



48370-17

**REPUBBLICA ITALIANA**  
In nome del Popolo Italiano  
**LA CORTE SUPREMA DI CASSAZIONE**  
QUINTA SEZIONE PENALE

Composta da:

CAMERA DI CONSIGLIO  
DEL 30/05/2017

PAOLO ANTONIO BRUNO  
GRAZIA LAPALORCIA  
CARLO ZAZA  
ANTONIO SETTEMBRE  
GIUSEPPE DE MARZO

- Presidente - Sent. n. sez.  
787/2017  
- Rel. Consigliere -

REGISTRO GENERALE  
N.15512/2017

ha pronunciato la seguente

**SENTENZA**

sui ricorsi proposti da:

OCCHIONERO FRANCESCA MARIA nato il 31/10/1968 a MENFORD( STATI UNITI  
AMERICA)  
OCCHIONERO GIULIO nato il 21/01/1971 a ROMA

avverso l'ordinanza del 30/01/2017 del TRIB. LIBERTA' di ROMA

sentita la relazione svolta dal Consigliere GRAZIA LAPALORCIA;

lette/sentite le conclusioni del PG PASQUALE FIMIANI

IL PG CONCLUDE PER LA RIMESSIONE ALLE SEZIONI UNITE , IN SUBORDINE  
L'ANNULLAMENTO CON RINVIO PER LE ESIGENZE CAUTELARI E RIGETTO NEL  
RESTO

Udito il difensore

L'AVV.TO BOTTACCHIARI SI RIPORTA AL RICORSO *per Francesca M. Occhionero;*

L'AVV.TO PARRETTA CHIEDE L'ANNULLAMENTO DELL'ORDINANZA IMPUGNATA *per*

*Giulio Occhionero*

*16*

## RITENUTO IN FATTO

1. Il Tribunale del riesame di Roma, con l'ordinanza impugnata, ha confermato quella del Giudice per le indagini preliminari dello stesso tribunale, di applicazione della custodia cautelare in carcere ai fratelli Giulio e Francesca Maria Occhionero, indagati per i reati di cui agli artt. 494, 615-ter, 617-quater e *quinquies* perché, capo A), accedevano abusivamente alla casella di posta elettronica in uso allo studio legale dell'avv. Ernesto Stajano, da dove, sostituendosi alla persona del legale, ponevano in essere, inviando all'ENAV un messaggio di posta contenente in allegato un virus informatico, atti idonei all'accesso abusivo al relativo sistema informatico contenente dati relativi alla sicurezza pubblica nel settore dell'aviazione civile e all'intercettazione delle comunicazioni telematiche al suo interno. Inoltre, capo B), per i reati di cui agli artt. 615-ter, 615-quater e 617-*quinquies* cod. pen. perché accedevano abusivamente a caselle di posta elettronica appartenenti a professionisti del settore giuridico ed economico, ad autorità politiche e militari di importanza strategica, nonché utilizzati dallo Stato e da altri enti pubblici, da cui, mediante installazione del predetto virus informatico, acquisivano notizie riservate o dati personali e sensibili.

2. La misura era disposta in relazione agli artt. 615-ter, 617-quater e 617-*quinquies*, il primo aggravato ai sensi del secondo comma n.3 e dal terzo comma, il 617-quater aggravato trattandosi di sistemi informatici o telematici utilizzati dallo Stato o da enti pubblici, il 617-*quinquies* aggravato ai sensi dell'art. 617-quater.

3. La vicenda processuale nasce dalla denuncia di Francesco Di Maio, responsabile della sicurezza dell'ENAV, di aver ricevuto, in data 26-1-2016, una *e-mail* apparentemente trasmessa dallo studio legale Stajano, contenente un allegato che egli, senza aprirlo in quanto non aveva rapporti con il mittente, aveva invece inviato per l'analisi tecnica alla Mentat Solutions srl, operante nel settore della sicurezza informatica ed in particolare nell'analisi sui *malware*.

