N. 6652/2018 R. G. N. R.
N. 2098/2021 R. G. Dib.

TRIBUNALE DI PERUGIA

SEZIONE PENALE

Il Tribunale di Perugia, in composizione collegiale, nella persona dei seguenti magistrati:

- dott.ssa Carla Maria Giangamboni — Presidente
- dott. Edoardo Esposito — Giudice
- dott.ssa Serena Ciliberto — Giudice

a scioglimento della riserva assunta all'udienza del 13.12.2022, sull'eccezione, sollevata dalla difesa di Luca PALAMARA, di inutilizzabilità delle intercettazioni ottenute mediante captazione dei flussi di comunicazione sul telefono cellulare dell'imputato con *trojan horse*, per violazione dell'art. 268 comma 3 c.p.p.

OSSERVA

L'eccezione difensiva si fonda sul presupposto per cui l'attività captativa effettuata sul telefono cellulare dell'imputato PALAMARA non sarebbe stata gestita direttamente da un *server* installato nella Procura della Repubblica di Roma (competente per le indagini prima della trasmissione degli atti alla Procura della Repubblica di Perugia ai sensi dell'art. 11 c.p.p.), ma con l'intervento mediato di altri due, ulteriori *server* intermedi collocati "nel territorio di Napoli", che secondo i difensori dell'imputato sarebbero non meri *server* di transito, ma impianti in grado di alterare i *files* riproducenti i contenuti delle conversazioni captate e finanche "riscriverli", omettendo spezzoni delle conversazioni soggette a captazione e trasmettendo all'unico *server* autorizzato e legittimato a ricevere le comunicazioni intercettate (quello installato presso la Procura della Repubblica di Roma) i risultati non dell'originale captazione ma altri risultati, non conformi a quelli originali.

Per affrontare e correttamente risolvere l'eccezione prospettata dalla difesa, conviene partire dalla ricostruzione delle modalità di funzionamento del sistema di captazione installato sul telefono cellulare di Luca PALAMARA.

Nella relazione tecnica della società R. C. S. s.p.a. – appaltatrice del servizio captativo - in atti (contenuta tra i documenti depositati dal Pubblico Ministero all'udienza del 23.4.2021 e intitolata "dettagli tecnici relativi al sistema R. C. S. per le intercettazioni telematiche attive e passive) il sistema delle intercettazioni telematiche attive viene descritto come basato su di un captatore informatico che recupera delle evidenze sul terminale su cui è installato. Si tratta di un *software* che viene installato sull'apparecchio bersaglio dietro al quale si cela un virus informatico (*spyware*) appartenente al genere del

"*trojan horse*", in grado di attivare il microfono dell'apparecchio di destinazione e formare copia della messaggistica inviata e ricevuta dall'utente: il captatore "preleva" le evidenze sul terminale bersaglio e le trasferisce, previa cifratura, sul *web* – tramite protocollo di trasferimento sicuro HTTPS - prima ad un *server* intermedio, di tipo CSS (Cyber Stealth Surveillance) che serve solo alla decriptazione ed anonimizzazione dei dati raccolti, mediante un algoritmo simmetrico AES-256; questo *server*, a seguito della decriptazione, inoltra ulteriormente i dati – senza memorizzarli, anzi cancellandoli dalla memoria locale, e tramite protocollo di trasferimento sicuro SFTP - ad un altro *server*, questa volta di tipo IVS (Internet Visualization System) installato presso i locali della Procura che ha autorizzato le intercettazioni, il quale decodifica le evidenze intercettate in arrivo, le memorizza su una posizione criptata e permette la visualizzazione, in formato audio, delle comunicazioni captate agli operatori che sovrintendono all'attività.

Di tale meccanismo di funzionamento l'ing. Duilio Bianchi (direttore della Divisione IP di RCS s.p.a., società di Milano appaltatrice del servizio captativo) ha dato spiegazione al Consiglio Superiore della Magistratura nel corso dell'udienza disciplinare tenutasi a carico del dott. PALAMARA il 23.9.2020 e il 28.9.2020, rappresentando che il *software* agiva creando – nell'ambito dell'orario preimpostato dalla P. G. operante - registrazioni di cinque minuti solo ed esclusivamente quando il telefono era in standby a schermo spento, interrompendo la registrazione sia al termine dei cinque minuti, sia ogniqualvolta il cellulare veniva utilizzato per qualsivoglia ragione che avesse fatto accendere lo schermo; successivamente, inoltrava le comunicazioni intercettate e cifrate - di durata pari a cinque minuti, o anche inferiore in caso di accensione dello schermo – tramite i due *server* CSS e IVS all'interno dei locali della "*Procura di Roma*", autorizzati per eccezionali ragioni di urgenza con decreto motivato dall'allora Procuratore della Repubblica di Perugia, dott. De Ficchy, e vistato dall'allora Procuratore della Repubblica di Roma, dott. Pignatone.

