AGG 1

2

# ORDINE EUROPEO DI INDAGINE (OEI)

Il presente OEI è stato emesso da un'autorità competente. L'autorità di emissione certifica che l'emissione del presente OEI è necessaria e proporzionata ai fini del procedimento in esso specificato, tenendo conto dei diritti della persona sottoposta alle indagini o dell'imputato, e che gli atti di indagine richiesti avrebbero potuto essere disposti alle stesse condizioni in un caso interno analogo. Si chiede il compimento dell'atto o degli atti di indagine indicati di seguito, tenendo in debito conto la riservatezza dell'indagine, e il trasferimento delle prove acquisite in esito all'esecuzione dell'OEI.

**SEZIONE A:**
Stato di emissione: **ITALIA**
Stato di esecuzione: **FRANCIA**

**SEZIONE B: Urgenza**
Si prega di indicare se sussiste un'urgenza dovuta:
X ad occultamento o distruzione di prove;
□ all'imminenza della data del processo;
X ad altri motivi

Precisare:

I termini di esecuzione dell'OEI sono stabiliti nella direttiva 2014/41/UE. Tuttavia, se è necessario un termine più breve o specifico, si prega di indicare la data e di spiegarne il motivo:

*Quest'Ufficio di Procura sta dirigendo e coordinando delicate indagini attieni ad un traffico internazionale di sostanze stupefacenti che interessa famiglie di 'ndrangheta operanti sia sulla fascia tirrenica sia sulla fascia ionica della Provincia di Reggio Calabria con ramificazioni anche in Sud America.*

*Le evidenze investigative hanno consentito di addivenire all'individuazione e alla compiuta identificazione di diversi soggetti operativi all'interno dello scalo portuale di Gioia Tauro incaricati del recupero e della successiva esfiltrazione dal sedime portuale di tonnellate di cocaina proveniente dal Sudamerica e destinata alle principali famiglie di 'ndrangheta del territorio; a riscontro di ciò, dal[redacted] sono stati sequestrati [redacted] chilogrammi di cocaina oggetto di recuperi non andati a buon fine.*

*Le attività sinora svolte hanno consentito di individuare, tra l'altro, alcune utenze telefoniche associate a codici IMEI di particolare interesse investigativo in quanto dedicate alle comunicazioni riservate effettuate mediante l'utilizzo di sistemi criptati, sia specifici IMSI/IMEI relativi ad altri dispositivi sicuramente utilizzati da altri indagati facenti parte della medesima organizzazione criminale, sicuramente riconducibili alla piattaforma SKY ECC in quanto, a seguito della diffusione della notizia della violazione della piattaforma da parte delle law enforcement agencies, gli indagati hanno interrotto l'utilizzo di detti apparati.*

*Nel corso delle indagini, inoltre, è stata certificata l'esistenza ed operatività di almeno un'altra squadra di operatori portuali infedeli incaricati del recupero e della successiva esfiltrazione dello stupefacente dal medesimo sedime portuale.*

*L'urgenza di ricevere le richieste informazioni è connessa al fatto che le indagini in rassegna sono tuttora in corso e che, attesa la violazione della piattaforma SKY ECC, gli indagati potrebbero occultare e/o distruggere le prove connesse agli accertati traffici illeciti, ovvero darsi alla fuga.*

**SEZIONE C:** Atto o atti di indagine da compiere

1. Si prega di descrivere l'assistenza/l'atto o gli atti di indagine oggetto della richiesta e di indicare, se del caso, se si tratta di uno degli atti di indagine seguenti:

   *Per quanto precede, accertato che gli indagati hanno utilizzato sistemi criptati - riconducibili alla piattaforma SKY ECC - per le comunicazioni relative agli illeciti traffici di sostanza stupefacente, al fine di acquisire ulteriori utili elementi investigativi, è di particolare importanza per questo Ufficio acquisire ogni eventuale informazione in possesso in ordine*

3

*ai target di seguito riportati (anche con riferimento a tutte le comunicazioni in entrata/uscita - immagini, files audio e video).*

*Si tratta, nello specifico:*

| *IMSI* | *IMEI* | *Modello Dispositivo* | *Nr. Telefonico/ Seriale SIM* | *Utilizzatore* |
|---|---|---|---|---|
| [redacted] | | | | |
| [redacted] | [redacted] | *I PHONE 7* | [redacted] | [redacted] |
| [redacted] | [redacted] | *I PHONE 7* | [redacted] | [redacted] |
| [redacted] | | | | |
| [redacted] | [redacted] | *I PHONE 7* | [redacted] | [redacted] |
| [redacted] | [redacted] | *I PHONE 7* | [redacted] | [redacted] |
| [redacted] | | | | |
| [redacted] | [redacted] | *I PHONE 7* | [redacted] | [redacted] |
| [redacted] | [redacted] | *I PHONE 8* | [redacted] | [redacted] |
| [redacted] | | | | |
| [redacted] | [redacted] | *I PHONE 7* | [redacted] | [redacted] |
| [redacted] | | | | |

*Si riportano, inoltre, i seguenti alias utilizzati dagli indagati che potrebbero corrispondere ai nick name degli utenti di detti apparati:*

- [redacted] *(potrebbe essere riferito a* [redacted]*);*
- [redacted] *(potrebbe essere riferito a* [redacted]*);*
- [redacted] *(potrebbe essere riferito a* [redacted]*);*
- [redacted]
- [redacted]
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*
- [redacted]*;*

6

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

*Atteso il ragguardevole quantitativo e le accertate modalità di trasporto/esfiltrazione, è di palmare evidenza che il relativo traffico sia gestito da un sodalizio transnazionale responsabile di diverse importazioni con consolidate ed efficienti ramificazioni in territorio sudamericano.*

*Nel corso delle indagini, inoltre, è stata certificata l'esistenza ed operatività di almeno un'altra squadra di operatori portuali incaricati del recupero e della successiva esfiltrazione dello stupefacente dal medesimo sedime portuale.*

*Pertanto, è interesse di questo Ufficio di Procura di ricevere tutte le informazioni in possesso riferite ad ogni target/operatore portuale anche se diverso da quelli sopra riportati.*

X Acquisizione di informazioni o di prove già in possesso dell'autorità di esecuzione;

**SEZIONE F:** Tipo di procedimento per il quale l'OEI è emesso:

X a) in relazione a un procedimento penale avviato da un'autorità giudiziaria, o che può essere promosso davanti alla stessa, con riferimento a un illecito penale ai sensi del diritto nazionale dello Stato di emissione; o

□ b) procedimento avviato dalle autorità amministrative in relazione a fatti punibili in base al diritto nazionale dello Stato di emissione in quanto violazioni di norme giuridiche, quando la decisione può dar luogo ad un procedimento davanti a un organo giurisdizionale competente segnatamente in materia penale; o

□ c) procedimento avviato dalle autorità giudiziarie in relazione a fatti punibili in base al diritto nazionale dello Stato di emissione in quanto violazioni di norme giuridiche, quando la decisione può dar luogo a un procedimento davanti a un organo giurisdizionale competente segnatamente in materia penale;

□ d) in connessione con i procedimenti di cui alle lettere a), b) e c) relativi a reati o violazioni per i quali una persona giuridica può essere considerata responsabile o punita nello Stato di emissione.

**SEZIONE G:** Motivi dell'emissione dell'OEI

1. Sintesi dei fatti

Si prega di fornire i motivi dell'emissione dell'OEI, compresi una sintesi dei fatti, una descrizione dei reati contestati o oggetto d'indagine, l'indicazione della fase in cui si trovano le indagini, i motivi di eventuali fattori di rischio e altre informazioni pertinenti.

*Il Gruppo Investigazione Criminalità Organizzata della Guardia di Finanza di Reggio Calabria, su delega di questo Ufficio di Procura, sta svolgendo indagini attieni ad un traffico internazionale di sostanze stupefacenti che interessa famiglie di 'ndrangheta operanti sia sulla fascia tirrenica sia sulla fascia ionica della Provincia di Reggio Calabria con ramificazioni anche in Sud America.*

5

*Le evidenze investigative hanno consentito di addivenire all'individuazione e alla compiuta identificazione di diversi soggetti operativi all'interno dello scalo portuale di Gioia Tauro incaricati del recupero e della successiva esfiltrazione dal sedime portuale di tonnellate di cocaina proveniente dal Sudamerica e destinata alle principali famiglie di 'ndrangheta del territorio; a riscontro di ciò, dal [redacted] al [redacted], sono stati sequestrati [redacted] chilogrammi di cocaina oggetto di recuperi non andati a buon fine.*

*Le attività sinora svolte hanno consentito di individuare, tra l'altro, alcune utenze telefoniche associate a codici IMEI di particolare interesse investigativo in quanto dedicate alle comunicazioni riservate effettuate mediante l'utilizzo di sistemi criptati, sia specifici IMSI/IMEI relativi ad altri dispositivi sicuramente utilizzati da altri indagati facenti parte della medesima organizzazione criminale, sicuramente riconducibili alla piattaforma SKY ECC in quanto, a seguito della diffusione della notizia della violazione della piattaforma da parte delle law enforcement agencies, gli indagati hanno interrotto l'utilizzo di detti apparati.*

*Nel corso delle indagini, inoltre, è stata certificata l'esistenza ed operatività di almeno un'altra squadra di operatori portuali incaricati del recupero e della successiva esfiltrazione dello stupefacente dal medesimo sedime portuale.*

*Pertanto, è interesse di questo Ufficio di Procura di ricevere tutte le informazioni in possesso riferite ad ogni target/ operatore portuale, anche se diverso da quelli sopra riportati.*

2. Natura e qualificazione giuridica del o dei reati per i quali è stato emesso l'OEI e disposizioni di legge applicabili: *Art. 61* bis c.p., *74 D.P.R. nr. 309 del 1990 (Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope con l'aggravante della transnazionalità, 416 bis (Associazione di tipo mafioso) del codice penale.*

3. Il reato per il quale è stato emesso l'OEI è punibile nello Stato di emissione con una pena detentiva o una misura privativa della libertà personale della durata massima non inferiore a tre anni ai sensi del diritto dello Stato di emissione e figura nell'elenco di reati di seguito riportato (contrassegnare la casella pertinente)

X partecipazione a un'organizzazione criminale;
□ terrorismo;
□ tratta di esseri umani;
□ sfruttamento sessuale dei minori e pedopornografia;
X traffico illecito di stupefacenti e sostanze psicotrope;
□ traffico illecito di armi, munizioni ed esplosivi;
□ corruzione;
□ frode, compresa la frode che lede gli interessi finanziari dell'Unione europea ai sensi della:
□ convenzione del 26 luglio 1995 relativa alla tutela degli interessi finanziari delle Comunità europee;
□ riciclaggio di proventi di reato;
□ falsificazione di monete, compresa la contraffazione dell'euro;
□ criminalità informatica;
□ criminalità ambientale, compresi il traffico illecito di specie animali protette e il traffico illecito di specie e di essenze vegetali protette;
□ favoreggiamento dell'ingresso e del soggiorno illegali;
□ omicidio volontario, lesioni personali gravi;
□ traffico illecito di organi e tessuti umani;
□ rapimento, sequestro e presa di ostaggi;
□ razzismo e xenofobia;
□ rapina organizzata o a mano armata;
□ traffico illecito di beni culturali, compresi gli oggetti d'antiquariato e le opere d'arte;
□ truffa;
□ racket e estorsione;

- ☐ contraffazione e pirateria di prodotti;
- ☐ falsificazione di atti amministrativi e traffico di documenti falsi;
- ☐ falsificazione di mezzi di pagamento;
- ☐ traffico illecito di sostanze ormonali ed altri fattori di crescita;
- ☐ traffico illecito di materie nucleari e radioattive
- ☐ traffico di veicoli rubati;
- ☐ violenza sessuale;
- ☐ incendio doloso;
- ☐ reati che rientrano nella competenza giurisdizionale della Corte penale internazionale;
- ☐ dirottamento di aereo/nave;
- ☐ sabotaggio.