4. L'invio della *e-mail*, il cui allegato conteneva un *virus* informatico, era ricondotto dalla Mentat a Giulio Occhionero essendo emerso che, per quanto l'indirizzo IP mittente appartenesse ad un nodo di uscita della rete di anonimizzazione Tor, la versione del virus operava reinoltrando il contenuto delle caselle utilizzate per le operazioni di esfiltrazione verso un *account* del dominio *hospenta.com* al quale sono collegati altri domini che, pur essendo registrati con il meccanismo dello schermo, risultavano riferibili all'indagato.

5. Questi risultava aver acquistato la licenza (MailBee.net) relativa al *software* utilizzato dal *malware* dal 2010 al 2015. Gli esiti dell'intercettazione telematica consentivano di individuare la rete utilizzata dagli indagati identificando indirizzi IP e le funzionalità di alcuni *server* statunitensi nei quali erano memorizzati i *files* abusivamente prelevati dai computer infettati dal *virus*. Tra i domini collegati ad uno

degli indirizzi di un *server* ve n'erano alcuni associati al dominio *hospenta.com* utilizzato dal *malware* al quale, come già osservato, sono collegati altri domini a loro volta collegati all'indagato. Tra i dati captati vi è una cartella denominata 'data' contenente un *database* chiamato Infopyramid.accdb contenente nomi, cognomi, indirizzi di posta, domini *web*, *password*, tra i quali l'ordinanza generica ha citato quelli più significativi inerenti al settore politico ed economico, nonché relativi ad enti pubblici e a società esercenti servizi di pubblica utilità, mentre dal contenuto del computer di Occhionero si è ricavato che questi, utilizzando il *malware*, si era introdotto nei sistemi informatici protetti estraendone dati.

6. Gli indagati ricorrono avverso l'ordinanza del tribunale con atti separati a firma dei rispettivi difensori.

7. Francesca Maria Occhionero articola cinque motivi di doglianza.

8. Con il primo deduce violazione degli artt. 292, comma 2 lett. c) e 309, comma 9, ultimo inciso, cod. proc. pen. per mancanza, nel provvedimento genetico della misura, dell'autonoma valutazione delle specifiche esigenze cautelari e degli indizi, essendosi l'intervento del giudice limitato alla trascrizione mediante 'copia e incolla' della richiesta del P.M., accompagnata dall'affermazione di condividerne le ragioni.

9. Il secondo e il terzo motivo investono il raggiungimento della soglia di gravità indiziaria sotto il profilo tanto della inosservanza o erronea applicazione della legge penale, quanto del vizio di motivazione.

10. Dopo aver riportato la parte di interesse della memoria depositata al tribunale del riesame, alla quale non sarebbe stata data risposta, la ricorrente assume che la specifica trattazione sull'argomento contenuta nell'ordinanza impugnata è meramente assertiva quanto alla rilevanza attribuita alle conversazioni telefoniche intercettate, due delle quali dell'indagata con il fratello, la terza della stessa con un tecnico informatico, mentre l'elemento rappresentato dalla mancata collaborazione da lei prestata in occasione delle perquisizioni (a casa della madre e casa sua) non sarebbe idonea a colmare le lacune della valutazione critica delle fonti indiziarie.

11. Il quarto motivo denuncia violazione di legge in ordine alle esigenze cautelari.

12. Quanto al pericolo di reiterazione del reato, il tribunale ha confuso tra continuità della condotta criminosa ed attualità della stessa in quanto l'ultimo preteso fatto criminoso (l'e-mail inviata all'ENAV da Giulio Occhionero) risale al gennaio 2016, mentre il tentativo di cancellazione di dati, sempre da parte del fratello, attiene al diverso profilo del pericolo di inquinamento delle prove.

13. Pericolo, quest'ultimo, ritenuto per l'appunto sulla base di tale tentativo di cancellazione di dati su *server* statunitensi, trascurando che questi ultimi erano stati sequestrati dall'FBI e comunque scollegati dalla rete, con conseguente impossibilità, per di più da remoto, di alterare o cancellare dati.