In sede di audizione dinanzi alla Sezione disciplinare del C. S. M., l'ing. Bianchi ha precisato che questi frammenti di conversazione, di cinque minuti o meno di durata (denominati "*chunks*") venivano direttamente inoltrati sul *server* installato presso la Procura della Repubblica di Roma (alla domanda del P. G., dott. Gaeta, "*quindi ci conferma che non c'era assolutamente alcun server intermedio tra l'apparecchio intercettato e il server della Procura*", l'ing. Bianchi risponde "*no, va direttamente sul server della Procura*").

Tuttavia, durante l'interrogatorio reso alla Procura della Repubblica presso il Tribunale di Firenze in data 22.4.2021 e nel corso dell'esame reso ai sensi dell'art. 210 c.p.p. dinanzi al G. U. P. di Perugia all'udienza del 3.5.2021, lo stesso ing. Bianchi, confermando quanto dichiarato a sommarie informazioni alla P. G. in data 20.2.2021, precisava che sul telefono cellulare del dott. PALAMARA il captatore, dopo aver prelevato i frammenti di conversazione intercettati, li inoltrava ad un server CSS

(con indirizzo IP fisso: 93.39.197.234) installato *"presso i locali server della Procura di Napoli"*, che *"serviva da transito per tutte le Procure inquirenti del territorio nazionale per le evidenze intercettate"*; a sua volta, il *"il server CSS trasmetteva i dati sul server HDM, anch'esso installato nei locali della Procura della Repubblica di Napoli, tramite protocollo SFTP sull'indirizzo IP interno privato n. 172.16.5.6; a sua volta, il server HDM, utilizzando l'indirizzo IP pubblico n. 93.39.197.236 smistava, con protocollo SFTP le evidenze intercettate ai vari server IVS installati nelle sale server delle Procure inquirenti. I server IVS servono per memorizzare e visualizzare i dati intercettati.*

Sia il server CSS che l'HDM, come detto attestati presso la sala server della Procura della Repubblica di Napoli, ricevevano ed immagazzinavano i dati per lo stretto tempo necessario alla ricostruzione ed invio al server IVS di pertinenza, e venivano cancellati automaticamente dall'applicativo di gestione dopo la trasmissione. In tale fase, ai dati che non erano criptati, potevano aver eventualmente accesso in remoto, solo gli amministratori di sistema di R. C. S. s.p.a. dalla sede di Milano".

È quindi emersa l'esistenza di due *server* intermedi, posti tra il telefono cellulare intercettato sui cui era stato inoculato il *trojan horse* e il *server* finale IVS presso la Procura della Repubblica di Roma, entrambi allocati, per ragioni tecniche, nei locali della Procura della Repubblica di Napoli.

Le evidenze raccolte dal captatore venivano memorizzate sul cellulare prima di essere spedite; venivano generati dal *software* un *file* audio e un *file* Json (contenente metadati, vale a dire informazioni relative alla registrazione); gli audio (i *"chunks"*) transitavano prima al *server* CSS tramite protocollo sicuro HTTPS per essere riassemblati e venivano contestualmente cancellati dalla memoria fisica del cellulare intercettato; poi passavano, tramite protocollo sicuro SFTP, sul *server* HDM, venivano contestualmente cancellati dal *server* CSS, ed erano infine smistati al *server* IVS finale di destinazione, previa cancellazione anche dal secondo *server* intermedio HDM.

Richiesto dagli inquirenti di spiegare perché in sede di audizione dinanzi al C. S. M. avesse descritto l'esistenza di un solo *server* intermedio e non di due, l'ing. Bianchi ha precisato di avere "commesso un errore" all'epoca, descrivendo quella che al settembre 2020 era l'architettura più recente del sistema; mentre all'epoca in cui il telefono cellulare del dott. PALAMARA è stato intercettato (dal 2.5.2019 all'8.9.2019) la configurazione era quella con due *server* intermedi tra l'apparecchio bersaglio e il *server* di destinazione, entrambi allocati, come riferito, presso la Procura della Repubblica di Napoli.