**SEZIONE K:** Dati dell'autorità che ha messo l'OEI

Tipo di autorità che ha emesso l'OEI:

X autorità giudiziaria

☐ qualsiasi altra autorità competente definita dal diritto dello Stato di emissione

Denominazione dell'autorità: *Procura della Repubblica presso il Tribunale di Reggio Calabria – Direzione Distrettuale Antimafia e Antiterrorismo*
Nome del rappresentante/punto di contatto: *dott.* [redacted], *Procuratore della Repubblica*
Numero di fascicolo: [redacted]
Indirizzo: *Via Sant'Anna - Palazzo CE.DIR. - 89128 Reggio Calabria (RC)*
Numero di telefono: *+39* [redacted]
Numero di fax: *+39* [redacted]
Indirizzo di posta elettronica: [redacted]
Lingue in cui è possibile comunicare con l'autorità di emissione: *italiano*
Si prega di fornire gli estremi della o delle persone da contattare per ottenere ulteriori informazioni o per stabilire le modalità pratiche per il trasferimento delle prove, se diversi da quelli indicati sopra:
Nome/Titolo/Organizzazione: *Sost. Proc. dott.ssa* [redacted] *Procura della Repubblica presso il Tribunale di Reggio Calabria – Direzione Distrettuale Antimafia e Antiterrorismo*
Indirizzo: *// Via Sant'Anna - Palazzo CE.DIR. - 89128 Reggio Calabria (RC)*
Indirizzo di posta elettronica/Numero di telefono: *//* [redacted] *;* +39 [redacted]
Firma dell'autorità di emissione e/o del suo rappresentante che certifica l'esattezza e la correttezza delle informazioni contenute nell'OEI:

[redacted], Procuratore della Procura della Repubblica di Reggio Calabria;

[redacted] Sostituto Procuratore della Procura della Repubblica di Reggio Calabria;

Data: 13-4-21

Timbro ufficiale (se disponibile): Il Procuratore della Repubblica [redacted]

Il Procuratore della Repubblica

[redacted]

Acc 2

MINISTERO DELL'INTERNO

Direzione generale della

POLIZIA NAZIONALE

DIREZIONE CENTRALE DELLA

POLIZIA GIUDIZIARIA

SOTTODIREZIONE

per la lotta contro la Criminalità informatica e

comunicazione

Ufficio Centrale per la Lotta

Contro la criminalità legata alla tecnologia

Informazioni e Comunicazione

Nanterre, 12 giugno 2019

Il Brigardier de police LAMBOY

Guillaume in carica presso

Un

Monsieur BERTHELOT Antoine

Sostituto procuratore presso la Corte

Grande istanza di Lille

-sotto la copertura della catena di comando

**OBJET**: Partecipazione a un'associazione a delinquere finalizzata alla preparazione di un crimine o di un reato punibile con 1 O anni di reclusione (natinf: 12214), Trasporto, possesso, offerta, trasferimento, acquisizione di stupefacenti (natinf: 7995) e fornitura di servizi crittografici senza dichiarazione (natinf: 35529). Caso C/X....

**RIFERIMENTI**: Procedura N 2019/91 e relative istruzioni.

Ho l'onore di riferirLe sull'andamento delle indagini svolte dai funzionari dell'Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione (OCLCTIC), nell'ambito della procedura summenzionata, condotte in via preliminare.

## I FATTI

Nel 2016 è stata aperta un'indagine nei Paesi Bassi e in Belgio riguardante la società canadese SKYECC. Ciò includeva la fornitura di soluzioni di crittografia PGP per telefoni cellulari tramite un'applicazione e un'infrastruttura dedicate.

L'indagine è iniziata in Belgio a seguito di un caso di traffico di stupefacenti nel porto di Anvers (Anversa) con il sequestro di telefoni criptati su cui l'applicazione SKYECC è stata installata per comunicare in modo discreto. Le autorità sopra menzionate hanno quindi stabilito che l'uso della soluzione SKYECC è stato utilizzato esclusivamente per facilitare attività criminali. In particolare, sono state citate decine di fascicoli della polizia giudiziaria di Anversa relativi a organizzazioni criminali che utilizzano dispositivi SKYECC. Più di 350 numeri SKYECC sono stati coinvolti solo per l'area di Anversa. Questa cifra è salita a 1000 numeri relativi ad attività criminali in tutto il paese belgo.

Le autorità belghe hanno anche specificato che SKYECC non ha collaborato con le forze di sicurezza, dopo aver ottenuto un mandato dal giudice.

Le autorità belghe e olandesi hanno indicato che c'erano circa 68.000 utenti dell'applicazione in tutto il mondo, la maggior parte in Europa, circa 8.000 utenti in Belgio e più di 100.000 sessioni di dati al giorno.

Un elenco di casi che coinvolgono cittadini francesi che utilizzano SKYECC e che compaiono in procedimenti belgi e olandesi sarà fornito in seguito.

L'acquisto di un telefono criptato con SKYECC installato è stato effettuato dagli investigatori belgi al fine di comprendere la procedura. Ciò ha confermato la natura sospetta della vendita di prodotti SKYECC.

In effetti, era impossibile acquistare questo tipo di telefono direttamente sul sito Web SKYECC, bisognava prima mettersi in contatto via e-mail. dopo sono stati rinviati una brochure commerciale nonché l'indirizzo e-mail del rivenditore più vicino. Un appuntamento è stato allora dato, il presente caso in una retrobottega di un bar poco famoso, con uno rivenditore. Quest'ultimo accettava solo soldi contanti e non chiedeva prove di indirizzo o identificazione. Inoltre, non sono state emesse nessuna fattura o documento di vendita.

l'indagine delle autorità belghe ha stabilito che il server che ospitava le comunicazioni di SKYEC era un server Blackberry BES (Business Enterprise(ditta) Server) situato presso OVH SAS (società di hosting) a Roubaix in Francia.

A seguito dell'invio di un primo DEE (decisione dell'indagine Europea) belghe nella data 13/12/2018 alla procura del TGI ( tribunale giudiziare)di Lilla , è stata analizzata l'architettura dei server ospitati in Francia. Presso OVH si trovavano due server, il server principale, collegato direttamente a Internet, con indirizzo IP 5.135.135.94 e un server di backup con indirizzo IP: 188.165.14.8.

È stato stabilito che questi due server comunicavano tra loro tramite una rete di tipo LAN chiamata vRack di OVH.

Il 13 febbraio 2019, il pubblico ministero di Lille ha deciso di aprire un'indagine in forma preliminare riguardante SKYECC mantenendo i reati di partecipazione a un'associazione criminale per la preparazione di un crimine o un reato punibile con I 0 anni di reclusione e reato alla legislazione sui mezzi di crittografia.

## L'indagine

Inizialmente, una richiesta giudiziaria è stata inviata all'ANSSI ( l'autorità nazionale in materia di sicurezza) per confermare che nessuna richiesta di autorizzazione di mezzi e servizi di crittografia della società SKYECC era stata fatta alle autorità francesi. L'ANSSI (l'autorità nazionale in materia di sicurezza) ha confermato di non aver ricevuto tale richiesta.

Le richieste sono state quindi inviate ai quattro operatori storici per determinare se i clienti utilizzavano la soluzione SKYECC. Infatti, per poterlo utilizzare era necessario passare attraverso l'APN (Access Point Name ou relais de connection a internet ) di SKYEC. Questo APN ha modificato quello degli operatori, quindi era potenzialmente visibile a loro.

Finora, solo SFR ha risposto fornendo una tabella contenente 303 IMSI (numero di carta SIM) utilizzando l'APN SKYECC identificato.

Una ricerca negli archivi dei procedimenti giudiziari ha rivelato una trentina di casi recenti di uso di telefoni criptati PGP utilizzati nel traffico di droga e vari reati di diritto comune (rapina a mano armata in banda organizzata, veicolo in banda organizzata ...). Tuttavia, poiché il verbale non indicava in dettaglio l'applicazione utilizzata, era impossibile sapere se si trattasse di SKYECC o di un'altra applicazione concorrente.

Un elenco contenente quasi 9000 messaggi di utenti SKYECC francesi è stato fornito dalle autorità olandesi. Questo elenco proviene da scambi tra utenti SKYECC scoperti durante l'indagine olandese.

Scritti in gergo, ruotavano principalmente attorno al traffico di stupefacenti (cocaina e cannabis) e al regolamento di conti tra spacciatori. Il periodo andava dal 2016 alla metà del 2017.

A seguito di una riunione presso Europol il 27 maggio 2019 con le autorità belghe e olandesi, è stato specificato che anche le autorità statunitensi avevano aperto un'indagine riguardante SKYECC e che il loro obiettivo, in ultima analisi, era quello di interrogare i dirigenti in Canada.

Tuttavia, un tacito accordo tra le autorità americane e olandesi ha permesso di proseguire le indagini europee, sospendendo le operazioni americane alla luce dei risultati delle indagini in corso.

## ➢ REATI

- **Partecipazione a un'associazione criminale finalizzata alla preparazione di un crimine o di un reato punibile con 10 anni di reclusione (Natinf 12214):**
  Atti previsti dall'articolo 450-1 al.1 del codice penale e punibili dall'articolo 450-1 al.2 del codice penale.

- **Trasporto, possesso, offerta, trasferimento, acquisizione di stupefacenti (Natinf 7995):**

  Atti previsti e punibili dagli articoli 222-37 comma 1 del codice penale.

- **Fornitura di servizi di crittografia per garantire funzioni di riservatezza senza una dichiarazione conforme (Natinf 35529):**
  Fatti previsti dall'Art.35 titolo Iii della legge del 2004-575 del 21/06/2004., Art.31 titolo I della legge 2004-575 del 21/06/2004, Art.3 del decreto 2007-663 del 02/05/2007, Art.4 del decreto 2007-663 del 02/05/2007, Art.5 del decreto 2007-663 del 02/05/2007, Art.8 del decreto 2007-663 del 02/05/2007, Art.29 del prato 2004-575 del 21/06/2004.

Represso dall'art.35 titolo I II della l oi 2004-575 del 21/06/2004 e dall'art.35 titolo IV della l oi 2004-575 del 21.06.2004.

## CONCLUSIONE

In questa fase dell'indagine, ai sensi degli articoli 706-73-1 e 706-95 del codice di procedura penale e dell'articolo L.32 del codice delle poste e delle comunicazioni elettroniche, sembrerebbe opportuno predisporre un dispositivo di intercettazione delle comunicazioni TCP/IP in entrata e in uscita (flussi di rete) tra due server francesi gestiti da OVH, rispondendo agli indirizzi IP: 5.135.135.94 (server principale) e 188.165.14.8 (server di backup) nonché l'intercettazione sul server principale dell'indirizzo IP: 5.135.135.94 a Internet.

In effetti, per quanto riguarda la comunicazione interna (vRack) tra il server online e il server di backup, potrebbe essere una fonte significativa di informazioni, incluso se il server di archiviazione riceve chiavi di decrittografia e memorizza messaggi dagli utenti. Infine, un'intercettazione di primo livello (senza il contenuto dei pacchetti) sul server principale verso Internet consentirebbe di determinare con precisione il suo ruolo nell'implementazione della soluzione SKYECC.

IL BRIGADIERE DI POLIZIA

Aee 3

**CORTE D'APPELLO DI DOUAI**

**Giurisdizioone interregionale specializzata presso il tribunale di Lilla**

**TRIBUNALE INTERREGIONALE DI LILLE**
**PROCURA**

**RICHIESTA DI FINALITÀ**
**INTERCETTAZIONE DELLA CORRISPONDENZA**
(Intercettazione della corrispondenza **inviata tramite comunicazioni elettroniche**)

**N procura : 19043000263**

**N Jirs : JIRS 26/2019**

## IL PUBBLICO MINISTERO PRESSO IL TRIBUNALE DI LILLA

VISTA l'indagine attualmente svolta dai servizi dell'Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione (OCLCTIC) nel numero di verbali 2019/91 dei capi di:

- **partecipazione ad un'associazione criminale per la preparazione di reati e reati punibili con dieci anni di reclusione (reati di traffico di stupefacenti e reato di importazione di stupefacenti in un gruppo organizzato);**
- **violazioni della legislazione sui mezzi di crittografia;**

Atti punibili con 10 anni di reclusione e di cui agli articoli 706-73 del codice di procedura penale;

**VISTI** gli allegati e in particolare la relazione redatta tramite OCLCTIC il 12 giugno 2019;

**CONSIDERATO** che dall'indagine preliminare avviata il 13 febbraio 2019 dalla procura del JIRS di Lille sotto i suddetti riferimenti risultano i seguenti fatti:

La ricevuta del DEE rilasciata dalle autorità belghe e olandesi per i server SkyECC:

Due decisioni di indagine europea (DEE) sono state trasmesse alla Procura di Lille, nell'ambito dell'assistenza giudiziaria internazionale in materia penale, dalle autorità belghe (Procura federale del BELGIO il 21 novembre 2018) e dalle autorità olandesi (Procura nazionale di AMSTERDAM il 3 dicembre 2018), che riguardavano i mezzi di crittografia messi a disposizione dei suoi clienti da SkyECC.