14. Il quinto motivo lamenta mancanza di pronuncia in ordine alla nullità dell'ordinanza cautelare per mancata fissazione del termine di durata delle indagini, prescritta dall'art. 292, comma 2 lett. d), cod. proc. pen..

15. Quattro i motivi a sostegno del ricorso nell'interesse di Giulio Occhionero.

16. Il primo, con le censure di cui alle lettere b), c) ed e) dell'art. 606 cod. proc. pen., ripropone la questione, di cui al primo motivo dell'altro ricorso, della mancata autonoma valutazione degli indizi e delle esigenze cautelari da parte del Giudice per le indagini preliminari.

17. Il secondo investe, con lo stesso tipo di censure, l'utilizzabilità dei risultati delle intercettazioni telematiche effettuate mediante captatore informatico (c.d. *trojan*), utilizzabilità ritenuta nel provvedimento impugnato distorcendo i principi affermati dalla giurisprudenza di legittimità (sentenze Virruso, Musumeci e, da ultimo, Sezioni Unite Scurato).

18. L'inutilizzabilità discenderebbe sia dai principi stabiliti dalle Sezioni Unite Scurato che vietano, al di fuori dei procedimenti relativi a criminalità organizzata, tutte le intercettazioni mediante *trojan* se effettuate in luogo di privata dimora, quale nella specie l'uso del *trojan* nel computer fisso dell'indagato collocato nella sua abitazione, sia dal rilievo che nella specie non si tratta di intercettazioni di flussi telematici ai sensi dell'art. 266-bis cod. proc. pen. (e cioè di dati che in transito dal PC alla rete), ma di captazione in tempo reale di un flusso di dati intercorso su un determinato schermo o all'interno di un supporto, il che integra un'attività non di intercettazione, ma di perquisizione/ispezione – contrariamente a quanto ritenuto nella sentenza Virruso che parla di 'prova atipica' - con acquisizione (sequestro) della copia, o meglio della fotografia, di un documento statico (*screenshot*) che compare a video o è prelevato dal supporto, profilo non esaminato dal tribunale.

19. Il terzo motivo investe con le censure di cui alle lettere b), c), ed e) la sussistenza dei gravi indizi. Si contesta in primo luogo la contraddittorietà dell'ordinanza tanto dove aveva ritenuto che la *mail* diretta all'ENAV fosse partita da Giulio Occhionero nonostante i consulenti di accusa e difesa siano concordi nell'affermare l'impossibilità tecnica di individuazione del mittente causa il transito della *mail* attraverso la rete di anonimizzazione Tor, quanto dove aveva affermato che nel computer dell'indagato erano stati rinvenuti *username* e *password* di persone fisiche e giuridiche pur essendo pacifico che non era stato possibile analizzare il contenuto dei computer sequestrati perché protetti da password che Occhionero non aveva inteso fornire.

20. Con lo stesso motivo il ricorrente osserva poi come il tribunale sia andato oltre l'ipotesi accusatoria laddove ha ritenuto consumata l'ipotesi di reato sub A), contestata invece come tentata. Quanto a tutte le condotte sub B), il tribunale non aveva motivato in modo soddisfacente la sussistenza dei gravi indizi sul fine di profitto, sull'utilizzo, o

almeno sul tentato utilizzo, delle credenziali di autorità politiche e militari, sulle notizie riservate illecitamente acquisite.

21. Il quarto motivo denuncia gli stessi vizi in ordine alle esigenze cautelari. Quanto al pericolo di inquinamento delle prove, il sequestro di tutto il materiale informatico e digitale e la disconnessione dalla rete dei *server* esteri rende non concreto né attuale tale pericolo, pur in presenza della già avvenuta distruzione, da parte dell'indagato, di parte del materiale esfiltrato. Del pari non ricorrente è il pericolo di reiterazione del reato a seguito della privazione dell'intera, complessa attrezzatura informatica, non facilmente e non rapidamente sostituibile, così come quello di fuga, basato sulla sola residenza a Londra, nonostante il rifiuto di un'offerta di lavoro all'estero.