Così ricostruito il sistema di captazione, osserva il Collegio che dall'informativa del C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) della Polizia postale, datata 24.5.2021 e depositata dal Pubblico Ministero all'udienza del 27.5.2021, emerge:

- che il *server* CSS è un *server* di "transito", destinato a configurare l'agente captatore nei limiti del provvedimento che dispone l'intercettazione, limitandosi successivamente a ricevere i frammenti del dato captativo contenuto nel dispositivo bersaglio (generando un *file* contenente i metadati del

risultato captativo e un *file* audio ad esso corrispondente) e a memorizzare i dati captati per il tempo tecnico necessario alla loro ricomposizione ed invio verso il *server* HDM, implementando sistemi di cancellazione automatica successivi all'invio stesso;

- che il *server* HDM è un *server* di "smistamento", programmato per raccogliere e riconoscere i vari *files* – di contenuto audio e di metadati – intercettati da uno stesso captatore (contrassegnato da un numero seriale identificativo – ID Agent) e successivamente trasmetterli presso il *server* IVS installato presso la Procura di destinazione finale, cancellando automaticamente i dati trasmessi subito dopo;
- che il *server* IVS è l'unico, tra i tre descritti, deputato all'immagazzinamento stabile dei dati ed alla visualizzazione di essi da parte della P. G. operante;
- che l'allocazione fisica dei *server* CSS e HDM è stata individuata, fino al 4.4.2019, presso la sede R. C. S. s.p.a. di Napoli, ubicata presso il Centro Direzionale – Isola E7, 13° piano, interno 58; dopo il 4.4.2019 – vale a dire prima dell'inizio delle operazioni captative sul telefono cellulare del dott. PALAMARA – questi *server* sono stati trasferiti, su disposizione del *management* aziendale, presso i locali della Procura della Repubblica di Napoli; infine, tra l'agosto ed il settembre 2019, l'architettura di sistema è stata completamente decentralizzata, con l'installazione di più *server* CSS installati presso ciascuna Procura della Repubblica ove la R. C. S. s.p.a. operava e l'eliminazione del *server* di smistamento HDM;
- che il tempo totale che il sistema impiega per cancellare automaticamente i dati dal *server* di passaggio precedente, *"salvo anomalie"*, è di circa 2 – 3 minuti;
- che a presidio dell'integrità del dato captato, non essendo state implementate nel sistema funzioni di *hashing* o firma digitale, si pone solo il codice (denominato ID Agent) che contraddistingue il singolo *spyware* di volta in volta operativo e i protocolli di trasferimento di sicurezza HTTPS (dal *server* CSS al *server* HDM) e SMTP (dal *server* HDM al *server* IVS): tale sistema, secondo gli ispettori del C.N.A.I.P.I.C., *"non garantisce univocamente che un determinato dato non possa esser stato modificato"*, ma per alterarlo *"occorrerebbe aggirare il protocollo di sicurezza ed avere accesso all'interno del sistema stesso, e a tal proposito la circostanza di un accesso abusivo potrebbe verosimilmente essere verificata mediante l'analisi dei files di log presenti sul sistema"* (p. 10 informativa);
- che all'interno del sistema CSS, in sede di ispezione, è stata accertata la presenza di *chunks* in *file* compressi, in formato .bz2, della dimensione di 256k.

A seguito dell'accertamento tecnico irripetibile ex art. 360 c.p.p. disposto dal G. U. P. di Perugia ex art. 421 bis c.p.p. per accertare il contenuto dei *files* rimasti sul sistema CSS, è stata redatta informativa da parte del C.N.A.I.P.I.C. in data 14.6.2021, dalla quale è emerso, in estrema sintesi, che si tratta di 19 *files* audio, intellegibili solo dopo la compressione, generati dal captatore informatico installato sul cellulare

del dott. PALAMARA e privi di qualsiasi rilevanza processuale (cfr. p. 7 ss. informativa); invece, sul *server* HDM non sono stati rinvenuti, dagli ispettori operanti, *files* di contenuto relativi ai dati captati dal *trojan* inoculato nell'apparecchio, bensì solo *files* di metadati in formato .json.