Le autorità olandesi hanno indicato, nell'ambito delle rispettive indagini, che la società Sky Holding Global Inc., domiciliata in 1012-130 W Georgie St., V6E2Y3 VANCOUVER, CANADA, utilizzava a tal fine un **server Blackberry Enterprise** (BES) ospitato dal fornitore di servizi francese OVH SAS, sis. 2 rue Kellerman a ROUBAIX, con indirizzo IP 54.36.16.104.

Le autorità belghe hanno avviato un'indagine sulla stessa soluzione di comunicazione criptata SkyECC, che in precedenza aveva dimostrato sul suo sito Internet che poteva costituire una protezione contro gli interventi giudiziari e di polizia, che corrisponde agli standard di mezzi sicuri utilizzati dai criminali che agiscono nel contesto della criminalità organizzata. Le loro indagini tendevano a isolare un **server Blackberry Enterprise ospitato con il fornitore di servizi francese OVH con un indirizzo IP di 54.36.16.112.**

È quindi nell'ambito della sua competenza territoriale che le autorità belghe e olandesi hanno chiesto alla procura di Lille di ottenere, in un primo tempo , mediante richiesta dalla società OVH SAS, con sede a ROUBAIX, le informazioni richieste per l'identificazione di conti, server, macchine virtuali relative a Sky Holding o all'applicazione SkyECC.

L'OCLCTIC è stato colto dalla procura di Lilla dell'esecuzione di queste richieste di assistenza reciproca

**Utilizzo dei dati risultanti dalle decisioni investigative europee:**

Le autorità olandesi hanno osservato che, nel corso di varie indagini, membri di organizzazioni criminali, o coloro che sono coinvolti nella preparazione e nell'esecuzione di reati gravi, violenti o organizzati, hanno utilizzato regolarmente telefoni dotati di software di comunicazione sicura SkyECC.

Questa soluzione è stata fornita da un fornitore di servizi canadese che, attraverso una rete globale di distributori e rivenditori, è in grado di fornire telefoni preconfigurati con abbonamento, probabilmente pagati in modo scarsamente tracciabile e in particolare in contanti dai rivenditori o in criptovaluta (bitcoin)

La soluzione SkyECC include diversi moduli denominati PGP-email, ECC-email e ECC-chat, ECC- chat crittografati vocali, ECC-Gruppochat ,distruzione dei messaggi automatici, memopad crittografato e immagini crittografati . indicano le funzionalità e-mail, discussione istantanea, discussione di gruppo, promemoria ,chiamata vocale, immagini e messaggi di autodistruzione,

Le autorità olandesi, già incaricate di smantellare diverse altre soluzioni di crittografia utilizzate a fini criminali, hanno in questi casi, dopo aver controllato il server, effettuato chiamate agli utenti in modo che le persone che ritenevano di dover beneficiare della protezione legale della loro corrispondenza, potessero segnalarsi, chiamate che sono rimaste inascoltate, confermando la natura occulta e malvagia dell'uso di queste soluzioni.

Le autorità belghe hanno avviato un'indagine sulla nuova soluzione di comunicazione criptata SkyECC, che in precedenza ha mostrato sul suo sito web che potrebbe costituire una protezione contro gli interventi giudiziari e di polizia, che corrisponde agli standard di mezzi sicuri utilizzati dai criminali che agiscono nel contesto della criminalità organizzata.

utilizzo di dati open source:

Il funzionamento del sito web SkyECC consente la raccolta le seguenti informazioni:

- SkyECC ha messo online una versione francese del suo sito, indicando che si rivolge a una clientela francofona (https://www.skyecc.store/index fr.php?c=yes&l=fr);
- L'argomento principale è la riservatezza della soluzione di comunicazione proposta.

Immagine (SKYECC)

Pagina 3 dell'allegato in francese

- il discorso di vendita si riferisce a una soluzione di comunicazione con crittografia end-to-end - end-io-end -, reputata per resistere ai tentativi di decrittazione con la forza bruta - test esauriente di combinazioni di decrittazione mediante l'uso della potenza di calcolo -, con chiavi di crittografia solo memorizzate nel dispositivo, e dati quindi visualizzabili esclusivamente dal mittente e dal destinatario;
- è possibile fare domanda per entrare a far parte della rete di rivenditori SkyECC essendo in Francia.

dell'allegato in francese

PAGINA 3 IMMAGINE

- I recapiti disponibili sul sito per ordinare un terminale o beneficiare del supporto passano attraverso l'applicazione Wickr Messenger, a sua volta crittografata, o direttamente tramite un ID su SkyECC; la pagina dei contatti è un modulo che non fornisce i dati di contatto dell'interlocutore;
- Le soluzioni di pagamento proposte integrano effettivamente valute virtuali (Bitcoin, Ethereum) o applicazioni di trasferimento online (PayPal, bonifico bancario)
- la politica di adempimento degli obblighi di legge e in particolare di risposta alle richieste delle forze dell'ordine e dei servizi investigativi è dettagliata in una pagina esclusivamente in inglese (https://www.skyecc.store/terms-of-use.php#law-enforcement-guidelines), che avverte il lettore che le informazioni fornite sono puramente informative e che l'operatore si riserva il diritto di disporne "

**Questa guida è pubblicata solo a scopo informativo e nessuna dichiarazione deve essere interpretata come una promessa o garanzia che SKY ECC agirà in un determinato modo in risposta a una richiesta delle forze dell'ordine. SKY ECC si riserva il diritto di discostarsi dalle pratiche qui descritte qualora le circostanze lo richiedano");**

- La Società si presenta come soggetta alla legge canadese, ed in particolare alle richieste emesse e convalidate dall'autorità nazionale canadese nell'ambito delle richieste di assistenza reciproca, ma annuncia che può comunicare solo la data di creazione o ultimo utilizzo di un account identificato dal suo"ID account", esclusi i dati decifrabili e in particolare i messaggi o i dati da contenuti, dati identificativi, metadati, volumi di attività, indirizzi IP e geolocalizzazione;

- Le Condizioni d'uso prevedono che il Cliente abbia accesso e utilizzo della soluzione di crittografia per "(i) **la prevenzione di furti di identità, hacking, attacchi dannosi o spionaggio; (ii) la protezione della tua persona! diritti alla privacy; e (iii) il funzionamento sicuro della tua persona legittima! o affari commerciali, e non lontano qualsiasi** uso illecito, illegale o criminale", o che la comunicazione sicura deve proteggere da attacchi informatici, preservare la privacy o le attività lecite dell'utente, ad eccezione dell'uso illecito, illegale o criminale; tuttavia, questa visualizzazione non è accompagnata da alcun controllo efficace percepibile;

È quindi risultato che la soluzione di cifratura SkyECC presentava le caratteristiche di uno strumento utilizzato principalmente nell'ambito di attività relative alla criminalità organizzata e, in particolare, nell'ambito di applicazione degli articoli 706-73 del codice di procedura penale, e che, essendo ospitato dai server dell'OVH situati a Roubaix, il JIRS di Lilla si è dimostrato competente a indagare su tali casi.

Utilizzo di SkyECC nelle procedure già elencate:

È stato effettuato un confronto con le prove raccolte nell'ambito della procedura JIRSAC/16/2 (16105000139), relativa a una rete di importatori di farmaci tra i Paesi Bassi e la Francia, in cui è stata menzionata la tecnologia SkyECC:

D3479 - Estratto dal rapporto del JRCGN che include l'esperienza di un dispositivo Blackberry sequestrato contro uno dei sospetti durante una perquisizione in ogglomerato di Lilla

**IV-3 SIGILLO R DOM TRE**

Prendiamo in considerazione il sigillo R TRE contenente un telefono BLACKBERRY Q10 non il numero IMEI esr su: 356761055193194, cosi come una SIM card i cui numeri identificativi sono i seguenti:
Numero di identificazione della carta (ICCID):8901170425231711232 1
Numero di identificazione dell'abbonato (IMSI): 310170231711232
Nessun dato utente è presente sulla scheda SIM
Il telefono BACKBERRY Q10 essendo presupposto blocco, implementiamo un'operazione tecnica invasiva che ci permette di estrarre l'impronta crittografica della password: ox17Lb
Sal: F43ccc9EAAG0F90
Hash : 31A49D77F4CB51347550ABCONC446110518B8130E6540F06686-41126FD926-
JENG1345.621D1112FF4BIEDB225/754263854DKIEDADCJEE$DSAFF8380F625AB
SIAMO IN GRADO DI TROVARE LA PASSWORD ASOCIATA : (ZOVZOV)
Avviamo il telefono e lo sblocchiamo, troviamo un documento che contiene i seguenti informazioni :
abbiamo trovato due contatti : 0613718460,633017494
notiamo anche la presenza del'applicazione Skyecc, questa applicazione è un'applicazione di messaggistica sicura che consente la comunicazione con i corrispondenti BLACKBERRY PGP O SKYECC ,per memorizzare e trasmettere dei messaggi.

Immagini, messagi hanno una vita breve e vengono distrutti in 48 ore al massimo dopo il loro inviare o ricevere
Questi dati vengono crittografati dall'applicazione Skyecc e crittografati anche dal dispositivo Blachberry , attraverso operazioni invasive e modifiche ai dati del dispositivo .
Siamo in grado di esportare i dati dell 'applicazione senza il livello di crittografia del dispositivo copiamo i file contenente questi dati (xdb.db) su un CD che mettiamo sotto il sigillo di esperti 523/17/INL/1
La chiave segreta utilizzata per decifrare i dati contenuti nel file xdb.db (messaggi note e contatti ) e stata parzialmente cancellata , tuttavia è possibile eseguire un attacco per trovare la parte mancante e decrittografare i dati , non siamo ancora in grado di offrire questo tipo di attacco nel nostro laboratorio

*DI225 - Estratto da una conversazione intercettata telefonicamente tra un trafficante rifugiato in Marocco e suo cognato e complice rimasto in Francia, riguardante la necessità di comunicare tra due terminali dotati di SkyECC*

MAKHLOUF MOHAMED: ho detto che ho recuperato un telefono, ma non so se funziona con il tuo

CK MAROC un SKY?

MAKHLOUF Mohamud si

CK MAROC eh, no no non va bene

MAKHLOUF MOHAMED, dai, dai nel tuo ambiente , c'è qualcuno che ne ha uno ?

CK MAROC eh si vedremo , mandami il tuo indirizzo

MAKHLOUF MOHAMED dai su questo telefono?

CK MAROC cosa ?

MAKHLOUF MOHAMED ho detto , su questo telefono la ?

CK MAROC si, e tu stai bene ?

L'uso di questo mezzo di crittografia a fini criminali, da parte di soggetti desiderosi di garantire la perfetta sicurezza dei loro scambi cospirativi, potrebbe quindi essere riscontrato in un fascicolo di traffico di droga sotto la giurisdizione del JIRS di Lille, che è anche territorialmente competente al riguardo

Si può notare che data la mera natura dei terminali venduti dalla società SkyECC, questi sono destinati a rimanere molto difficili da rilevare in quanto terminali crittografati per investigatori non specializzati, essendo nascosta l'interfaccia che consente l'accesso alle funzionalità crittografate per evitare il rilevamento.

| **Necessità di una cooperazione rafforzata in materia penale** |
| --- |
| **e l'avvio di un'indagine preliminare sotto l'autorità del JJRS di LILLE:** |

In queste circostanze, al di là delle indagini svolte da altre autorità europee e dell'esecuzione degli EED, la necessità di condurre, in Francia, indagini per comprendere il fenomeno, identificare gli autori di atti commessi utilizzando questa soluzione di crittografia e gli autori di fatti legati all'esistenza di questa soluzione di crittografia.