22. Con memoria depositata il 24 scorso il difensore di Occhionero ha insistito nel secondo motivo di ricorso e in particolare nella questione se l'art. 266-*bis* cod. proc. pen. sia applicabile anche ai flussi di dati ed informazioni che non intercorrono tra più sistemi informatici ma tra componenti dello stesso sistema informatico.

### **CONSIDERATO IN DIRITTO**

1. La prima questione, comune ai due ricorsi, relativa all'assenza di autonoma valutazione da parte del Giudice per le indagini preliminari degli indizi e delle esigenze cautelari, è infondata per le ragioni indicate nell'ordinanza impugnata.

2. In primo luogo occorre contestare l'assunto dei ricorrenti secondo il quale la motivazione *per relationem*, di cui non negano la legittimità, sarebbe qualcosa di ontologicamente e radicalmente diverso della motivazione mediante 'copia e incolla', attuata nella specie dal Giudice per le indagini preliminari.

3. La prima è infatti integrata dal richiamo ad un altro atto, collegato a quello che si redige, che in tal modo entra sostanzialmente a farne parte, la seconda se ne differenzia solo perché la parte di atto richiamata entra a far parte, anche fisicamente grazie ai progressi dell'informatica, di quello richiamante, con il risultato pratico che il lettore ha anche visivamente dinanzi il contenuto dell'atto richiamato.

4. Ciò posto, quello che necessita ai fini dell'adempimento dell'obbligo di autonoma valutazione degli indizi e delle esigenze cautelari, introdotto all'art. 292, comma primo, lett. c), cod. proc. pen., dalla legge 16 aprile 2015, n. 47, ad esplicitazione, peraltro, di un principio immanente al sistema, è che il giudice della cautela mostri di aver preso pienamente cognizione degli elementi indiziari e delle esigenze cautelari esposti dal pubblico ministero e ne faccia oggetto di una propria, originale, verifica di gravità quanto ai primi, di attuale sussistenza quanto alle seconde.

5. Se dunque l'autonomia della valutazione ad opera del giudice della cautela, introdotta dalla novella, impone di esplicitare, indipendentemente dal richiamo in tutto o in parte di altri atti del procedimento, anche se effettuato con la tecnica del c.d.

copia-incolla (Sez. 6, n. 51936 del 17/11/2016, Aliperti, Rv. 268523), i criteri adottati a fondamento della decisione, senza nondimeno implicare la necessità di una riscrittura "originale" degli elementi o circostanze rilevanti ai fini dell'applicazione della misura (Sez. 6, n. 13864 del 16/03/2017, Marra, Rv. 269648), appare dunque sufficiente, nel caso in esame - che si caratterizza per l'elevato tasso di tecnicismo degli elementi indiziari, la più parte dei quali (si pensi a quelli relativi alla riferibilità all'indagato della *e-mail* inviata al responsabile dei servizi di sicurezza dell'ENAV, apparentemente proveniente dall'avv. Ernesto Stajano), sono frutto di accertamenti ad alta specializzazione informatica, che il giudice abbia affermato, previa implicita valutazione critica non meramente adesiva, di condividere tali accertamenti e i loro esiti, tenuto anche conto che la difesa non ha fatto altro che contrapporvi, oltre ad un'eccezione di inutilizzabilità, i risultati di una consulenza tecnica di parte, così confermando che lo scontro fra le parti si consuma sul terreno delle verifiche tecnico-informatiche.

6. Il secondo motivo del ricorso nell'interesse di Giulio Occhionero, ulteriormente ripreso nella memoria difensiva, è infondato.

7. Non è in primo luogo condivisibile, per le ragioni già evidenziate dal tribunale, il richiamo, da parte del ricorrente, alla pronuncia delle Sezioni Unite Scurato, sia pure al solo fine di trarne indicazioni generali.