Di conseguenza, tenuto conto anche dell'infinitesimale dimensione dei dati (3,1 MB) rimasti presenti sul sistema rispetto al carico di *files* transitato sul *server* CSS (circa 43 TB, laddove un Terabyte equivale a un milione di Megabyte), ne appare evidentemente confermata, ad avviso del Collegio, la natura di mero *server* di transito e di passaggio dati, avente funzioni di ricezione, ricostruzione, trasferimento e immediata cancellazione dei dati inviati dal captatore; parimenti, quanto al *server* HDM, è risultata confermata la sua natura di semplice *server* di smistamento – previa identificazione del captatore contrassegnato dal proprio ID Agent – al *server* finale IVS di visualizzazione installato presso la Procura della Repubblica procedente (in questo caso, la Procura di Roma previo decreto autorizzativo congiunto dei Procuratori della Repubblica di Perugia e Roma).

È chiaro, a questo punto, che il "pericolo" di una manipolazione di dati (vuoi effettuata in maniera automatica dal *software* di captazione, vuoi – consapevolmente o meno - dagli operatori di P. G. preposti alla gestione del sistema) appare, ad avviso dello scrivente Collegio, confinata su di un piano meramente congetturale.

Per potere anche solo immaginare un'alterazione delle evidenze intercettate, infatti, data l'architettura del sistema come sopra complessivamente ricostruita, uno dei due *server* intermedi (CSS e HDM) avrebbe dovuto manifestare caratteristiche diverse da quelle descritte dall'ing. Bianchi e, in seguito, concretamente accertate dal C.N.A.I.P.I.C. della Polizia Postale: mentre, come detto, la circostanza per cui sui due *server* in questione siano stati rinvenuti, rispettivamente, frammenti di *files* di dimensione assolutamente infinitesimale e solo *files* di metadati, unitamente alla considerazione che i *files* audio relativi alle comunicazioni captate veniva automaticamente cancellato in tempo brevissimo dopo ciascun transito, induce a escludere radicalmente che vi possa essere concretamente stata un'attività di manipolazione o di alterazione dei dati raccolti, sotto il profilo della genuinità ed autenticità del risultato probatorio.

Quanto, invece, al profilo della denunciata violazione dell'art. 268 comma 3 c.p.p., occorre evidenziare che la disposizione normativa prevede, testualmente: *"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 di urgenza, il pubblico ministero può disporre, con provvedimento motivato, il compimento delle operazioni mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria"*.

Sul tema del bilanciamento dell'attività captativa con i parametri costituzionalmente tutelati della libertà e della segretezza della corrispondenza (art. 15 Cost.) e del diritto di difesa (art. 24 Cost.), la Consulta è

intervenuta, già nella vigenza del codice di procedura penale abrogato (art. 226 ultimo comma c.p.p.), con la sentenza n. 34 del 6.4.1973, così pronunciandosi: *"nel nostro sistema quindi la compressione del diritto alla riservatezza delle comunicazioni telefoniche, che l'intercettazione innegabilmente comporta, non resta affidata all'organo di polizia, ma si attua sotto il diretto controllo del giudice. É al magistrato che la legge riconosce il potere di disporre l'intercettazione e dalla legge stessa sono desumibili i limiti di siffatto potere. La richiesta di provvedimenti autorizzativi della intercettazione va valutata con cautela scrupolosa giacché da provvedimenti del genere deriva una grave limitazione alla libertà e segretezza delle comunicazioni. Nel compiere questa valutazione il giudice deve tendere al contemperamento dei due interessi costituzionali protetti onde impedire che il diritto alla riservatezza delle comunicazioni telefoniche venga ad essere sproporzionatamente sacrificato dalla necessità di garantire una efficace repressione degli illeciti penali. A tal fine é indispensabile che accerti se ricorrano effettive esigenze, proprie dell'amministrazione della giustizia, che realmente legittimino simile forma di indagine e se sussistano fondati motivi per ritenere che mediante la stessa possano essere acquisiti risultati positivi per le indagini in corso.*

Del corretto uso del potere attribuitogli il giudice deve dare concreta dimostrazione con una adeguata e specifica motivazione del provvedimento autorizzativo. Discende da quanto si é detto - vale a dire dal principio che il diritto garantito dall'art. 15 Cost. possa essere compresso solo nei limiti effettivamente richiesti da concrete, gravi esigenze di giustizia - la conseguenza che il provvedimento di autorizzazione stabilisca anche la durata delle intercettazioni e che, quando una proroga si renda necessaria, se ne offra concreta, motivata giustificazione.