Pertanto, e tenendo conto dei criteri di competenza precedentemente menzionati, la procura del JIRS di LILLE, con verbale delle conclusioni e del rinvio datato 13 febbraio 2019, ha aperto un'indagine preliminare sui seguenti capi d'accusa:

- **partecipazione a un'associazione a delinquere finalizzata alla 11riparazione** di **crimini e reati punibili con dieci anni di reclusione;**
- **violazioni della legislazione sui mezzi di crittologia.**

L'OCLCTIC, già responsabile dell'esecuzione dell'EED emesso dalle autorità belghe e, infine, di quello emesso dalle autorità olandesi, è stato investito di tale procedura.

| Necessità e modalità di predisposizione di un'intercettazione<br>Scambi di comunicazioni elettroniche da parte di Vaie |
| --- |

L'analisi dell'architettura tecnica dei server identificati, messa a disposizione di SkyECC dall'host OVH, ha rivelato che due server separati hanno permesso il funzionamento operativo della soluzione SkyECC:

- **il server principale, collegato direttamente a Internet, con indirizzo IP: 5.135.135.94;**
- **un server di backup con indirizzo IP: 188.165.14.8.**

È stato inoltre stabilito che questi due server comunicavano tra loro tramite una intranet di tipo LAN, corrispondente al nome commerciale di "vRack" all'interno della società OVH. Questa tecnologia chiamata "vRack", o "baia virtuale", è stata sviluppata dall'ospite OVH. Ciò consente ai prodotti OVH compatibili di essere collegati, isolati o distribuiti all'interno di una o più reti private. Il vRack offre la possibilità di comunicare server all'interno di quella che viene analizzata come una rete privata.

Immagine pagina 7

L'intercettazione degli scambi mediante comunicazione elettroniche tra questi due server è pertanto richiesta, sulla base degli articoli 706-95 del codice di procedura penale e con riguardo alle disposizioni dell'articolo L32 del codice delle poste e delle comunicazioni elettroniche, che definisce in particolare le comunicazioni elettroniche e le reti di comunicazione elettronica:

Articolo L32
Modificato dalla LEGGE n. 2016-1321 del 7 ottobre 2016 - art. 68
"I° Comunicazioni elettroniche:

Per comunicazioni elettroniche si intende l'esistenza, la trasmissione o la ricezione di segni, segnali, scritti, immagini o suoni con mezzi elettromagnetici.
2° Rete di comunicazione elettronica:
Per rete di comunicazione elettronica si intende qualsiasi impianto o insieme di mezzi di trasporto o di radiodiffusione e, se del caso, altri mezzi per la trasmissione di comunicazioni elettroniche, in particolare la commutazione e l'instradamento.
Le reti di comunicazione elettronica comprendono: le reti satellitari, le reti terrestri, i sistemi che utilizzano la rete elettrica nella misura in cui sono utilizzati per la trasmissione di comunicazioni elettroniche e le reti di diffusione o utilizzate per la distribuzione di servizi di comunicazione audiovisiva. »

## La riunione del 27 maggio 2019 sotto gli auspici di Europol

Gli investigatori dei tre paesi interessati si sono incontrati il 27 maggio 2019 a LA HAYE su iniziativa di Europol.

I due ricercatori francesi di OCLCTIC, nell'ambito degli scambi con le équipe belga e olandese, hanno ottenuto informazioni operative e tecniche sul funzionamento dei server SKY ECC, sul loro metodo di distribuzione e sull'architettura globale dell'infrastruttura tecnica.

Le autorità olandesi trasmettevano elementi di una precedente procedura denominata «PGP SAFE», in base alla quale erano stati decifrati messaggi criptati mediante questa soluzione di criptofonia smantellata in passato, e in particolare 9000 messaggi in lingua francese inviati o ricevuti dagli utenti dei terminali SKY ECC.

Il primo sfruttamento del contenuto di questi messaggi ha reso molto chiaro il sostegno all'utilizzo della soluzione SKY ECC per scopi criminali, e in particolare nel contesto del traffico di droga, tema presente nella maggior parte dei messaggi raccolti.

Dalle indagini effettuate in Belgio e nei Paesi Bassi è inoltre emerso che un processo di acquisto attraverso il sito ufficiale SKY ECC ha portato a contatti con un rivenditore e appuntamenti al di fuori di qualsiasi circuito commerciale tradizionale (incontri clandestini nei retrobottega dei bar, pagamento esclusivamente in contanti o BitCoin in particolare), tovare per il suo uso esplicito per scopi illeciti.

## Elementi ottenuti nel contesto delle inchieste francesi e prospettive attuali

L'Agenzia Nazionale per la Sicurezza dei Sistemi Informativi ANSSI è stata contattata e ha confermato che la società SKY ECC non aveva reso una dichiarazione di importazione riguardante l'utilizzo di strumenti di crittografia sul territorio nazionale.

I 4 operatori di telefonia mobile sono stati contattati per determinare la fattibilità dell'identificazione degli usi dell'APN di SKYECC. Per il momento, il solo ritorno dell'operatore SFR ha permesso di contare circa 330 utenti dell'APN.

È stato inoltre compilato un elenco di casi di telefoni cellulari crittografati PGP, principalmente in casi di traffico di stupefacenti. La difficoltà maggiore di tale censimento risiedeva nell'assenza di dati tecnici raccolti al momento dell'inserimento di tali terminali nelle procedure di cui trattasi, il che rendeva quindi impossibile sapere se il terminale fosse dotato della soluzione SKY. Ulteriori ricerche sono in corso

**SI CONSIDERA** che, nel contesto di questa indagine preliminare, sia fondamentale, al fine di individuare il proseguimento delle indagini, comprendere con precisione l'architettura tecnica dei server che consentono il funzionamento di questa applicazione consentendo a molti trafficanti di droga e organizzazioni criminali di ogni tipo di garantire la riservatezza dei loro scambi di cospirazioni;

**SI ATTENDE** pertanto che l'intercettazione

1) in primo luogo, gli scambi tra questi due server, mediante comunicazioni elettroniche;

2) dall'altro, gli scambi tra il server principale, con indirizzo IP: 5.135.135.94, e Internet;

sono essenziali per la manifestazione della verità, e in particolare per la successiva attuazione di mezzi tecnici che consentano l'attuazione della sorveglianza in tempo reale su tali server o sui terminali degli utenti;

**considerando** che le indagini tecniche abbiano stabilito che i due server affittati da SkyECC comunicano tra loro e che tali procedure operative rientrano pertanto pienamente nella definizione sia di comunicazioni elettroniche che di reti di comunicazione elettronica; che tale corrispondenza elettronica tra i due server può essere intercettata sulla base delle disposizioni dell'articolo 706-95 del codice di procedura penale;

**Considerando** che tale analisi possa essere pienamente trasposta alle comunicazioni elettroniche tra il server principale e Internet;

**Visti** le disposizioni degli articoli 100, secondo comma, 100-1 e da 100-3 a 100-8, 706-73, 706-74 e 706-95 del codice di procedura penale;

**CHIEDE** di piacere al Giudice per le libertà e la detenzione di autorizzare con ordinanza, per un periodo aggiuntivo di un mese, il Direttore dell'Ufficio centrale per la lotta alla criminalità connessa alle tecnologie dell'informazione e della comunicazione (OCLCTIC), e l'eventuale polizia giudiziaria agente che agisce sotto il suo controllo, assistito se necessario da agenti di polizia giudiziaria e ausiliari di polizia giudiziaria, nell'estensione dell'intercettazione, della registrazione e della trascrizione:

1) **comunicazioni elettroniche tra i due server situati ai seguenti indirizzi IP, che si trovano fisicamente presso l'hosting provider OVH situato a ROOBAIX:**

- il server principale, collegato direttamente a Internet, con indirizzo IP: 5.135.135.94;
- un server di backup con indirizzo IP: 188.165.14.8.

2) comunicazioni elettroniche in entrata e in uscita dal server principale dell'indirizzo IP:

5.135.135.94, fisicamente situato presso l'hosting provider OVH situato in ROBAIX

A LILLA GIUGNO 14, 2019

P/PUBILICO MINISTERO

AP. k

**CORTE D'APPELLO DI DOUAI**

**TRIBUNAL DE GRANDE ISTANZA DI LILLA**

**AUTORIZZAZIONE D'INTERCETTAZIONE, REGISTRAZIONR E TRASCRIZIONE DI CORRISPONDENZA TRASMESSA MEDIANTE COMUNICAZIONI ELETTRONICHE**

referenze : JIRS 26/2019

**Noi, Ali HAROUNE, Vicepresidente, giudice delle libertà e della detenzione presso l'Alta Corte di LILLE,**

**visti gli articoli 706-73, 706-73-1, 706-95, 100, 100-1 e da 100-3 a 100-8 del codice di procedura penale, visto l'articolo L.32 del codice delle poste e delle comunicazioni elettroniche,**

**Vista l'Indagine preliminare n°2019/91 condotta dall'Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione (OCLCTIC) dei responsabili di:**

- **-partecipazione ad un'associazione criminale per la preparazione di reati e reati, punibile con dieci anni di reclusione (reati di traffico di stupefacenti, importazione di stupefacenti da parte di un gruppo organizzato),**
- **-violazioni della legislazione sui mezzi di crittografia**

**atti punibili con una pena penale di 10 anni di reclusione e di cui agli articoli 706-73 del codice di procedura penale;**

**visto il rapporto del brigadiere di polizia LAMBOY Guillaume dell'O.C.L.C.T.I.C. del 12 giugno 2019**

**vista la richiesta del pubblico ministero presso il Tribunale di grande istanza di LILLA del 13 giugno 2013,**

La richiesta di cui sopra e il rapporto della polizia mostrano quanto segue:

A seguito di un'indagine condotta dalla polizia belga nell'ambito di un caso di traffico di droga organizzato nel porto di Anversa che ha portato al sequestro di telefoni criptati su cui è stata installata l'applicazione SKYECC per comunicare discretamente. È stato stabilito che l'uso di questa applicazione SKYECC è stato utilizzato esclusivamente per facilitare attività criminali. Decine di casi sono stati identificati dalla polizia giudiziaria di Anversa relativi a organizzazioni criminali che utilizzano dispositivi SKYECC. Le autorità belghe hanno anche specificato che SKYECC non ha collaborato con la polizia, anche dopo aver ottenuto un mandato dal giudice.

Pertanto, come parte della loro indagine, gli agenti di polizia belgi hanno acquistato un telefono crittografato utilizzando l'applicazione SKYECC installata per comprendere la procedura. Ha confermato la natura sospetta della vendita dei prodotti SKYECC. Era infatti impossibile acquistare questo tipo di telefono direttamente sul sito SKYECC. È stato prima necessario prendere contatto via e-mail. È successivamente e stata inviata una brochure commerciale insieme a un indirizzo e-mail del rivenditore più vicino. È stato poi fissato un appuntamento, in questo caso, nel retrobottega di un bar, con un rivenditore. Quest'ultimo ha

**CORTE D'APPELLO DI DOUAI**

**TRIBUNAL DE GRANDE ISTANZA DI LILLA**

**AUTORIZZAZIONE D'INTERCETTAZIONE, REGISTRAZIONR E TRASCRIZIONE DI CORRISPONDENZA TRASMESSA MEDIANTE COMUNICAZIONI ELETTRONICHE**

referenze : JIRS 26/2019

**Noi, Ali HAROUNE, Vicepresidente, giudice delle libertà e della detenzione presso l'Alta Corte di LILLE,**

**visti gli articoli 706-73, 706-73-1, 706-95, 100, 100-1 e da 100-3 a 100-8 del codice di procedura penale, visto l'articolo L.32 del codice delle poste e delle comunicazioni elettroniche,**

**Vista l'Indagine preliminare n°2019/91 condotta dall'Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione (OCLCTIC) dei responsabili di:**

- **-partecipazione ad un'associazione criminale per la preparazione di reati e reati, punibile con dieci anni di reclusione (reati di traffico di stupefacenti, importazione di stupefacenti da parte di un gruppo organizzato),**
- **-violazioni della legislazione sui mezzi di crittografia**

**atti punibili con una pena penale di 10 anni di reclusione e di cui agli articoli 706-73 del codice di procedura penale;**

**visto il rapporto del brigadiere di polizia LAMBOY Guillaume dell'O.C.L.C.T.I.C. del 12 giugno 2019**

**vista la richiesta del pubblico ministero presso il Tribunale di grande istanza di LILLA del 13 giugno 2013,**

La richiesta di cui sopra e il rapporto della polizia mostrano quanto segue:

A seguito di un'indagine condotta dalla polizia belga nell'ambito di un caso di traffico di droga organizzato nel porto di Anversa che ha portato al sequestro di telefoni criptati su cui è stata installata l'applicazione SKYECC per comunicare discretamente. È stato stabilito che l'uso di questa applicazione SKYECC è stato utilizzato esclusivamente per facilitare attività criminali. Decine di casi sono stati identificati dalla polizia giudiziaria di Anversa relativi a organizzazioni criminali che utilizzano dispositivi SKYECC. Le autorità belghe hanno anche specificato che SKYECC non ha collaborato con la polizia, anche dopo aver ottenuto un mandato dal giudice.