8. Secondo tale pronuncia, l'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico il quale segue i movimenti nello spazio dell'utilizzatore di un dispositivo elettronico (*smartphone, tablet, PC portatile*), è consentita nei soli procedimenti per delitti di criminalità organizzata per i quali trova applicazione la disciplina di cui all'art. 13 del D.L. n. 151 del 1991, convertito dalla senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sede di attività criminosa in atto (Sez. U, n. 26889 del 28/04/2016, Scurato, Rv. 266905).

9. Essa si riferisce, dunque, in via esclusiva, alle 'intercettazioni tra presenti'. Con la conseguenza che il supremo organo nomofilattico non solo non ha escluso la legittimità dell'uso di tale strumento captativo per le intercettazioni tra presenti nei luoghi di privata dimora dove si stia svolgendo l'attività criminosa, ma soprattutto, ed è ciò che qui rileva, non l'ha esclusa per le ulteriori forme di intercettazione, tra cui quelle telematiche ex art. 266-*bis*, cod. proc. pen.. Del resto anche il disegno di legge in corso di approvazione definitiva al momento della presente decisione, contenente la delega al governo in materia di intercettazioni, ha ad oggetto soltanto la disciplina delle intercettazioni di comunicazioni o conversazioni 'tra presenti' mediante immissione di captatori informatici in dispositivi elettronici portatili, modalità all'evidenza ritenuta la più invasiva dal momento che tali ultimi dispositivi seguono gli spostamenti dell'utilizzatore con conseguente necessità di specifica tutela dei luoghi di privata dimora.

10. Posto dunque che le Sezioni Unite Scurato si sono occupate dell'intercettazione mediante *trojan horse* soltanto nel caso di 'intercettazione tra presenti', tale decisione non riguarda la captazione che ha interessato l'Occhionero. Né sarebbe lecito trarre da quell'approdo giurisprudenziale un principio generale estensibile alle intercettazioni telematiche, che, a tacer d'altro, non sono intercettazioni caratterizzate dal doppio requisito di essere sia comunicative che tra presenti.

11. In secondo luogo l'assunto del ricorrente che nella specie non si tratterebbe di intercettazioni di flussi telematici ai sensi dell'art. 266-bis cod. proc. pen. (e cioè di dati per così dire in movimento), ma della captazione 'in tempo reale' di un 'flusso di dati' intercorso su un determinato schermo o all'interno di un supporto', con la conseguenza che sarebbero state applicabili le norme sulla perquisizione e sul sequestro, si basa, da una parte, su un dato fattuale meramente assertivo, e cioè che l'agente intrusore utilizzato nella specie fosse idoneo alla captazione dei soli dati già formati e contenuti nella memoria del *personal computer*, dall'altra sulla circostanza che nella specie sarebbero stati - comunque - captati soltanto dati di quest'ultimo tipo.

12. Tale ultima circostanza è smentita, quanto meno in parte, nell'ordinanza impugnata laddove, a contrasto della medesima doglianza prospettata con la memoria depositata dalla difesa dell'Occhionero al tribunale del riesame, riconduce le operazioni della polizia giudiziaria alla captazione in tempo reale di flussi informatici transitati sul computer dell'indagato, con acquisizione di 'dati contenuti nel computer, ovvero - congiunzione disgiuntiva *n.d.r.* - (d)i flussi informatici transitati sui dispositivi', rientrando, quest'ultima, nel concetto di intercettazione. Dal provvedimento impugnato si ricava, in altre parole, che l'agente intrusore impiegato ha captato, comunque, anche un flusso di comunicazioni, richiedente un dialogo con altri soggetti, oltre a documentazione relativa ad un flusso unidirezionale di dati confinati all'interno dei circuiti del *computer*, secondo la distinzione effettuata dalla giurisprudenza di questa Corte (Sez. 5, n. 16556 del 14/10/2009 - dep. 2010, Virruso, Rv. 246954).