Ma il rispetto della norma costituzionale di raffronto non trova soddisfazione solo nell'obbligo della puntuale motivazione del decreto dell'autorità giudiziaria. Altre garanzie sono richieste: a) garanzie che attengono alla predisposizione anche materiale dei servizi tecnici necessari per le intercettazioni telefoniche, in modo che l'autorità giudiziaria possa esercitare anche di fatto il controllo necessario ad assicurare che si proceda alle intercettazioni autorizzate, solo a queste e solo nei limiti dell'autorizzazione; b) garanzie di ordine giuridico che attengono al controllo sulla legittimità del decreto di autorizzazione ed ai limiti entro i quali il materiale raccolto attraverso le intercettazioni sia utilizzabile nel processo.

Sul primo punto la Corte osserva che il legislatore gode di un ampio margine di discrezionalità nell'organizzazione del servizio, ma sente il dovere di formulare l'auspicio che si realizzino opportuni interventi legislativi idonei ad attuare anche sul piano tecnico le condizioni necessarie all'effettivo controllo di cui innanzi si é detto.

Sul secondo punto la Corte osserva che non é necessario che le garanzie siano puntualmente poste nel testo normativo che disciplina le intercettazioni, potendo esse essere rinvenute anche in altre norme ed anche nei principi generali che disciplinano le attività processuali".

A sua volta, la Suprema Corte di Cassazione, con la fondamentale pronuncia a Sezioni Unite n. 36359 del 26.6.2008 (imp. Carli) ha in tal modo ricostruito la *ratio* della disposizione di cui all'art. 268 comma 3 c.p.p. alla luce della pronuncia del Giudice delle leggi, precisando limiti e significato operativo delle attività di captazione: *"In proposito è necessario ricordare come la disciplina originaria del codice del 1930 (contenuta*

negli artt. 226 ultimo comma e 339) prevedeva che le intercettazioni venissero effettuate «presso impianti telefonici di pubblico servizio». In sintonia con il dato normativo allora vigente fino agli inizi degli anni '70 le operazioni di captazione, registrazione ed ascolto delle conversazioni intercettate venivano perciò svolte in unità di tempo e di luogo attraverso registratori collocati presso l'operatore telefonico e presidiati da personale di polizia giudiziaria.

Questa metodologia si prestava ad evidenti abusi, consentendo agevolmente la realizzazione di ascolti illeciti, sottratti al controllo dell'autorità giudiziaria.

In tale contesto intervenne l'autorevole monito della Corte Costituzionale (Corte Cost. 6 aprile 1973, n. 34), la quale, nel dichiarare non fondata la questione di legittimità costituzionale del citato art. 226 ultimo comma, dettò però le condizioni di compatibilità delle intercettazioni con i princìpi della carta fondamentale in materia di riservatezza delle comunicazioni, evidenziando come le stesse dovessero essere subordinate al rigoroso rispetto di precise garanzie, non soltanto di ordine giuridico, ma anche di ordine "tecnico", finalizzate alla possibilità che l'autorità giudiziaria esercitasse il controllo necessario ad assicurare che si procedesse soltanto alle intercettazioni autorizzate.

A breve distanza di tempo è poi sopravvenuto l'intervento del legislatore, che ha significativamente riformato la disciplina delle intercettazioni. La legge 8 aprile 1974, n. 98 ha così introdotto nel codice abrogato, all'art. 226 quater, l'obbligo di concentrare le operazioni di intercettazione esclusivamente presso gli impianti installati nelle Procure, proprio al fine di evitare il rischio dei segnalati abusi, instaurando un diretto controllo del pubblico ministero sull'esecuzione delle medesime (il secondo comma dell'art. 226 quater, come sostituito dal d. l. n. 59 del 1978 convertito nella l. n. 191 del 1978 consentiva peraltro il ricorso agli impianti in dotazione alla polizia giudiziaria "per ragioni d'urgenza").