Pertanto, come parte della loro indagine, gli agenti di polizia belgi hanno acquistato un telefono crittografato utilizzando l'applicazione SKYECC installata per comprendere la procedura. Ha confermato la natura sospetta della vendita dei prodotti SKYECC. Era infatti impossibile acquistare questo tipo di telefono direttamente sul sito SKYECC. È stato prima necessario prendere contatto via e-mail. È successivamente e stata inviata una brochure commerciale insieme a un indirizzo e-mail del rivenditore più vicino. È stato poi fissato un appuntamento, in questo caso, nel retrobottega di un bar, con un rivenditore. Quest'ultimo ha

accettato solo contanti e non ha chiesto alcuna prova di residenza né alcun documento di identità. Nessuna fattura o documento di vendita è stato emesso.

L'indagine delle autorità belghe ha rilevato che il server che ospitava le comunicazioni di SKYEC era un server Blackberry BES (Business Enterprise Server) situato presso O.V.H. S.A.S. (società di hosting) a ROUBAIX, FRANCIA.

Pertanto, nell'ambito della sua competenza territoriale, la procura della Repubblica di Lilla è stata invitata dalle autorità belghe e olandesi ad ottenere, mediante richiesta dalla società OVH SAS, con sede in ROUBAIX, le informazioni richieste sull'identificazione di conti, server, macchine virtuali relative a Sky Holding o all'applicazione SkyECC.

La soluzione SkyECC sembrava avere le caratteristiche di uno strumento utilizzato principalmente nel contesto delle attività della criminalità organizzata.

A seguito dell'invio di una prima decisione d'inchiesta europea sul beige datata 13 dicembre

2018 presso la procura del Tribunale regionale di Lille, è stata analizzata l'architettura dei server ospitati in Francia. Sono stati individuati due server situati presso OVH: il server principale, collegato direttamente a Internet, con un indirizzo IP: 5.135.135.94 e un server di backup con un indirizzo IP: 188.165.14.8.

È stato inoltre stabilito che questi due server comunicavano tra loro tramite una intranet di tipo LAN, recante il nome commerciale di "vRack" all'interno della società O.V.H. Questa tecnologia chiamata "vRack", o "array virtuale", è stata sviluppata dall'ospite O.V.H. Consente di connettere, isolare o distribuire i prodotti OVH compatibili all'interno di una o più reti private. Il "vRack" offre la possibilità di comunicare i server all'interno di quella che viene analizzata come una rete privata.

Il 13 febbraio 2019, il pubblico ministero del T.G.I. di Lille ha deciso di aprire un'indagine preliminare riguardante la società SKYECC

Una requisizione giudiziaria è stata trasmessa all'A.N.S.S.I. al fine di verificare se una richiesta di autorizzazione di mezzi e servizi di crittografia ava.it stata effettuata dalla società SKYECC. L'agenzia non ha risposto negativamente, in quanto nessuna richiesta era stata presentata alle autorità francesi.

Le richieste sono state quindi inviate ai quattro operatori telefonici francesi per rilevare se i clienti utilizzavano la soluzione SKYECC. Infatti, per poterlo utilizzare era necessario passare attraverso l'APN (Access Point Name o relay point di connessione a internet) di SKYECC. Questa telecamera ha modificato quella degli operatori, quindi era potenzialmente visibile a loro.

L'operatore S.F.R. ha risposto gridando una tabella contenente 303 IMSI (numero di carta SIM utilizzando l'APN di SKYECC e attualmente in fase di identificazione.

Un elenco contenente quasi 9000 messaggi di utenti francesi di SKYECC è stato fornito dalle autorità olandesi, Questo elenco ha avuto origine da scambi tra utenti SKYECC scoperti durante l'indagine olandese Scritti in gergo, ruotavano principalmente attorno al traffico di stupefacenti (cocaina e cannabis) e al regolamento di conti tra "spacciatori",

Pertanto, gli investigatori desiderano predisporre un dispositivo per intercettare le comunicazioni trasmesse tramite comunicazioni elettroniche TCP/IP in entrata e in uscita (flussi di rete) tra due server francesi gestiti dalla società OVH, rispondendo agli indirizzi IP: 5.135.135.94 (server principale) e IP 188.145.14.8 (server di backup) nonché un'intercettazione sul server principale dell'indirizzo IP: 5.135.135.94 su Internet, per quanto riguarda la comunicazione interna (vRack) tra il server online e il

server di backup, questa potrebbe essere una fonte significativa di informazioni, in particolare se il server di archiviazione riceve chiavi di decrittografia e memorizza i messaggi degli utenti, e oltre determinare se SKYECC stia effettivamente utilizzando indirizzi informatici, anche se non ha presentato alcuna richiesta di autorizzazione di mezzi e servizi di crittografia. di SKYECC non è stata fusa con le autorità francesi e non beneficia di autorizzazione.

Di conseguenza, le esigenze dell'indagine richiedono che la richiesta sia accolta,

**PER QUESTI MOTIVI**

**AUTORIZZIAMO** il commissario di polizia, il direttore dell'Ufficio centrale per la lotta contro la criminalità informatica e qualsiasi ufficiale giudiziario di polizia che agisca sotto il suo controllo, assistiti se del caso da agenti di polizia giudiziaria e vice ufficiali di polizia giudiziaria, a procedere, per un periodo di un mese dalla collocazione del dispositivo, all'intercettazione, la registrazione e la trascrizione delle comunicazioni effettuate mediante comunicazioni elettroniche

1- comunicazioni elettroniche tra i due server situati agli indirizzi IP di seguito, che si trovano fisicamente presso l'ospite 0.V.R situato in ROUBAIX 59100:

- il server principale, collegato direttamente a Internet, con indirizzo IP: 5.135.135.94;
- un server di backup (" backup 11) con indirizzo IP: 188.165.14.8.

(2) comunicazioni elettroniche in entrata e in uscita dal server principale di indirizzi IP: 5 .135 .135 .94;

nonché la registrazione delle comunicazioni inviate per mezzo di comunicazioni elettroniche inviate o ricevute da questa linea e la loro trascrizione;

Diciamo che questi atti saranno compiuti sotto il nostro controllo e che saremo informati senza indugio del loro completamento da parte del pubblico ministero degli atti compiuti, in particolare dei rapporti redatti in esecuzione di questa autorizzazione, ai sensi degli articoli I00-4 e 100-5 del codice di procedura penale.

A LILLE, 14 giugno 2019

Il giudice della libertà e della detenzione

- Affinché il controllo sia reale ed efficace, informazione del giudice delle libertà e detenzione del Tribunale di grande istanza di LILLE delle diligenze effettuate nell'ambito di queste intercettazioni di corrispondenza telefonica il :

All. 5

**CORTE D'APPELLO DI DOUAI**

**TRIBUNAL DE GRANDE INSTANCE DE LILLE**

AUTORIZZAZIONE D'INTERCETTAZIONE, DI CORRISPONDENZE TELEFONICHE

( rinnovo)

referenze : JIRS 26/2019

Noi, Sandrine NORMAND, giudice delle libertà e della detenzione presso l'Alta Corte di LILLA,

visti gli articoli 706-73, 706-73-1, 706-95, 100, 100-1 e da 100-3 a 100-7del codice di procedura penale

Vista l'indagine n° 2019/91 condotta dall'Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione (OCLCTIC) dei responsabili dell'organizzazione;

- partecipazione ad un'associazione criminale per la preparazione di reati e reati, punibile con dieci anni di reclusione (reati di traffico di stupefacenti, importazione di stupefacenti da parte di un gruppo organizzato),
- violazioni della legislazione sui mezzi di crittologia,

reati di cui agli articoli 706-73 e 706-73-1 del codice di procedura penale

**visto** il rapporto della polizia del 18 luglio 2019

**vista** la richiesta del pubblico ministero di questo giorno

**La richiesta di cui sopra e il rapporto della polizia mostrano quanto segue:**

A seguito di un'indagine condotta dalla polizia belga nell'ambito di un caso di traffico di droga organizzato nel porto di Anversa che ha portato al sequestro di telefoni criptati su cui è stata installata l'applicazione SKYECC per comunicare discretamente. È stato stabilito che l'uso di questa applicazione SKYECC è stato utilizzato esclusivamente per facilitare attività criminali. Decine di casi sono stati identificati dalla polizia giudiziaria di Anversa relativi a organizzazioni criminali che utilizzano dispositivi SKYECC. Le autorità belghe hanno anche specificato che SKYECC non ha collaborato con la polizia, anche dopo aver ottenuto un mandato dal giudice.

Pertanto, come parte della loro indagine, gli agenti di polizia belgi hanno acquistato un telefono crittografato utilizzando l'applicazione SKYECC installata per comprendere la procedura. Ha confermato la natura sospetta della vendita dei prodotti SKYECC. Era infatti impossibile acquistare questo tipo di telefono direttamente sul sito SKYECC. È stato prima necessario prendere contatto via e-mail. È successivamente e stata inviata una brochure commerciale insieme a un indirizzo e-mail del rivenditore più vicino. È stato poi fissato un appuntamento, in questo caso, nel retrobottega di un bar, con un rivenditore. Quest'ultimo ha accettato solo contanti e non ha chiesto alcuna prova di residenza né alcun documento di identità. Nessuna fattura o documento di vendita è stato emesso.

L'indagine delle autorità belghe ha rilevato che il server che ospitava le comunicazioni di SKYEC era un server Blackberry BES (Business Enterprise Server) situato presso O.V.H. S.A.S. (società di hosting) a ROUBAIX, FRANCIA.

Pertanto, nell'ambito della sua competenza territoriale, la procura della Repubblica di LILLA è stata invitata dalle autorità belghe e olandesi ad ottenere, mediante richiesta dalla società OVH SAS, con sede in ROUBAIX, le informazioni richieste sull'identificazione di conti, server, macchine virtuali relative a Sky Holding o all'applicazione SkyECC.

La soluzione SkyECC sembrava avere le caratteristiche di uno strumento utilizzato principalmente nel contesto delle attività della criminalità organizzata.

A seguito dell'invio di una prima decisione d'inchiesta europea belga datata 13 dicembre 2018 presso la procura del Tribunale regionale di Lilla, è stata analizzata l'architettura dei server ospitati in Francia. Sono stati individuati due server situati presso OVH: il server principale, collegato direttamente a Internet, con un indirizzo IP: 5.135.135.94 e un server di backup con un indirizzo IP: 188.165.14.8.

È stato inoltre stabilito che questi due server comunicavano tra loro tramite una intranet di tipo LAN, recante il nome commerciale di "vRack" all'interno della società O.V.H. Questa tecnologia chiamata "vRack", o "array virtuale", è stata sviluppata dall'ospite O.V.H. Consente di connettere, isolare o distribuire i prodotti OVH compatibili all'interno di una o più reti private. Il "vRack" offre la possibilità di comunicare i server all'interno di quella che viene analizzata come una rete privata.

Il 13 febbraio 2019, il pubblico ministero del T.G.I. di Lille ha deciso di aprire un'indagine preliminare riguardante la società SKYECC

Una requisizione giudiziaria è stata trasmessa all'A.N.S.S.I. al fine di verificare se una richiesta di autorizzazione di mezzi e servizi di crittografia ava.it stata effettuata dalla società SKYECC. L'agenzia non ha risposto negativamente, in quanto nessuna richiesta era stata presentata alle autorità francesi.

Le richieste sono state quindi inviate ai quattro operatori telefonici francesi per rilevare se i clienti utilizzavano la soluzione SKYECC. Infatti, per poterlo utilizzare era necessario passare attraverso l'APN (Access Point Name o relay point di connessione a internet) di SKYECC. Questa telecamera ha modificato quella degli operatori, quindi era potenzialmente visibile a loro.

L'operatore S.F.R. ha risposto gridando una tabella contenente 303 IMSI (numero di carta SIM) utilizzando l'APN di SKYECC e attualmente in fase di identificazione.

