER D., *La storia di Hacking Team, dall'inizio*, in Internet al sito http://www.ilpost.it/2016/05/15/hacking-team/.

LA CORTE G., *Il trojan: le intercettazioni nell'era digitale a contrasto della criminalità organizzata*, in *Giur. pen. web*, 2017, 6.

LASAGNI G., *L'uso di captatori informatici (trojans) nelle intercettazioni fra presenti*, in Internet al sito http://www.penalecontemporaneo.it/.

LEO G., *La nozione processuale di criminalità organizzata*, in *Corr. mer.*, 2005, p. 830.

LIGUORI L., *E' in vigore il nuovo regolamento generale sulla protezione dei dati*, in Internet al sito https://www.filodiritto.com/articoli/2016/06/-in-vigore-il-nuovo-regolamento-generale-sulla-protezione-dei-dati.html.

MALENKOVICH S., *Che cosa sono i rootkit?*, in Internet al sito https://blog.kaspersky.it/che-cosa-sono-i-rootkit/645/.

MANCUSO E. M., *L'acquisizione di contenuti e-mail*, in *Le indagini atipiche*, op. cit., p. 70.

MANGANELLI A. e GABRIELLI F., in *Investigare – Manuale pratico delle tecnologie di indagine*, Cedam, Padova, 2007, pp. 125-126.

MARALFA G., *Le intercettazioni*, in *Dir. Pen.,* Editore G. Pirapini, 2004, p. 12.

MARCOLINI S., *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, di F. Ruggeri e L. Picotti, Giappichelli Editore, Torino, 2011, pp. 339 e ss.

MARINELLI C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007, p. 4.

MATTIUCCI M. e DELFINIS G., *Forensic Computing,* in *Rassegna dell'Arma dei Carabinieri*, Anno LIV, aprile/giugno 2006, n. 2-2006, pp. 51 e ss.

MEZZALAMA M., LIOY A., METWALLEY H., *Anatomia del malware*, in *Mondo digitale n. 47*, settembre 2013.

MONTAGNA A., *Intercettazioni ambientali tramite virus negli smartphone: la decisione delle Sezioni Unite*, in *Quotidiano Giuridico*, 4 luglio 2016, pp. 3-4.

MONTEVERDE L., *Le nuove "frontiere" delle intercettazioni*, in *Arch. pen.,* 3, 2014.

MONTEVERDE L., *Le nuove "frontiere" delle intercettazioni*, in *Arch. pen.*, 2014, n. 3, p. 11.

MORALES GRACIA O., *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul Cyber-Crime*, in *Il diritto penale dell'informatica*, di L. Picotti, Padova, 2000, p. 123.

MORTATI C., *Istituzioni di diritto pubblico*, vol. 2, CEDAM, 1976, p. 1062.

NAKASHIMA E., *NSA chief defends collecting American's data*, in Internet al sito https://www.washingtonpost.com/world/national-security/nsa-chief-defends-collecting-americans-data/2013/09/25/5db2583c-25f1-11e3-b75d-5b7f66349852_story.html?utm_term=.8b60d80cad2a.

NAPPI A., *Guida al codice di procedura penale*, Giuffrè, Milano, 1997, p. 154.

NAPPI A., *Sull'abuso delle intercettazioni*, in *Cass. pen.*, 2009, pp. 470-471.

NASI M., *Decreto antiterrorismo, bocciato il trojan di stato*, in Internet al sito https://www.ilsoftware.it/articoli.asp?tag=Decreto-antiterrorismo-bocciato-il-trojan-di-Stato_12033.

ORLANDI R., *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in Internet al sito http://www.archiviopenale.it/.

ORLANDI R., *Questioni in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 134.

PACE A., *Commento all'art. 15 Cost.*, in *Commentario della Costituzione*, di G. Branca, Zanichelli, Bologna, 1977, p. 107.

PALAZZO F., *La riforma penale alza il tiro? Considerazioni sul disegno di legge A. S. 2067 e connessi*, in *Dir. pen. cont.*, *Riv. trim.*, 2016, n.1, pp. 52 e ss.