La modifica legislativa ha avuto una immediata ricaduta sulla tecnica di intercettazione. Ed invero, dovendo collocare gli impianti di registrazione non più presso la centrale dell'operatore telefonico, bensì presso gli uffici della Procura della Repubblica, si è reso necessario utilizzare un dispositivo (il c.d. "traslatore") in grado di deviare la comunicazione anche ad un punto d'ascolto e di registrazione ivi istituito, posto che necessariamente la captazione in senso proprio delle conversazioni non poteva (e come si è già precedentemente detto, allo stato non può) che avvenire presso lo stesso operatore.

Il codice del 1988 ha recepito questo assetto in un contesto tecnologico sostanzialmente immutato, se non per la raggiunta maggiore sofisticazione dei traslatori. Ma nella sua essenza la tecnica di intercettazione era, al momento dell'entrata in vigore della nuova legge processuale, la stessa assunta a paradigma della normativa previgente.

In tal senso, dunque, l'art. 268 ha ribadito i contenuti del precedente art. 226 quater, se si eccettua la previsione nel secondo comma dell'obbligo di trascrizione sommaria nel verbale del contenuto delle intercettazioni, nonchè per lo "spostamento" nell'art. 89 disp. att. della descrizione degli ulteriori contenuti dello stesso verbale, che l'art. 226 quater citato invece illustrava direttamente, anche ricorrendo all'espressione di sintesi «descrizione delle modalità di registrazione».

Dopo l'entrata in vigore del nuovo codice, la rapida evoluzione delle tecnologie, riguardanti la telefonia (si pensi ad esempio all'affermazione della telefonia mobile) e la registrazione, ha però affidato all'interprete il delicato compito di coniugare le nuove tecniche operative con un dato normativo elaborato prima del loro avvento.

Va ribadito (richiamando quanto innanzi già detto) come l'art. 268 del vigente codice di rito sostanzialmente operi una segmentazione dell'attività di intercettazione in frammenti che assumono anche autonoma e diversa rilevanza sul piano giuridico: captazione, registrazione, ascolto, verbalizzazione. È necessario altresì sottolineare come il primo segmento, la captazione delle conversazioni (e cioè l'intercettazione in senso stretto), non può che essere effettuata presso l'operatore telefonico che "trasporta" la comunicazione, quale che sia la tecnica utilizzata. Anche se sono in corso di sperimentazione sistemi che consentono il comando di captazione in remoto, rendendo dunque le intercettazioni indipendenti dall'azione dell'operatore telefonico, allo stato tale soluzione non è ancora effettivamente disponibile e dunque non v'è dubbio che la materiale captazione delle comunicazioni avviene formalmente al di fuori degli uffici della Procura, dove il segnale sonoro viene semplicemente deviato per la registrazione e l'ascolto. Circostanza che consente anche alla dottrina di ritenere che le operazioni e gli impianti menzionati nel terzo comma dell'art. 268 cod. proc. pen. riguardino la sola attività di registrazione e non, per l'appunto, quella di captazione.

Con specifico riguardo all'attività di ascolto va invece precisato come all'epoca del varo del nuovo codice di procedura penale la stessa non poteva di fatto essere separata da quella di registrazione. Infatti, entrambe le operazioni venivano effettuate attraverso il medesimo apparato, un registratore monolinea a nastri magnetici, sui quali venivano impressi i flussi vocali captati (ed infatti l'art. 89 disp. att. tuttora fa riferimento, al secondo comma, ai «nastri contenenti le registrazioni», riferimento divenuto oramai del tutto anacronistico).

La rivoluzione che ha trasformato la telefonia nel recente passato ha segnato, in estrema sintesi, il progressivo passaggio dalla trasmissione di segnali in maniera analogica a quella di dati in forma digitale, trasformando il servizio telefonico (a partire da quello di telefonia mobile) in un sistema informatico o telematico. E' dunque mutato lo stesso oggetto fisico della comunicazione telefonica e, quindi, della sua intercettazione. Di conseguenza è stato fatto progressivamente ricorso alla utilizzazione di sistemi di registrazione digitale computerizzata che hanno sostituito gli apparti "meccanici".