Un elenco contenente quasi 9000 messaggi di utenti francesi di SKYECC è stato fornito dalle autorità olandesi, Questo elenco ha avuto origine da scambi tra utenti SKYECC scoperti durante l'indagine olandese Scritti in gergo, ruotavano principalmente attorno al traffico di stupefacenti (cocaina e cannabis) e al regolamento di conti tra "spacciatori",

Con ordinanza del giudice delle libertà e della detenzione del 14 giugno 2019 è stato autorizzato un provvedimento di intercettazione di comunicazioni elettroniche su:

• scambi mediante comunicazioni elettroniche tra il server principale, collegato direttamente

internet, con indirizzo IP: 5.135.135.94, e il server di backup con indirizzo IP:

188.165.14.8;

• comunicazioni in entrata e in uscita dal server principale, indirizzo IP: 5.135.135.94.

Tali controlli tecnici sono stati posti in essere il 24 e 26 giugno 2019.

Nell'ambito di questo primo periodo di intercettazione, e dopo scambi tecnici con autorità estere su decisione o autorizzazione investigativa europea presa sulla base dell'articolo 695-9-31 e seguenti ed in particolare dell'articolo 695-9-40 del codice di procedura penale, gli inquirenti potrebbero effettuare i rilievi esposti nella relazione del 18 luglio ed in particolare il seguente:

è stata confermata una significativa densità di traffico, con, su un campione di 25 ore, la creazione di cento nuovi account, quasi 500.000 messaggi inviati e quasi un milione di messaggi cancellati;

i messaggi degli utenti e i metadati associati potevano essere visualizzati ma rimanevano crittografati;

I dati "in chiaro" hanno invece consentito di rivelare attivazioni di account, richieste SQL al database Sky ECC relative a modifiche degli account utente o aggiunte di chiavi di crittografia, per iniziare a comprendere l'architettura informatica della soluzione di crittografia con l'aggiornamento di base chiamato esplicitamente "client", "msg", "contatto" e per collegare gli identificatori utenti rilasciati da Sky ECC con numeri IMEI identificativi del terminale.

Questo primo sfruttamento ha quindi confermato l'uso massiccio della soluzione di crittografia Sky ECC, ha permesso di percepirne l'architettura, presupposto necessario per l'implementazione di procedure di decrittazione e/o nuove indagini informatiche, e ha rivelato l'assenza di dati utili all'identificazione degli utenti della domanda, la maggior parte delle quali era stata confermata da precedenti indagini come illegittima. Gli inquirenti desiderano quindi proseguire le intercettazioni e le esigenze dell'indagine giustificano l'accoglimento della loro richiesta.

**Per questi motivi**

AUTORIZZIAMO il Sig. Direttore dell'Ufficio Centrale per la Lotta alla Criminalità legata alle Tecnologie di Informazione e Comunicazione (OCLCTIC) e qualsiasi agente di polizia giudiziaria che agisca sotto il suo controllo, eventualmente assistito da agenti di polizia giudiziaria e ausiliari di polizia giudiziaria, secondo quanto previsto dagli articoli 706-73, 706 -73-1, 706-95, 100, 100-1 e da 100-3 a 100-7 cpp, di procedere, per un ulteriore periodo di un mese (legge 0°2011-267 del 14 marzo 2011) dalla fine del primo periodo di l'installazione dell'intercettazione, sull'intercettazione, registrazione e trascrizione:

1) comunicazioni elettroniche che avvengono tra i due server ubicati ai seguenti indirizzi IP, che sono fisicamente ubicati presso l'host OVH situato in ROUBAIX:

- il server principale, collegato direttamente a Internet, con indirizzo IP: 5.135.135.94;
- un server di backup (" backup 11) con indirizzo IP: 188.165.14.8.

(2) comunicazioni elettroniche in entrata e in uscita dal server principale di indirizzi IP: 5 .135 .135 .94; impiantato fisicamente con l'ospite OVH con sede a Roubaix,

DICIAMO che questi atti saranno compiuti sotto la nostra autorità e il nostro controllo e che saremo informati senza indugio del loro compimento dal Pubblico Ministero.

Fatto a Lilla il 22 luglio 2019

Il giudice della libertà e della detenzione

D.193

**CORTE D'APPELLO DI DOUAI**

**Tribunale de Grande Instanza di Lilla**

**Ufficio di Valérie CULIOLI**

**Giudice istruttore**

N Procura: 19043000263

Istruzione n.: JI CJIRSBC19000006

Giustizia ID: 1900451491T

valerie.culioli@justice.fr

25 ott 2019

Il Cancelliere Esperto
Dr.ssa Katia Incognito

**COMMISIONE ROGATORIA**

**INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA N3**

Noi, Valérie CULIOLI, giudice istruttore, siamo nel nostro ufficio presso il Tribunale di Grande Instanza di Lilla, Viste le informazioni fornite contro:

X

Accusato per i reati : FORNITURA DI UN MEZZO DI CRITTOLOGIA CHE NON GARANTISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE fatti commessi nel mese di gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e alle partenze di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I I, ART.30 §III. ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3. ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §1 I, §IV LEGGE 2004-575 DEL 2 L/06/2004.

IMPORTAZIONE DI UN MEZZO DI CRITTOLOGIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1 °, ART.30 §III, ART.29 LEGGE 2004-575 DEL 2 I /06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §1 1 °, §IV LEGGE 2004-575 DEL 21/06/2004.

FORNITURA DI SERVIZI DI CRITTOLOGIA PER GARANTIRE LA RISERVATEZZA DELLE FUNZIONI SENZA VERA DICHIARAZIONE fatti fatti nel gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §111, ART.31 §1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §111, §IV LEGGE 2004-575 DEL 21/06/2004.

**PARTECIPAZIONE A COSPIRAZIONE SUI CRIMINALI PER LA PREPARAZIONE DI UN CRIMINE PUNI 10 ANNI DI RECLUSIONE** FATTI COMMESSI DURANTE IL 20 GENNAIO 18 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE.

previsto dall'ART.450-1 AL. I, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE.

**PARTECIPAZIONE AD UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN REATO** atti commessi durante il 20 gennaio 2018e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL. I, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 Cod.PENALE.

VISTI gli articoli 18, 81, 100, 100-1, 100-3, 100-8, 151 e seguenti del codice di procedura penale

Premesso che le indagini in corso fanno sorgere il sospetto che gli utenti delle soluzioni criptate fornite da **SkyECC**, i cui dati di utilizzo transitano attraverso i server messi a disposizione da **OVH**, partecipino alla commissione di reati punibili con la reclusione di almeno tre anni, in questo caso gli atti di associazione a delinquere finalizzati in particolare alla preparazione di reati importazione di stupefacenti da parte di un gruppo organizzato e reati punibili con dieci anni di reclusione, compresi l'acquisizione, la detenzione, il trasporto e il trasferimento di stupefacenti, reati connessi alla legislazione vigente,

considerando che i due server affittati da SkyECC a OVH comunicano tra loro, il server principale comunica anche con Internet, queste procedure operative costituiscono comunicazioni elettroniche e reti di comunicazione elettronica che possono essere soggette ad intercettazione sulla base delle suddette disposizioni di legge,

considerando che dalle indagini svolte in particolare dalle autorità belghe e olandesi risulta che gli utenti della soluzione SkyECC si scambiano in modo particolarmente criptato le modalità di acquisizione, trasporto di stupefacenti (Cocaina,resina di cannabis), armi a livello internazionale,

considerando che una relazione comunicata dalle autorità belghe in seguito allo sfruttamento dei dati dell'intercettazione delle comunicazioni autorizzate nell'ambito dell'indagine preliminare conferma l'utilizzo da parte degli attori delle organizzazioni criminali delle soluzioni SkyECC, in particolare evidenziando identificatori e gruppi legati ad attività criminali, "El chapo(capo) è tornato" "Generale in armi", gruppi relativi al recupero e al trasporto di stupefacenti

Dato che le intercettazioni attualmente in corso non consentono di intercettare l'intero traffico Internet come previsto nella misura di intercettazione, che solo il 50% delle comunicazioni effettuate utilizzando telefoni criptati SkyECC non sono soggetti all'intercettazione , che un filtro messo in atto da ELEKTRON non permette l'intercettazione di tutto il traffico di rete esterne in entrata e in uscita verso il server identificato a OVH dall'IP, che le viene quindi richiesto una intercettazione della totalità delle comunicazioni in entrata e in uscita del server identificato presso OVH con il suo nome ns62400.ip-5-l 35-135.eu,

Considerando che l'attuazione di questa nuova intercettazione delle comunicazioni appare da allora necessaria per manifestazione della verità al fine di proseguire le indagini sull'architettura dei server, sulle comunicazioni di dati relativi alle organizzazioni criminali, di raccogliere elementi (prove) e identificare le squadre criminali utilizzano la soluzione SkyECC, tali intercettazioni appaiono proporzionate alla gravità dei fatti associazione criminale ai fini della preparazione di un procedimento e di reati punibili con dieci anni di reclusione oggetto del presente procedimento,

essendo nell'impossibilità di procedere noi stessi gli atti necessari allegati,

Diamo commissione regatoria a:

Signor Direttore dell'Ufficio centrale contro la criminalità in relazione alle tecnologie dell'informazione e della comunicazione

101 rue des trois Fontanot

92000 Nanterre

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà trasmesso nel modo più tempestivo, entro il 15 maggio 2020

Faie nel nostro ufficio, 13 dicembre 2019

Il giudice istruttore

Valèrie Culioli

## MISSIONE

Ho l'onore di chiederLe di effettuare tutte le richieste necessarie per intercettare, registrare e trascrivere le comunicazioni esterne in entrata e in uscita del server identificato presso OYH con il suo nome ns62400.ip-5-l 35-l 35.eu. per un periodo di **quattro mesi** decorrere dal 13 dicembre.

2019 fino al 13 aprile 2020

Redigerai un rapporto di ciascuna delle operazioni di intercettazione e registrazione, il suddetto rapporto menzionando la data e l'ora In cui l'operazione è iniziata e quelli in cui si è conclusa.

Ci informerai regolarmente dell'evoluzione della vostra missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

Fatto nel nostro ufficio, questo 13 dicembre 2019

Il giudice istruttore

Giudice istruttore VALèRIE CULIOLI

COUR D'APPEL DE DOUAI

**TRIBUNALE DI GRANDE ISTANZA DI LILLA**

**Ufficio di Valérie CULIOLI**

**Giudice**

N° Procura: 19043000263

N° istruzione: JI CJIRSBC19000006

identificatore di giustizia: 1900451491T

valerie.culioli@justice.fr

Il Cancelliere Esperto
Dr.ssa Katia Incognito

**COMMISSIONE ROGATORIA**

**INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA**

Noi, Valèrie CULIOLI , giudice istruttore siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

- **FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §III, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §III, §IV LEGGE 2004-575 DEL 21/06/2004.

-PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLA

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENALE.