PAOLONI A. e ZAVATTARO D., *Intercettazioni telefoniche ed ambientali. Metodi, limiti e sviluppi nella trascrizione e verbalizzazione*, Centro Scientifico Editore, 2007, pp. 84 e ss.

PARODI C., *Le Intercettazioni. Profili operative e giurisprudenziali,* in *Giurisprudenza Oggi*, di P. CENDON, Giappichelli Editore, 2002, pp. 11 e ss.

PARODI C., Procura della Repubblica di Torino, *La riforma "Orlando": la delega in tema di "captatori informatici"*, in Internet al sito http://www.magistraturaindipendente.it/la-riforma-orlando-la-delega-in-tema-di-captatori-informatici.htm.

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.

PERROTTA G., *Ratio Legis*, n. 4, Primiceri Editore, 2016, pp. 181 e ss.

PICOTTI V., *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen.*, 2016, II, p. 354.

PIO E., *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *Parola alla difesa*, 1, Pisa, 2016, p. 160.

PITONI A., *Hacking Team, revocata l'autorizzazione globale all'export del software spia: stop anche per l'Egitto dopo il caso Regeni,* in Internet al sito http://www.ilfattoquotidiano.it/2016/04/06/hacking-team-revocata-lautorizzazione-globale-allexport-del-software-spia-stop-anche-per-legitto-dopo-il-caso-regeni/2610721.

PORCU V., *"Vi spiego come ho attaccato l'Hacking Team"*, in Internet al sito http://www.repubblica.it/tecnologia/sicurezza/2016/04/20/news/hacking_team_attacco-138026549/.

RECCIA E., *L'aggravante ex art. 7 d.l. 152 del 13 maggio 1991: una sintesi di "inafferrabilità del penalmente rilevante"*, in *Dir. pen. cont.,* n. 2/2015, p. 251.

RINGOLD J. S. III, *Corporate Forensics Toolkit*, in Internet all'indirizzo http://mn-isfa.org/presentations/corporateforensicstoolkit.ppt.

RIVIEZZO C., *La trascrizione delle intercettazioni telefoniche*, in *GG* 1994, 20, p. 22.

ROMANO B. e TINEBRA G., *Il diritto penale della criminalità organizzata*, Giuffrè, Milano, 2013.

ROMANO S. e SORIO C., *L'utilizzo dei c.d. trojan horses nelle indagini penali e la tutela "progressiva" della libertà e segretezza delle comunicazioni*, in *Law and Media Working Paper Series*, 2016, n. 14.

ROSSI C., *Il rispetto della corrispondenza nella Convenzione europea dei diritti dell'uomo. Le intercettazioni nella legislazione italiana*, in *Riv. int. dir. uomo,* 1994, p. 67.

RUGGERI F., *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Giuffrè, Milano, 2001, pp. 111 e ss.

S. ZIRULIA, *Riforma Orlando: la "nuova" prescrizione e le altre modifiche al codice penale*, in Internet al sito http://www.penalecontemporaneo.it/d/5501-riforma-orlando-la-nuova-prescrizione-e-le-altre-modifiche-al-codice-penale.

SARZANA C. e IPPOLITO C., *Informatica e diritto penale*, Giuffrè, Milano, 1994, p. 224.

SAVIO E., *Remotizzazione dell'ascolto: dalla recente giurisprudenza al progetto Alfano*, in *Diritto penale e processo*, Ipsoa, Padova, 2010, n. 4, p. 494.

SCACCIANOCE C., *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui*, in *Le indagini atipiche*, op. cit., p. 41.

SCHIAFFINO M., *Virus, manipolazione e false prove: tutti i rischi dei Trojan usati dallo Stato*, in Internet al sito http://www.ilfattoquotidiano.it/2016/06/07/virus-manipolazione-e-false-prove-tutti-i-rischi-dei-trojan-usati-dallo-stato/2801363/.