In definitiva si è assistito ad una profonda trasformazione della realtà presupposta dal legislatore del 1988. Da qualche anno, infatti, per la registrazione vengono utilizzati apparati multilinea (collegati cioè ad un flusso di linee telefoniche) che registrano dati trasmessi in forma digitale e successivamente decodificati in file vocali immagazzinati in memorie informatiche centralizzate. I dati così memorizzati vengono poi di regola trasferiti su supporti informatici (essenzialmente Cd-Rom o DVD) per renderli fruibili all'interno dei singoli procedimenti. In pratica dunque i supporti costituiscono il corredo documentale in precedenza rappresentato dai nastri magnetici.

Insomma il trasferimento (o "scaricamento") dei dati sui supporti costituisce uno dei segmenti dell'intercettazione, autonomo rispetto alla "registrazione" e tecnicamente diverso da questa.

Le operazioni di "registrazione", che in forza del terzo comma, parte prima, dell'art. 268 c.p.p., debbono essere compiute esclusivamente per mezzo degli impianti installati nella procura della Repubblica, consistono dunque, come è agevole desumere da quanto fin qui detto, nella immissione dei dati (captati presso la centrale dell'operatore telefonico e trasmessi

agli impianti in Procura) nella memoria informatica centralizzata (cd. server) che si trova nei locali della Procura della Repubblica a ciò destinati.

I menzionati apparati permettono altresì di "remotizzare" agevolmente (attraverso il sistema c.d. client–server) l'ascolto - nonché, volendo, anche una registrazione (ovviamente derivata da quella effettuata in Procura, e da non potersi a questa sostituire) deviando il flusso in entrata anche verso molteplici punti di ricezione, collocabili in qualsiasi luogo (e dunque anche all'esterno degli uffici di Procura) e collegati con il sistema centrale verso cui l'operatore telefonico ha trasmesso il flusso di dati captati.

Spinta più oltre, la tecnica in questione può poi trasformare l'impianto presente in Procura in una sorta di mero "ripetitore", utilizzato esclusivamente per l'instradamento del flusso di dati dall'operatore telefonico a quello di polizia, senza l'inserimento e la "registrazione" di quei dati nel server (memoria informatica centralizzata) esistente nei locali della Procura; infatti, è sufficiente che presso la Procura venga occupata la linea telefonica verso cui avviene la trasmissione dei dati captati dall'operatore telefonico, immediatamente resi disponibili in remoto: un'intercettazione così effettuata sarebbe certamente illegittima, con sanzione di inutilizzabilità.

7.2 - Quanto detto consente di trarre le conclusioni per addivenire alla nozione di registrazione, ai fini che in questa sede rilevano con riferimento alle disposizioni di cui all'art. 268 c.p.p.

La "registrazione" dei dati captati nella centrale dell'operatore telefonico, e da lì trasmessi all'impianto esistente nei locali della Procura della Repubblica, si realizza con l'immissione di quei dati nel server di detto impianto. Ed è a tale specifico segmento della complessiva attività di intercettazione che l'art. 268 c.p.p. si riferisce laddove dispone che le operazioni possono essere compiute esclusivamente per mezzo degli impianti installati nella procura della Repubblica.

Per qualsiasi altra operazione, in quanto estranea alla nozione di registrazione così definita, non assume alcun rilievo, ai fini della utilizzabilità delle intercettazioni, il luogo dove la stessa è avvenuta: discorso che vale, dunque, anche per quell'operazione che consiste nello scaricamento dei dati su supporti informatici quali CD-ROM o DVD (operazione sulla quale ha posto specificamente l'accento la sentenza Sinesi della Sesta Sezione sopra ricordata), e che, pertanto, ben può essere compiuta eventualmente presso uffici di P.G. nel caso di ascolto remotizzato, previa utilizzazione della registrazione derivata da quella (che deve essere necessariamente) eseguita in Procura.

D'altra parte il legislatore ha previsto specifici mezzi di tutela, per le ipotesi in cui possano sorgere dubbi circa la regolarità della "registrazione" o sospetti di manipolazione: ed invero, in forza del sesto comma dell'art. 268 c.p.p., "ai difensori delle parti è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche".