13. Se così è, e non vi è ragione di dubitarne, non è necessario addentrarsi nella questione, irrilevante per quanto si osserverà subito dopo, se l'acquisizione dei dati presenti nell'*hard disk* del computer costituisca intercettazione (come ritenuto per i messaggi di posta elettronica, anche se già ricevuti o spediti dall'indagato e conservati nelle rispettive caselle di posta in entrata e in uscita, indipendentemente dal sistema intrusivo adottato dagli inquirenti, cioè tramite accesso diretto al *computer* o inserimento di un programma spia, da Sez. 4, n. 40903 del 28/06/2016, Grassi e altri, Rv. 268228), oppure se integri prova atipica (come ritenuto, allorché attraverso l'installazione di un captatore informatico, si proceda all'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati, dalla già evocata sentenza Virruso; ovvero, ancora, richieda un provvedimento di perquisizione e

sequestro (senza dire, *per incidens*, da una parte che i dati captati potrebbero essere sottoposti a sequestro, dall'altra che i provvedimenti di perquisizione e sequestro sono stati adottati, ma hanno sortito nullo o scarso esito per il comportamento ostruzionistico dei due fratelli che hanno fatto in modo - Giulio Occhionero grazie anche ad un sofisticato sistema di videosorveglianza dell'abitazione - di bloccare abilmente il funzionamento delle loro apparecchiature elettroniche, rifiutandosi poi, nell'esercizio del diritto di difesa, di fornire le relative *password* di accesso).

14. La questione, come anticipato, è irrilevante giacché spettava al ricorrente precisare, in ossequio al principio di specificità delle impugnazioni, quali dei dati captati tramite *trojan* fossero eventualmente colpiti dalla sanzione dell'inutilizzabilità e, vieppiù, chiarirne l'incidenza sul complessivo compendio indiziario già valutato, sì da potersene inferire la decisività in riferimento al provvedimento impugnato (Sez. U, n. 23868 del 23/04/2009, Fruci, Rv. 243416). Il che non risulta essere stato fatto.

15. Ciò in quanto, nella specie, le intercettazioni telematiche costituiscono una parte della provvista indiziaria che ha giustificato l'applicazione agli indagati della misura cautelare coercitiva, dal momento che, ad esempio, la contestazione sub A) - e cioè il tentativo di accesso alla casella di posta del responsabile della sicurezza dell'ENAV tramite l'invio di una *e-mail* (con allegato il *malware*) di apparente provenienza dall'avv. Ernesto Stajano - fonda su accertamenti tecnici che, a quanto risulta dall'ordinanza impugnata, e dal provvedimento genetico delle misura, a partire da pag. 6, sono stati effettuati dalla Mentat Solutions srl, su iniziale incarico del dr. Di Maio, destinatario della *e-mail* infetta, in modo autonomo rispetto agli esiti delle captazioni effettuate mediante agente intrusore sul computer di Occhionero.

16. Altra parte del materiale indiziario è poi rappresentata dalle intercettazioni telefoniche tra i due fratelli e tra Francesca Maria Occhionero ed un terzo, che, a loro volta, esulano completamente dalla questione di inutilizzabilità prospettata dal ricorrente.

17. Pure infondato è il terzo motivo del ricorso nell'interesse di Giulio Occhionero che investe il raggiungimento della soglia della gravità indiziaria.

18. Nell'ordinanza oggetto di impugnazione non sono ravvisabili i profili di contraddittorietà prospettati avendo la stessa, come del resto ancora più specificamente il giudice per le indagini preliminari, da un lato, ben spiegato il procedimento tecnico ricostruttivo attraverso il quale le indagini hanno individuato in Giulio Occhionero il mittente della *mail* diretta all'ENAV, ancorché opportunamente schermato tramite l'espedito del transito attraverso la rete di anonimizzazione Tor, dall'altro dato conto dell'acquisizione, nonostante il comportamento ostruzionistico dell'indagato, dell'elenco di *username* e di *password* di persone fisiche e giuridiche in suo possesso.

19. Prive di significativo rilievo sono poi le ragioni per le quali il tribunale ha ritenuto consumata l'ipotesi di reato sub A), contestata invece come tentata, posto che



tale affermazione è rimasta del tutto priva di ricadute sulla contestazione, lasciata invariata.