SEGANTINI E., *Difesa di privacy e sicurezza alla rete serve una governance*, in Intenet al sito http://www.corriere.it/opinioni/15_dicembre_23/rassegniamoci-anche-internet-ha bisogno-regole-b1f03282-a93b-11e5-8f07 76e7bd2ba963.shtml.

SEGHETTI A. V., *Intercettazioni telefoniche illegittime per motivazione insufficiente e nullità della custodia cautelare*, *GI*, II, 1992, p. 133.

SEMINARA S., *La responsabilità penale degli operatori su Internet*, in *Il diritto dell'informazione e dell'informatica*, 1998, p. 745.

SENOR M. A., *DDL Orlando, ecco le conseguenze giudiziarie delle intercettazioni con trojan*, in Internet al sito https://www.agendadigitale.eu/documenti/ddl-orlando-ecco-le-conseguenze-giudiziarie-delle-intercettazioni-con-trojan/.

SENOR M., Centro Studi Processo Telematico, *Trojan di Stato: perché serve una base giuridica adeguata*, in Internet al sito https://www.agendadigitale.eu/documenti/trojan-di-stato-perche-serve-una-base-giuridica-adeguata/.

SGHERZA A., *Un virus per pc inchioda Bisignani. Lo stato diventa hacker a fin di bene*, in Internet al sito http://www.repubblica.it/politica/2011/06/22/news/mail_spia_hacker-18041273/.

SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in *Riv. trim. di dir. pen. dell'econ.*, 1997, p. 496.

SIGNORATO S., *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, pp. 580 e ss.

SINISCALCO M., *Domicilio (violazione di)*, in *Enc. dir.,* XIII, Milano, 1964, p. 871.

SPANGHER G., *DDL n. 2067: sulle proposte di modifica al codice di procedura penale*, in *Giur. pen. web*, 2017, 3, in Internet al sito http://www.giurisprudenzapenale.com/wp-content/uploads/2017/03/spangher_gp_2017_3.pdf.

SPANGHER G., *La disciplina italiana delle intercettazioni di comunicazioni o conversazioni*, *AP*, 1994, 3-15, 5.

SPATARO C., *Le intercettazioni telefoniche: problemi operativi e processuali*, in *Quaderni del c.s.m.* 1994, 69, p. 144.

STALLINGS W., *Sicurezza delle reti. Applicazioni e standard*, Pearson, 2007, p. 348.

STRAMAGLIA M., *Il pedinamento satellitare: ricerca ed uso di una prova atipica*, in *Dir. pen. proc.*, 2011, p. 213.

TAORMINA C., *Diritto processuale penale*, vol. I, Giappichelli Editore, Torino, 1995, p. 327.

TESTAGUZZA A., *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. e proc.*, 2015, p. 761.

TONELLOTTO M., *Evidenza informatica, computer forensics e best practices*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. VIII, n. 2, maggio-agosto 2014.

TONINI P., *Manuale di procedura penale*, Giuffrè, Padova, 2000, p. 368

TORRE M., *Mezzi di ricerca della prova informatica e garanzie difensive: dagli accertamenti investigativi al virus di Stato – 15 luglio 2015*, in *Le indagini atipiche – Perquisizioni on line e captatore informatico nel diritto vivente*, in Internet al sito http://www.fondazioneforensefirenze.it/uploads/fff/files/2015/2015.II/2015.07.15%20Mezzi%20ricerca%20prova%20informatica/Slides%20Dott_%20Marco%20Torre.pdf.

TORTORELLA M., *Intercettazioni: come funziona negli altri Paesi*, in Internet al sito http://www.panorama.it/news/in-giustizia/intercettazioni-come-funziona-negli-altri-paesi/.

TRAFICANTE F., *Regolamento UE Privacy: Data Security e Data Breach Notification*, in Internet al sito http://www.techeconomy.it/2016/03/03/regolamento-ue-privacy-parte-1-data-security-data-breach-notification/.

TROGU M., *Sorveglianza e "perquisizione" on-line su materiale informatico*, in *Le indagini atipiche*, op. cit., pp. 444 e ss.