In tema di intercettazioni a mezzo captatore informatico, il principio stabilito dalla Suprema Corte, nella sua composizione più autorevole, è stato poi ribadito anche da Cass. pen. Sez. I, sent. n. 52464 dell'8.11.2017, secondo cui *"condizione necessaria per l'utilizzabilità delle intercettazioni è che l'attività di registrazione - che, sulla base delle tecnologie attualmente in uso, consiste nella immissione dei dati captati in una memoria*

informatica centralizzata - avvenga nei locali della Procura della Repubblica mediante l'utilizzo di impianti ivi esistenti, mentre non rileva che i file audio registrati non siano trasmessi automaticamente dagli apparecchi digitali adoperati per le captazioni tra presenti, ma siano periodicamente prelevati dalla polizia giudiziaria incaricata delle operazioni e riversati "a mano" nel server dell'ufficio requirente".

Richiamati i superiori principi in diritto, è agevole a questo punto concludere che non vi è inutilizzabilità dei risultati dell'attività captativa se i relativi dati, pur transitando attraverso canali esterni – benché adeguatamente protetti dal possibile accesso di terzi – finiscono per confluire sul *server* installato, in conformità all'art. 268 comma 3 c.p.p., presso i locali della procura della Repubblica costituente il primo e finale luogo di memorizzazione del dato.

Mentre, d'altro canto, secondo la giurisprudenza assolutamente dominante (*ex multis*, Cass. pen. Sez. III, sent. n. 47557 del 26.9.2019; Cass. pen. Sez. II, sent. n. 34969 del 10.5.2013) non è necessario che gli *"impianti installati nella procura della Repubblica"* richiamati dalla disposizione in esame debbano essere quelli della singola procura della Repubblica che procede, essendo sufficiente anche l'utilizzazione degli impianti di una qualsivoglia altra procura (non dovendo essere emanato in questo caso - non trattandosi di impianti diversi di pubblico servizio o in dotazione alla P. G. - il decreto autorizzativo motivato del Pubblico Ministero di cui all'art. 268 comma 3 seconda parte c.p.p.) né che il pubblico ministero procedente deleghi l'atto di indagine ad altro pubblico ministero ai sensi dell'art. 370 comma 3 c.p.p.

Fermi i superiori principi in diritto ed in conclusione, nel caso di specie nessuna violazione dell'art. 268 comma 3 c.p.p. è dato riscontrare: le conversazioni captate dal *trojan* hanno infatti viaggiato, partendo dal telefono cellulare del dott. PALAMARA, attraverso canali protetti e sicuri (protocollo HTTPS tra l'apparecchio e il *server* CSS; protocollo SFTP tra i *server* CSS – HDM – IVS) per un periodo di tempo ristrettissimo prima della cancellazione dal *server* di transito, su impianti collocati in due distinte Procure della Repubblica (Napoli per i *server* CSS e HDM; Roma per il *server* di destinazione finale IVS), in tal modo pienamente soddisfacendo il duplice presidio tecnico – giuridico di utilizzabilità posto dalla disposizione in commento; né la difesa ha comunque dimostrato – tantomeno ha offerto di dimostrare – concrete ed effettive interferenze nell'attività captativa intervenute durante le operazioni, al di là della mera, teorica "possibilità" di manipolazione (comunque remotissima, stante i protocolli di sicurezza adottati dal sistema e confermati anche all'esito dell'integrazione probatoria disposta dal G.U.P.).

Ne consegue che l'eccezione sollevata dalla difesa PALAMARA all'udienza del 13.12.2022 con riferimento ai risultati dell'intercettazione telematica attiva mediante *trojan* di cui al RIT 175/19 deve essere rigettata.

Per i motivi descritti in narrativa, stante la completezza e attendibilità dell'analisi tecnica compiuta dagli ispettori del C.N.A.I.P.I.C. della Polizia Postale sul sistema di captazione, anche la richiesta di perizia

formulata dalla difesa si manifesta immeritevole di accoglimento, poiché superflua (rispetto al tema d'indagine suggerito, già ampiamente sviscerato in sede di udienza preliminare) ed esplorativa (poiché ancorata a profili meramente congetturali in ordine alla possibile manipolazione dei dati raccolti).

P. Q. M.

rigetta l'eccezione di inutilizzabilità delle intercettazioni telematiche attive mediante *trojan* di cui al RIT 175/19 e la richiesta di perizia avanzate dalla difesa PALAMARA e dispone procedersi oltre.

Il Presidente
Dott.ssa Carla Maria Giangamboni

I giudici *a latere*
Dott. Edoardo Esposito

Dott.ssa Serena Ciliberto

FUNZIONARIO GIUDIZIARIO
(Alfonsina Guerrieri)