20. Le doglianze relative all'imputazione sub B), con le quali si ritiene non verificata la sussistenza dei gravi indizi sul fine di profitto, sull'utilizzo, o almeno sul tentato utilizzo, delle credenziali di autorità politiche e militari, sulle notizie riservate illecitamente acquisite, sono affette da estrinseca genericità dal momento che non si confrontano con i contenuti dell'ordinanza impugnata e, vieppiù, di quella genetica della misura che la integra, dalla quale risulta, a partire dalla pag. 23, la specifica indicazione di studi professionali, società di recupero crediti, enti istituzionali, il Vaticano, società di costruzioni ecc., i cui *computer* erano rimasti vittime dell'infezione e i cui dati carpiri dal *malware* inoculato da Occhionero erano stati inoltrati al PC a questi in uso e di poi inviati ai *server* dove erano immagazzinati.

21. Infondato, da ultimo, anche il quarto motivo del ricorso di Giulio Occhionero in tema di esigenze cautelari.

22. Quanto al pericolo di inquinamento delle prove, non è esatto l'assunto del ricorrente secondo il quale il sequestro di tutto il materiale informatico e digitale e la disconnessione dalla rete dei *server* esteri renderebbe non concreto né attuale tale pericolo. Invero, come evidenziato dal tribunale, avendo l'indagato già avuto modo di distruggere parte del materiale esfiltrato e tenuto conto dello spregiudicato comportamento tenuto in occasione delle perquisizioni, le sue indiscutibilmente non comuni capacità in campo informatico rendono del tutto plausibile che una dotazione informatica anche minima gli consentirebbe in concreto, come sottolineato dal giudice per le indagini preliminari, di continuare, in eventuale regime autocustodiale, a monitorare l'attività del *virus* informatico, le cui vittime, come si legge nell'ordinanza impugnata, sono state ad oggi solo in parte individuate.

23. Quanto al pericolo di reiterazione del reato, che sarebbe venuto meno a seguito della privazione della complessa attrezzatura informatica, esso, come ritenuto dal tribunale, è invece ancora concreto ed attuale, date sia le dimensioni e ripetitività nel tempo delle condotte, sia le capacità tecniche dimostrate dall'indagato anche per eludere le investigazioni utilizzando una serie di domini atti a rendere difficile l'attribuzione dell'utilizzo del *malware*, essendo meramente assertivo, e comunque non decisivo, il rilievo che la predetta attrezzatura sarebbe non facilmente e non rapidamente sostituibile.

24. La ricorrenza del pericolo di fuga, infine, è stata correttamente ancorata ad una serie di convergenti elementi, che il ricorso tenta invano di svalutare facendoli oggetto di una valutazione atomizzata, quali i perduranti contatti ed interessenze in società estere (ammessi ma non precisati in sede di interrogatorio), la residenza londinese, le plurime offerte di lavoro all'estero (come in particolare da pag. 44 del provvedimento genetico della misura), l'attivazione sulla linea telefonica in uso all'indagato dell'opzione

per l'Europa 'Tim in viaggio *full*' (l'offerta della TIM per parlare, inviare *sms* e navigare da *smartphone*, *tablet* e PC).

25. Del pari infondato il ricorso di Francesca Maria Occhionero.

26. Per quanto attiene al primo motivo, si rinvia a quanto già osservato trattando l'omologa doglianza del fratello.

27. Il secondo ed il terzo, che investono il raggiungimento della soglia di gravità indiziaria con le censure di inosservanza o erronea applicazione della legge penale e di vizio di motivazione, sono nel complesso infondati.

28. Per quanto attiene alle conversazioni telefoniche intercettate, valorizzate nel provvedimento impugnato, va premesso che, secondo la giurisprudenza di questa Corte, l'interpretazione di esse, beninteso se non travisante, è questione di fatto rimessa all'apprezzamento del giudice di merito e si sottrae al giudizio di legittimità se la valutazione risulta logica in rapporto alle massime di esperienza utilizzate (Sez. 6, n. 17619 del 08/01/2008, Gionta, Rv. 239724), potendo la censura di diritto riguardare soltanto la logica della chiave interpretativa.