TURCO E., *Nota a sent. Cass. sez. un., 26 giugno 2008, n. 36359*, in *For. it.*, Zanichelli, Bologna, 2009, n. 2, II, p. 80.

Ufficio del Massimario, Servizio Penale, *Orientamenti sulle linee interpretative della giurisprudenza e della dottrina in materia di intercettazioni*, Rel. n. 55/2005.

UGOCCIONI L., *Sub art. 11 L. 23/12/1993 N. 547 (Criminalità informatica), LP,* 1996, pp. 142 e ss.

VACIAGO G., *Digital Evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli Editore, Torino, 2012, pp. 12 e ss.

VELANI L. G., *Nuove tecnologie e prova penale: il sistema di individuazione satellitare G.P.S.*, in *Giur. It.*, 2003, pp. 2372 e ss.

VERDE G., *Le inchieste di Napoli e le intercettazioni "esplorative"*, in *Il Mattino*, in Internet al sito https://www.pressreader.com/italy/il-mattino-caserta/20170113/282643212244457.

VERGARA D., *Stuxnet: il virus che sconvolse il mondo*, in Internet al sito http://tech.everyeye.it/articoli/speciale-stuxnet-virus-che-sconvolse-mondo-30317.html.

VIGANO' F., *Oltre l'art. 416-bis: qualche riflessione sull'associazione con finalità di terrorismo*, in *Scenari di mafia. Orizzonte criminologico e innovazioni normative*, di G. Fiandaca e C. Visconti, Giappichelli Editore, Torino, 2010, p. 177.

VINCENZI M., *Il giudice federale alla NSA: raccolta dati va fermata. "E' contro la Costituzione".*, in Internet al sito http://www.repubblica.it/esteri/2013/12/16/news/il_giudice_federale_alla_nsa_raccolta_dati_va_fermata_e_contro_la_costituzione-73788260/.

ZACCHE' F., *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. e giust.*, 2013, p. 108.

ZICCARDI G., *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali,* vol. II, seconda edizione, Giuffrè Editore, Milano, 2013, p. 236.

ZICCARDI G., *La procedura di analisi della fonte di prova digitale*, in *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, di L. Luparia e G. Ziccardi, Giuffrè, 2007.

ZICCARDI G., *Parlamento europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Arch. pen.*, 2017, n. 1.

ZONARO M., *Il Trojan – Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in *Dibattiti/Focus – Parola alla difesa*, 2016, pp. 163 e ss.

# Elenco giurisprudenza citata

*Katz v. United States*, 389 U.S. 347, (1967).

C. cost., sent. n. 34 del 6 aprile 1973, in *Giur. cost.,* 1973, p. 330.

*United States v. Martinez-Fuerte*, 428 U.S. 543, 561 (1976).

C. eur., 6 settembre 1978, Klass e altri c. Germania, n. 5029/71, punto 41.

Cass., sez. V, 6 novembre 1978, Triberti, in *CP*, 1981, p. 510.

Cass. sez. I, 28 febbraio 1979, Martinet, *C.P.M.A.,* 1982, p. 598.

Cass., sez. VI, 19 febbraio 1981, Semitaio, in *CP*, 1982, p. 1529.

Cass., sez. II, 16 febbraio 1985, Barresi, in *Foro it.,* 1986, II, p. 670.

Cass. sez. V, 18 novembre 1985, Perini, in *Mass. giur. lav.,* 1986, p. 426.

Cass. sez. V, 3 aprile 1987, in *Foro it.,* 1988, c. 272.

Cass. sez. I, 11 dicembre 1989, Baglio, in *GP*, 1990, III, p. 583.

Cass. sez. I, 12 marzo 1990, Bicici, in *GP*, 1991, III, p. 424.

Cass. sez. VI, 20 febbraio 1991, Morabito, in *Giur. it.,* 1991, II, p. 466.

C. cost. n. 366/1991, in *Giust. pen.*, 1992, I, pp. 35 ss.

C. cost. 23 luglio 1991, n. 366.

Ass. Cassino, 27 gennaio 1992, in *Foro it.,* 1993, II, c. 570.

Cass. sez. I, 22 settembre 1992, Zazza, in *ANPP*, 1993, p. 333.

Cass. sez. I, 19 ottobre 1992, Liggieri, in *Cass. pen.,* 1995, p. 991.

*Soldal v. Cook Cnty*., 506 U.S. 56, 61 (1992).

C. cost., 19 gennaio 1993, n.10, *GiC*, 1993, n. 52.

C. cost., 11 marzo 1993, n. 81.

C. cost., 24 febbraio 1994, n. 63.

Cass. sez. I, 23 marzo 1994, Pulito, in *Giust. pen.,* 1995, III, c. 217.

Cass. sez. I, 12 dicembre 1994, Manzi, *ANPP*, 1995, p. 710.

Cass. sez. I, 16 gennaio 1995, Catti ed altri, *GP*, 1996, III, 226.

Cass. sez. VI, 7 aprile 1995, Celone, in *ANPP*, 1996, p. 156.

*Wilson v. Arkansas*, 514 U.S. 927, 930 (1995).

Cass. sez. VI, 8 giugno 1995, in *Arch. n. proc. pen.,* 1995, p. 863.

Cass. sez. V, 11 luglio 1995, Coluccia e altri, n. 8925, in *Giur. it.*, 1996, II, p. 576.

Cass. sez. un., 27 marzo 1996, Sala, in *Foro it.*, 1996, II, p. 473.

C. eur., 25 gennaio 1997, Halford c. Regno Unito, n. 20605/92.

Cass. sez. II, 21 aprile 1997, Viveri, in *ANPP*, 1998, p. 296.

Cass. sez. VI, 10 novembre 1997, n. 4397, in *C.E.D. Cass.,* n. 210063.

Cass. sez. VI, 21 gennaio 1998, Greco, in *Dir. pen. proc.,* 1998, p. 1234.

Cass. sez. III, 23 febbraio 1998, Derzsiova, in *RP*, 1998, p. 816.

C. eur., 25 marzo 1998, Kopp c. Svizzera, n. 23224/94.

*United States v. Barth*, 26 F. Supp. 2d 929, 9367-37 (W.D. Tex. 1998).

C. eur., 23 settembre 1998, McLeod c. Regno Unito, in *Recueil des arrêts et décisions*, VII, 1998, p. 2791, § 52.

Cass. sez. un., 24 settembre 1998, n. 21, in *Arch. n. proc. pen.,* 1998, n.4, p. 539.

Cass. sez. VI, 16 febbraio 1999, Stellino ed altri, *Gdir*, 1999, fasc. 17, p. 87.

Cass. sez. I, 2 marzo 1999, Cavinato, *Gazz. Giur.,* 1999, n. 29, p. 32.

Cass. sez. V, 11 maggio 1999, n. 7597, in *Giust. pen.,* 2000, II, p. 308.

Cass. sez. VI, 11 maggio 1999, Belocchi, n. 8645, in *Cass. pen.*, 2000, p. 3353.

Cass. sez. VI, 22 luglio 1999, Patricelli, n. 9428, in *Giust. pen.*, p. 188;

Cass. sez. VI, 14 dicembre 1999, Piersanti, *C.E.D. Cass.*, n. 214945.

Cass. sez. IV, 9 febbraio 2000, Arizi, *C.E.D. Cass.*, n. 215658.

GIP Trib. Roma, ord. 14 febbraio 2000, *CP*, 2000, 1931, con nota di C. Carmona.

Cass. sez. I, 26 febbraio 2000, Delle Grottaglie, *C.E.D. Cass.*, n. 216282.

C. eur., 15 marzo 2000, Khan c. Regno Unito, n. 35394/97.

Cass. sez. V, 29 marzo 2000, Terracciano, in *C.E.D. Cass.*, n. 215731.

Cass. sez. un., 8 maggio 2000, D'Amurri, *C.E.D. Cass.*, n. 215841.