29. Orbene sia il tribunale che il giudice per le indagini preliminari hanno fornito adeguata indicazione, non manifestamente illogica, delle ragioni (alle quali il ricorso si limita a contrapporre una prospettazione alternativa) per le quali il richiamo da parte di Giulio Occhionero nelle conversazioni con la sorella del 31 luglio e 8 agosto 2016, rispettivamente ai '*log* dei così nostri' (da deviare su SQL, sistema di gestione di database Microsoft), e al fatto che 'noi ce li abbiamo i server', sottintendesse la gestione anche da parte dell'indagata di imponenti dati allocati su *server*, di fatto individuati all'estero, come confermato dalla successiva telefonata della donna (il 5/10/2016, data delle perquisizioni) al tecnico del suo *Internet Provider Service* per segnalargli l'impossibilità di accesso a cartelle condivise che custodiva nel dominio *westlands.com* di Chicago – risultato collegato al dominio *hospenta.com* utilizzato per il funzionamento del *malware* da cui era possibile collegarsi al server C&C contenente i dati esfiltrati dai computer infettati -, cui 'noi accediamo' (così testualmente l'indagata) mediante *smartcard* (anche in questo caso l'uso del plurale è stato correttamente ritenuto sintomatico di condivisione della gestione e dell'utilizzo dei dati carpiri da parte dei due fratelli, quindi di concorso nei reati, considerato anche che l'indagata, come riferito in sede di interrogatorio, non svolgeva alcuna attività lavorativa).

30. Mentre l'elemento rappresentato dalla mancata collaborazione da lei prestata in occasione delle perquisizioni (tanto a casa della madre che a casa sua, dove faceva in modo di bloccare il funzionamento dei computer negando poi l'indicazione delle *password* e tentava di impedire la perquisizione di un box che, forzato dai vigili del fuoco, rivelava il deposito di scatoloni di documenti, in corso di esame) è stato utilizzato non già per colmare asserite lacune delle fonti indiziarie, bensì per trarne, nell'ambito di

un complessivo quadro indiziario convergente, ulteriore conferma del suo coinvolgimento nell'attività delittuosa.

31. Il quarto motivo, inerente a violazione di legge in ordine alla sussistenza delle esigenze cautelari, si espone agli stessi rilievi già svolti trattando l'omologa doglianza prospettata nel ricorso di Giulio Occhionero, solo dovendo aggiungersi che il tribunale non ha confuso continuità della condotta criminosa con attualità della stessa, in quanto, se è vero che l'invio della *e-mail* inviata all'ENAV da Giulio Occhionero risale al gennaio 2016, questo attiene al solo capo A), mentre i reati sub B) sono stati contestati come tuttora in atto.

32. Quanto poi all'asserita cessazione del pericolo di inquinamento delle prove - inquinamento di fatto già concretamente posto in essere da Giulio Occhionero tramite cancellazione di alcuni dati esfiltrati -, per effetto dei sequestri dei *server* eseguiti oltreoceano e dello scollegamento di essi dalla rete, valgono le considerazioni già svolte trattando l'altro ricorso.

33. Il quinto motivo è manifestamente privo di fondamento in quanto il termine di durata della misura va indicato solamente quando il pericolo di inquinamento sia il solo ritenuto, mentre per l'indagata è stato ritenuto anche quello di recidivanza.

34. Al rigetto dei ricorsi segue il carico delle spese per ciascuno degli impugnanti.

#### **P.Q.M.**

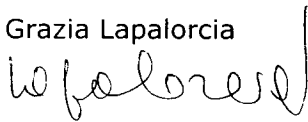
Rigetta i ricorsi e condanna ciascun ricorrente al pagamento delle spese processuali.

Manda alla Cancelleria per gli adempimenti di cui all'art. 94 comma 1-ter disp. att. cod. proc. pen..

Così deciso il 30/05/2017

Il Consigliere estensore

Grazia Lapalorcia



Il Presidente

Paolo Antonio Bruno