Cass. sez. un., 21 giugno 2000, Primavera ed altri, in *A. n. proc. pen.*, 2000, p. 650.

Cass. sez. un., 30 giugno 2000, Tammaro, *C.E.D. Cass.*, n. 216247

Cass. sez. I, 11 agosto 2000, Nicchio ed altri, n. 4979, in *C.E.D. Cass.*, n. 216747.

Cass. sez. IV, 29 gennaio 2001, n. 8437, inedita.

*State v. Schwartz*, 21 P. 3d 1128, 1131, 1135 (Or. Ct. App. 2001).

Cass. sez. un., 31 ottobre 2001, Policastro ed altri, in *Giust. pen.*, 2002, III, p. 625.

Cass. sez. I, 19 febbraio 2002, Panella, n. 13104, in *Guida al diritto*, 2002, 22, p. 82.

Cass. sez. V, 27 febbraio 2002, Bresciani, in *Foro it.*, 2002, II, c. 635.

C. eur., 14 marzo 2002, Puzinas c. Lituania, n. 44800/98.

C. cost., sent. 11 aprile 2002, n. 135, in *Giur. Cost.,* 2002, pp. 1062 ss.

C. cost., 24 aprile 2002, n. 135, in *Giur. cost.,* 2002, pp. 1062 ss.

C. cost., 24 aprile 2002, n. 135, in *Giur. cost.,* 2002, pp. 1062 ss.

Cass. sez. VI, 10 dicembre 2002, Palumbo, in *C.E.D. Cass.*, n. 223961.

Cass. sez. IV, 8 maggio 2003, Lanzetta, in *Cass. pen.*, 2006, p. 536.

Cass. sez. V, 13 maggio 2003, Pagano ed altri, n. 25522, in *Guida al diritto*, 2003, 40, p. 64.

Cass. sez. un., 28 maggio 2003, n. 36747, in *Cass. pen.,* 2004, p. 209.

Cass. sez. I, 6 giugno 2003, Faraci, in *C.E.D. Cass.,* n. 225141.

Cass., sez. un., 24 settembre 2003, Torcasio, in *C.E.D. Cass.*, n. 225465.

Cass. sez. V, 4 novembre 2003, Hani, n. 44718, in *Guida al Diritto*, 2004, 8, p. 82.

Cass. sez. VI, 22 dicembre 2003, Scremin, in *CP* 2005, p. 3926.

Cass. sez. VI, 15 gennaio 2004, n. 4942, in *C.E.D. Cass.*, n. 229999.

Cass. sez. V, 20 aprile 2004, Scardamaglia, n. 24229, in *Guida al diritto* 2004, 26, p. 76.

Cass. sez. IV, 30 giugno 2004, n. 37646, in *Cass. pen.*, 2006, 5, p. 1837.

Cass. sez. un., 22 marzo 2005, n. 17706, Petrarca, in *Cass. pen.,* 2005, p. 2916.

C. eur., 12 maggio 2005, Ocalan c. Turchia, n. 46221/99.

GIP Trib. Torino, 25 novembre 2005, *DG*, 2005, 15, 83.

Cass. sez. un., 29 novembre 2005, Campennì, n. 2737/06, in *Cass. mass.*, rv. 232605.

Cass. sez. un., 28 luglio 2006, P.A., *C.E.D. Cass.,* n. 233974.

Cass. sez. VI, 14 novembre 2006, Protopapa, in *Cass. pen.*, 2008, p. 2532.

Cass. sez. IV, 29 gennaio 2007, n. 8871, in *Cass. pen.*, 2008, p. 1137.

C. eur., 10 aprile 2007, Panarisi c. Italia, n.46794/99, in *CP* 2007, p. 3941.

Cass. sez. VI, 11 dicembre 2007, n. 15396, in *Cass. pen.*, 2009, 6, p. 2534.

*United States v. Welch* 291 F. App'x 193, 205 (10th Cir. 2008).

Bundesverfassungsgericht, 27 febbraio 2008, in Riv. trim. dir. pen. econ., 3, 2009, pp. 679 e ss.

Cass. sez. I, 28 maggio 2008, in *C.E.D. Cass.*, n. 240092.

Cass. sez. un., 26 giugno 2008, Carli, in *Cass. pen.*, 2009, p. 30.

*United States v. Ganoe*, 538 F. 3d 1117, 1127 (9th Cir. 2008).

C. eur, 10 febbraio 2009, Iordachi c. Moldavia, in *Cass. pen.*, 2009, p. 4021.

Cass. pen., Sez. VI, 12 febbraio 2009, n. 12722, in *Giur. It.* 2010, 5, 1186.

Cass. sez. I, 28 aprile 2009, n. 31570, in *Guida al dir.*, 44, 68.

Cass. sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.,* n. 246954.

Cass. sez. VI, 20 ottobre 2009 (dep. 31 dicembre 2009), Bassi, n. 50072, in *Giur. It.* 2010, 12, 2649.

Cass. sez. III, 25 febbraio 2010, n. 12562, in *C.E.D. Cass.*, n. 246594.

Cass. sez. I, 9 marzo 2010, n. 9416, in *Cass. pen.*, 2012, p. 1062.

Cass. sez. V, 10 marzo 2010, n. 9667, in *Dir. pen. proc.*, 2010, p. 1464.

Cass. sez. un., 25 luglio 2010, Donadio, in *C.E.D. Cass.*, n. 247994.

C. eur., sez. V, 2 settembre 2010, *Utza c. Germania.*

Cass. sez. V, 30 ottobre 2010, in *Dir. pen. proc.*, 2010, n. 1464.

Cfr. *United States v. Stabile*, 633 F. 3d 219, 237-39 (3d Cir. 2011).

Cass. sez. I, 10 gennaio 2012, n. 14529, inedita.

Corte Suprema USA, 23 gennaio 2012, *U.S. vs Jones*, in *Arch. pen.*, 2012, p. 309.

Cass. sez. VI, 27 novembre 2012, Bisignani, in *Mass. Uff.*, n. 254865.

*United States v. Gitarts*, 341 F. App'x 935 (4th Cir. 2009).

C. eur., grande sezione, cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e al.*, 8 aprile 2014.

Cass. sez. VI, 12 marzo 2015, n. 24237, Maglia, inedita.

Cass. sez. VI, 26 maggio 2015, n. 27100, Musumeci, in *C.E.D. Cass.,* n. 265654.

Cass. sez. III, 10 novembre 2015, n. 50452, in *C.E.D. Cass.*, n. 265615.

C. eur., 4 dicembre 2015, Zakharov c. Russia, n. 47143/06.

Cass. sez. V, 17 dicembre 2015, n. 11419, in *C.E.D. Cass.,* n. 266373.

Cass. sez. II, 18 dicembre 2015, n. 1924, in *C.E.D. Cass*, n. 265989.

C. eur., 23 febbraio 2016, *Capriotti c. Italia*, n. 28819/12, in *Riv. it. dir. e proc. pen.*, fasc. 2, 2016, p. 1100.

Cass. sez. VI, (ord.) 6 aprile 2016, Scurato, in *Arch. pen.*, al sito http://www.archiviopenale.it/.

Cass. sez. IV, 8 aprile 2016, n. 16670, in *C.E.D. Cass.*, n. 266983.

Cass. sez. un., 28 aprile 2016, Scurato, n. 26889, in *Dir. pen. cont.,* 4 luglio 2016, p. 22, in Internet al sito www.penalecontemporaneo.it.

Cass. sez. IV, 28 giugno 2016, n. 40903/16, in *C.E.D. Cass.* n. 268228.

Cass. sez. F., 23 agosto 2016, n. 35536, in *C.E.D. Cass.*, n. 267598.

Bundersverfassungsgericht, I Senato, 20 aprile 2016 – 1 BVR 966/09, 1 BVR 1140/09, in Internet al sito https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html.