**-FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §II , ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §II°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ**

**SENZA PREVIA DICHIARAZIONE** fatti commessi durante gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §II, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

**e punito dall'ART.35 §III, §IV LEGGE 2004-575 DEL 21/06/2004.**

**-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE** commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FRANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

considerando che le indagini svolte nell'ambito di tale indagine giudiziaria consentono di sospettare che gli utenti delle soluzioni criptate fornite da SkyECC, i cui dati di utilizzi passano attraverso i server(softwar) messi a disposizione dalla società OVH, partecipino alla commissione di reati punibili con una pena detentiva di almeno tre anni, nella fattispecie atti di associazione a delinquere finalizzati in particolare alla preparazione di reati particolarmente l'importazione di stupefacenti da parte di una banda organizzata e di reati punibili con la reclusione di dieci anni, compresi l'acquisizione, la detenzione, il trasporto e il trasferimento di stupefacenti, nonché i reati connessi alla legislazione sulle armi,

Considerando che i due server noleggiati dalla società SkyECC a OVH comunicano tra loro, che il server principale comunica anche con la rete Internet, tali modalità di funzionamento costituiscono comunicazioni elettroniche e reti di comunicazione elettronica che possono essere oggetto di intercettazione sulla base della citata legge disposizioni,

considerando che le indagini svolte in particolare dalle autorità belghe e olandesi dimostrano che gli utenti della soluzione SkyECC si scambiano in modo crittografato, in particolare sui termini di acquisizione. trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale,

Considerando che un rapporto comunicato dalle autorità belghe a seguito dello sfruttamento dei dati provenienti dall'intercettazione di comunicazioni autorizzate nell'ambito dell'indagine preliminare conferma l'utilizzo da parte degli attori delle organizzazioni criminali delle soluzioni SkyECC in particolare evidenziando identificatori e gruppi dc legati ad attività criminali, " El capo è tornato" "Generale in armi ", gruppi relativi al recupero, al trasporto di stupefacenti,

Considerando che le intercettazioni attualmente in corso non consentono dl intercettare tutto il traffico Internet previsto dal provvedimento di intercettazione, che solo il 50% delle comunicazioni effettuate con telefoni criptati SkyECC non sono soggette all'intercettazione, che un filtro posto in place by ELEKTRON non permette di intercettare tutto il traffico di rete esterna in entrata e in uscita verso il server identificato in OVH dall'IP, che è quindi richiesta un'intercettazione dc tutte le comunicazioni in entrata e in uscita dal server identificato in OYH dal suo nome ospite ns62400 .ip-5-l 35-135.eu, che si richiede inoltre di garantire l'intercettazione di tutti i dati e l'intercettazione delle comunicazioni esterne in entrata e in uscita dal server di backup identificato con il suo nome ospite ns6019808.ip-l 88-165- 14.eu,

considerando che l'attuazione di intercettazioni sui server utilizzati finora ha permesso di fornire ulteriori elementi di analisi utili alla manifestazione della verità, che l'attuazione di un'intercettazione delle comunicazioni sul traffico operato dal nuovo server appare pertanto necessaria per la manifestazione della verità al fine di proseguire le indagini sull'architettura dei server, sulla comunicazione di dati relativi a organizzazioni criminali, per raccogliere prove e identificare squadre criminali utilizzando la soluzione

SkyECC, tali intercettazioni appaiono proporzionate alla gravità degli atti di associazione a delinquere ai fini della preparazione di reati e reati punibili con dieci anni di reclusione oggetto del presente procedimento,

Non essere in grado di eseguire da soli gli atti necessari allegati,

Diamo rogatoria al Sig. Direttore

A:

Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione

106 RUE DES TROIS FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato al più presto, entro il 15 maggio2020

Fatto nel nostro ufficio, questo 10 gennaio 2020

Giudice istruttore

Valèrie CULIOLI

## INCARICO

Ho l'onore di chiedervi di procedere con tutte le richieste necessarie per procedere all'intercettazione, registrazione e trascrizione delle comunicazioni esterne in entrata e in uscita dal server identificato presso OYH dal suo nome ospite ns6019808.ip -188-165-14.eu per un periodo di tre mesi dal 13 gennaio 2020, ovvero fino al 13 aprile 2020.

Lei redigerà un verbale di ciascuna delle operazioni di intercettazione e registrazione, in detto verbale indicando la data e l'ora in cui l'operazione è iniziata e quelle in cui è terminata.

Ci informerai regolarmente dello stato di avanzamento della tua missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

Fatto nel nostro ufficio, 10 gennaio 2020

Giudice istruttore VALèRIE CULIOL

**Corte d'appello di DOUAI**

**CORTE DI GIUSTIZIA DI LLLE**

**Ufficio di VALèRIE CULIOLI**

**Vicepresidente incaricato delle indagini**

25-09-2019
15'7

Il Cancelliere Esperto
Dr.ssa Katia Incognito

Parquet 19043000263

Istruzioni: JI CJIRSBC19000006

Identificatore di giustizia: 1900451491T

**COMMISSIONE ROGATORIA**

**INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA**

Noi , Valèrie CULIOLI , giudice istruttore siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

**- FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §Iii, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §Iii, §IV LEGGE 2004-575 DEL 21/06/2004.

**-PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE** fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE.

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENALE.

**-FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §1 1 °, ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ**

**SENZA PREVIA DICHIARAZIONE** fatti commessi durante J anvier 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e **punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.**

**-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE** commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FRANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

considerando che le indagini svolte nell'ambito di tale indagine giudiziaria consentono di sospettare che gli utenti delle soluzioni criptate fornite da SkyECC, i cui dati di utilizzi passano attraverso i server(softwar) messi a disposizione dalla società OVH, partecipino alla commissione di reati punibili con una pena detentiva di almeno tre anni, nella fattispecie atti di associazione a delinquere finalizzati in particolare alla preparazione di reati particolarmente l'importazione di stupefacenti da parte di una banda organizzata e di reati punibili con la reclusione di dieci anni, compresi l'acquisizione, la detenzione, il trasporto e il trasferimento di stupefacenti, nonché i reati connessi alla legislazione sulle armi,

considerando che è stato accertato che i due server inizialmente affittati da SkyECC a OVH comunicano tra loro e che il server principale comunica anche con Internet; che tali procedure operative costituiscono reti di comunicazione elettronica e di comunicazione elettronica e sono state intercettate sulla base delle summenzionate disposizioni giuridiche,

Che queste misure di intercettazione sono state successivamente rinnovate dal magistrato inquirente;

considerando inoltre che le indagini svolte in particolare dalle autorità olandesi hanno dimostrato che gli utenti della soluzione SkyECC si scambiavano in modo criptato, in particolare per quanto riguarda le modalità di acquisizione, trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale,

considerando che una relazione comunicata dalle autorità olandesi in seguito allo sfruttamento dei dati dell'intercettazione delle comunicazioni autorizzate nell'ambito dell'indagine preliminare ha confermato l'utilizzo da parte di attori di organizzazioni criminali di soluzioni SkyECC, in particolare evidenziando identificatori e gruppi legati ad attività criminali, "El chapo è tornato" "Generai in armi", gruppi relativi al recupero e al trasporto di stupefacenti;che le autorità belghe confermano l'intercettazione di questi dati necessari al fine di poter comprendere l'architettura dei server e la loro comunicazione .

considerando che il proseguimento delle intercettazioni poste in essere appare quindi necessario per la manifestazione della verità per proseguire le indagini sull'architettura dei server, sulle comunicazioni di dati relativi alle organizzazioni criminali. per raccogliere prove e identificare squadre criminali utilizzando la soluzione SkyECC, tali intercettazioni appaiono proporzionate alla gravità degli atti di associazione a delinquere ai fini della preparazione di reati e reati punibili con dieci anni di reclusione oggetto del presente procedimento in corso .

essere nell'impossibilità di eseguire noi stessi gli atti necessari allegati,

Diamo commissione rogatoria al Sig. Direttore

A:

Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione

106 RUE DES TROIS FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato al più presto, entro il 30 aprile 2020

Fatto nel nostro ufficio, 19 febbraio 2020

Giudice istruttore **VALèRIE CULIOLI**

(8) 3

**Corte d'appello di DOUAI**

**CORTE DI GIUSTIZIA DI LLLE**

**Ufficio di VALèRIE CULIOLI**

**Vicepresidente incaricato delle indagini**

25-10-2021

Parquet 19043000263

Istruzioni: JI CJIRSBC19000006

Identificatore di giustizia: 1900451491T

Il Cancelliere Esperto
Dr.ssa Katia Incognito

**COMMISSIONE ROGATORIA**

**INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA**

Noi , Valèrie CULIOLI , giudice istruttore siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

**- FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §Iii, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §Iii, §IV LEGGE 2004-575 DEL 21/06/2004.

**-PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE** fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE.

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENALE.

**-FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §1 1 °, ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ**

**SENZA PREVIA DICHIARAZIONE** fatti commessi durante J anvier 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

**e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.**

**-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE** commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FRANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

considerando che le indagini svolte nell'ambito di tale indagine giudiziaria consentono di sospettare che gli utenti delle soluzioni criptate fornite da SkyECC, i cui dati di utilizzi passano attraverso i server(softwar) messi a disposizione dalla società OVH, partecipino alla commissione di reati punibili con una pena detentiva di almeno tre anni, nella fattispecie atti di associazione a delinquere finalizzati in particolare alla preparazione di reati particolarmente l'importazione di stupefacenti da parte di una banda organizzata e di reati punibili con la reclusione di dieci anni, compresi l'acquisizione, la detenzione, il trasporto e il trasferimento di stupefacenti, nonché i reati connessi alla legislazione sulle armi,

considerando che è stato accertato che i due server inizialmente affittati da SkyECC a OVH comunicano tra loro e che il server principale comunica anche con Internet; che tali procedure operative costituiscono reti di comunicazione elettronica e di comunicazione elettronica e sono state intercettate sulla base delle summenzionate disposizioni giuridiche,

Che queste misure di intercettazione sono state successivamente rinnovate dal magistrato inquirente;

considerando inoltre che le indagini svolte in particolare dalle autorità olandesi hanno dimostrato che gli utenti della soluzione SkyECC si scambiavano in modo criptato, in particolare per quanto riguarda le modalità di acquisizione, trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale,

considerando che una relazione comunicata dalle autorità olandesi in seguito allo sfruttamento dei dati dell'intercettazione delle comunicazioni autorizzate nell'ambito dell'indagine preliminare ha confermato l'utilizzo da parte di attori di organizzazioni criminali di soluzioni SkyECC, in particolare evidenziando identificatori e gruppi legati ad attività criminali, "El chapo è tornato" "Generai in armi", gruppi relativi al recupero e al trasporto di stupefacenti;che le autorità belghe confermano l'intercettazione di questi dati necessari al fine di poter comprendere l'architettura dei server e la loro comunicazione .

considerando che il proseguimento delle intercettazioni poste in essere appare quindi necessario per la manifestazione della verità per proseguire le indagini sull'architettura dei server, sulle comunicazioni di dati relativi alle organizzazioni criminali. per raccogliere prove e identificare squadre criminali utilizzando la soluzione SkyECC, tali intercettazioni appaiono proporzionate alla gravità degli atti di associazione a delinquere ai fini della preparazione di reati e reati punibili con dieci anni di reclusione oggetto del presente procedimento in corso .

essere nell'impossibilità di eseguire noi stessi gli atti necessari allegati,

Diamo commissione rogatoria al Sig. Direttore

A:

Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione

106 RUE DES TROIS FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato al più presto, entro il 30 aprile 2020

Fatto nel nostro ufficio, 19 febbraio 2020

Giudice istruttore VALèRIE CULIOLI

**INCARICO**

Ho l'onore di chiederLe di fare tutte le richieste necessarie per procedere con

intercettazione, registrazione e trascrizione delle comunicazioni elettroniche

intervenienti tra i due server localizzati all'indirizzi IP seguenti , che Sono impiantati fisicamente presso l'host( ospite ) OVH situato a ROUBAIX:

- il server principale , lega direttamente a rete internet , D'indirizzo IP :5.135.135.94
- un server di backup ,d'indirizzo IP,188.165.14.8

e per una durata di un mese et 24 jours , dal 20 febbraio 2020 fino 13 aprile 2020

Redigerai un rapporto di ciascuna delle operazioni di intercettazione e registrazione, il suddetto rapporto menzionando la data e l'ora in cui l'operazione è iniziata e quelli in cui si è conclusa.

Ci informerai regolarmente dei progressi della tua missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

Fatto nel nostro ufficio , 19 febbraio 2020

Guidice di istruzione VALèRIE CULIOLI

D.196

**CORTE D'APPELLO DI DOUAI**

**Tribunale giudiziario di Lilla**

Ufficio di , VALèRIE

Vicepresidente incaricato delle indagini

N° Procura : 19043000263

Numero di istruzione: JI CJIRSBC19000006

identificatore giudiziare : 1900451491T

25-10-2021

Il Cancelliere Esperto
Dr.ssa Katia Incognito

**Commissione Rogatoria**

**INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA**

Noi, VALèRIE CULIOLI, giudice istruttore siamo nel nostro ufficio presso la Tribunale giudiziaria di Lille;

vostra informazione contro

X

Implicati dei capi:

**FORNITURA DI SERVIZI DI CRIPTOLOGIA VOLTI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** impegnata nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sotto la giurisdizione del JIRS di LILLE

previsto dall'ART.35 III, ART.31 §1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §111, §IV LEGGE 2004-575 DEL 21/06/2004.

**PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE IN VISTA DELLA PREPARAZIONE DI UN REATO** commesso nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, sotto la giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito con ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE

**FORNITURA DI UN MEZZO DI CRITTOGRAFIA NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA DICHIARAZIONE PREVENTIVA** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sotto la giurisdizione del JIRS di LILLE

previsto dall'ART.35 §1 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART. 35 §1 1 °, §IV LEGGE 2004-57 5 DEL 21/06/2004.

**IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA DICHIARAZIONE PREVENTIVA IMPEGNATA NEL MESE DI GENNAIO 2018 E FINO AL 20 AGOSTO 2019 a ROUBAIX** e nei dipartimenti di NORD e PAS-DE-CALAIS, sotto la giurisdizione del JIRS di LILLE

previsto da ART.35 §11°, ART.30 §lii, ART.29 LOI 2004-575 DU 21/06/2004 ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**PARTECIPAZIONE AD UN'ASSOCIAZIONE A DELINQUERE FINALIZZATA ALLA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE** commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS ( regione francese), sotto la giurisdizione del JIRS de LILLE

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito con ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

vista la relazione de dell'OCLCTIC del 29 LUGLIO 2020 sollecitando la proroga delle intercettazioni in corso

Se le indagini in corso fanno sorgere il sospetto che gli utenti delle soluzioni crittografate fornite da SkyECC, i cui dati di utilizzo transitano attraverso i server messi a disposizione dalla società OVH, partecipino alla commissione di reati punibili con almeno tre anni di reclusione, in tale caso i fatti di associazione a delinquere finalizzata alla preparazione di reati, in particolare l'importazione di stupefacenti in una banda organizzata e i reati punibili con la reclusione a dieci anni, in particolare l'acquisto, la detenzione, il trasporto e la vendita di stupefacenti, i reati relativi alla la legislazione sulle armi.

Considerando, infatti, dalle indagini svolte in particolare dalle autorità olandesi e belghe che gli utenti della soluzione SkyECC si scambiano in maniera criptata, in particolare sulle modalità di acquisizione, trasporto di stupefacenti (cocaine, resina di cannabis), anni a livello internazionale, che più specificamente un rapporto comunicato dalle autorità olandesi a seguito dello sfruttamento dei dati provenienti dall'intercettazione delle comunicazioni confermi l'utilizzo da parte degli attori delle organizzazioni criminali delle soluzioni SkyECC, in particolare mettendo in evidenza identificatori e gruppi legati all'attività criminale, "El capo is back" "Generale in armi", gruppi relativi al recupero e al trasporto di stupefacenti, che il proseguimento delle intercettazioni ha permesso di confermare l'uso di questi telefoni da parte di gruppi criminali tramite questi gruppi di discussione,

considerando che i due server noleggiati da SkyECC da OVH comunicano tra loro, il server principale e il server di backup comunicano anche con Internet, tali modalità di funzionamento costituiscono

comunicazioni elettroniche e reti di comunicazione elettronica che possono essere oggetto di intercettazione sulla base delle citate disposizioni di legge ,

considerando sono quindi in corso tre intercettazioni riguardanti le comunicazioni in entrata e in uscita dei due server nonché le comunicazioni tra questi due server, che queste tre intercettazioni consentono di proseguire le indagini sull'architettura dei server e sui dati scambiati tramite questi server, per confermare il coinvolgimento degli utenti telefonici SkyECC nella criminalità organizzata, in particolare in termini di traffico di droga,

Considerando che tra aprile e agosto 2020 le indagini hanno consentito progressi decisivi nell'analisi dei messaggi scambiati tramite questa soluzione crittografata, in quanto la copiatura della RAM effettuata a maggio e giugno 2020 ha consentito di reperire dati utili alla comprensione e analisi dell'infrastruttura SkyECC, che la CTA è riuscita, in collaborazione con la squadra investigativa comune, ad effettuare la decrittazione di parte dei messaggi di gruppo, che tali indagini confermano l'utilizzo da parte di gruppi criminali di questa soluzione crittografata, soprattutto a seguito di una migrazione di utenti della soluzione crittografata Encrochat smantellata durante un'operazione congiunta tra Francia e Paesi verso la soluzione crittografata SkyECC da metà giugno 2020 (più di 30.000 nuovi utenti in relazione a questo smantellamento) in connessione con una migrazione dell'infrastruttura del personale SkyECC su altri server , a conferma del grande cautela e l'uso per scopi criminali di questa soluzione crittografata,

Considerato che la prosecuzione delle intercettazioni poste in essere appare quindi necessaria per la manifestazione della verità al fine di proseguire le proficue indagini sull'architettura dei server, sulle comunicazioni di dati relativi alle organizzazioni criminali, alla raccolta di elementi di prova e alla identificazione delle squadre criminali mediante la soluzione SkyECC, tali intercettazioni appaiono proporzionate alla gravità degli atti di associazione per delinquere in vista della preparazione di reati e delitti punibili con la reclusione di dieci anni coperti dalla presente procedura,

essendo nell'impossibilità di procedere noi stessi gli atti necessari allegati,

Diamo commissione regatoria a: Signor Direttore dell'Ufficio centrale contro la criminalità in relazione alle tecnologie dell'informazione e della comunicazione

101 rue des trois Fontanot

92000 Nanterre

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà trasmesso nel modo più tempestivo entro il 30 dècembre 2020

**Missione**

Ho l'onore di chiedervi di procedere con tutte le richieste utili per procedere all'intercettazione, registrazione e trascrizione

1-le comunicazioni elettroniche che avvengono tra i due server che rispondono ai seguenti indirizzi DNS che si trovano fisicamente presso l'host OVH situato in ROUBAIX: il server principale - ns62400.ip-5. 135-135.eu e il server di backup (Vrack) ns6019808.ip-188-165-14.eu.

2- comunicazioni elettroniche in entrata e in uscita dal server principale - ns62400.ip-5. 135.eu

3- comunicazioni elettroniche in entrata e in uscita dal server di backup - ns60 19808.ip-188-165-14

e questo per uno dei quattro mesi_dal 13 agosto 2020 al 13 dicembre 2020

Redigerai un rapporto di ciascuna delle operazioni di intercettazione e registrazione, il suddetto rapporto menzionando la data e l'ora in cui l'operazione è iniziata e quelli in cui si è conclusa.

Ci informerai regolarmente dell'evoluzione della vostra missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

Fatto nel nostro ufficio, questo 3 agosto 2020

Il giudice istruttore

Giudice istruttore VALèRIE CULIOLI

D202

**Corte d'appello di DOUAI**

**CORTE DI GIUSTIZIA DI LLLE**

**Uffucio di Marc CHEMIN**

**Vicepresidente incaricato delle indagini**

25-10-2022

Il Cancelliere Esperto
Dr.ssa Katia Incognito

Procura n : 19043000263

Istruzioni: JI CJIRSBC19000006

Identificatore giudiziale : 1900451491T

## COMMISSIONE ROGATORIA

**INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA**

n°5

Noi, Marc CHEMIN, vicepresidente responsabile delle indagini, siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

- **FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 aprile2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §Iii, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §Iii, §IV LEGGE 2004-575 DEL 21/06/2004.

-**PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE** fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE.

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENALE.

-**FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §1 1 °, ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi durante J anvier 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

**e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.**

**-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE** commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FRANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENAL.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENAL.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

considerando che le indagini svolte nell'ambito di tale indagine giudiziaria consentono di sospettare che gli utenti delle soluzioni criptate fornite da SkyECC, i cui dati di utilizzi passano attraverso i server(softwar) messi a disposizione dalla società OVH, partecipino alla commissione di reati punibili con una pena detentiva di almeno tre anni, nella fattispecie atti di associazione a delinquere finalizzati in particolare alla preparazione di reati particolarmente l'importazione di stupefacenti da parte di una banda organizzata e di reati punibili con la reclusione di dieci anni, compresi l'acquisizione, la detenzione, il trasporto e il trasferimento di stupefacenti, nonché i reati connessi alla legislazione sulle armi,

considerando che è stato accertato che i due server inizialmente affittati da SkyECC a OVH comunicano tra loro e che il server principale comunica anche con Internet; che tali procedure operative costituiscono reti di comunicazione elettronica e di comunicazione elettronica e sono state intercettate sulla base delle summenzionate disposizioni giuridiche,

Che queste misure di intercettazione sono state successivamente rinnovate dal magistrato inquirente;

considerando inoltre che le indagini svolte in particolare dalle autorità olandesi hanno dimostrato che gli utenti della soluzione SkyECC si scambiavano in modo criptato, in particolare per quanto riguarda le modalità di acquisizione, trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale,

considerando che una relazione comunicata dalle autorità olandesi in seguito allo sfruttamento dei dati dell'intercettazione delle comunicazioni autorizzate nell'ambito dell'indagine preliminare ha confermato l'utilizzo da parte di attori di organizzazioni criminali di soluzioni SkyECC, in particolare evidenziando identificatori e gruppi legati ad attività criminali, "El chapo è tornato" "Generai in armi", gruppi relativi al recupero e al trasporto di stupefacenti;

considerando che le indagini svolte in particolare dalle autorità belghe e olandesi confermano il fatto che gli utenti della soluzione SkyECC si scambiano in modo criptato, in particolare sulle modalità di acquisizione, trasporto di stupefacenti (coccarda, resina di cannabis), armi a livello internazionale,

considerando che nel corso delle intercettazioni è emerso che tra i due server circolavano comunicazioni non criptate contenenti interrogazioni SQL, dati utili per le indagini effettuate; che, tuttavia, secondo le informazioni fornite dalle autorità belghe dal 2 ottobre, i messaggi finora intercettati nelle missioni SQL che passavano tra i due server sono scomparsi; che è accertato che SKYSECURE ha noleggiato il 3 ottobre 2020 da OVH un terzo server più potente dei due noleggiati in precedenza;

Che venga quindi richiesta un'intercettazione di tutte le comunicazioni in entrata e in uscita di questo nuovo server identificato presso OVH con il suo nome di host ns61191227. Ip-51-91-129.eu,

considerando che l'attuazione di intercettazioni sui server utilizzati finora ha permesso di fornire ulteriori elementi di analisi utili alla manifestazione della verità, che l'attuazione di un'intercettazione delle comunicazioni sul traffico operato dal nuovo server appare pertanto necessaria per la manifestazione della verità al fine di proseguire le indagini sull'architettura dei server, sulla comunicazione di dati relativi a organizzazioni criminali, per raccogliere prove e identificare squadre criminali utilizzando la soluzione SkyECC, tali intercettazioni appaiono proporzionate alla gravità degli atti di associazione a delinquere ai fini della preparazione di reati e reati punibili con dieci anni di reclusione oggetto del presente procedimento,

Non essere in grado di eseguire da soli gli atti necessari allegati,

Diamo rogatoria al Sig. Direttore

A:

Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione

106 RUE DES TROIS FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato al più presto, entro il 15/12/2020

Fatto nel nostro ufficio, questo 6 ottobre 2020

Il vicepresidente incaricato dell'indagine

**Marc Chemain**

**Missione**

Ho l'onore di chiederLe di fare tutte le richieste necessarie per procedere con

intercettazione, registrazione e trascrizione

**comunicazioni elettroniche in entrata e in uscita (traffico di rete esterno) del server identificato come ns61191227.ip-51-91-129.eu hotel, fisicamente ubicato presso l'hosting provider OVH situato a ROUBAIX;**

e questo da oggi fino al 13 dicembre 2020.

Redigerai un rapporto di ciascuna delle operazioni di intercettazione e registrazione, il suddetto rapporto menzionando la data e l'ora in cui l'operazione è iniziata e quelli in cui si è conclusa.

Ci informerai regolarmente dei progressi della tua missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

**Vi prego di restituirmi questa rogatoria insieme ad una relazione riassuntiva.**

Fatto nel nostro ufficio, questo 6 ottobre 2020 Il vicepresidente incaricato dell'indagine

Marc Chemain

**MINISTERO DELL'INTERNO**

Corte d'appello di DOUAI

CORTE DI GIUSTIZIA DI LLLE

Ufficio di Marc CHEMIN

Vicepresidente incaricato delle indagini

Parquet 19043000263

Istruzioni: JI CJIRSBC19000006

Identificatore di giustizia: 1900451491T

25.10.2021

Il Cancelliere Esperto
Dr.ssa Katia Incognito

COMMISSIONE ROGATORIA

INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA

Noi , Valèrie CULIOLI , judice istruttore siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

- **FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §Iii, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §Iii, §IV LEGGE 2004-575 DEL 21/06/2004.

**-PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE** fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE.

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENALE.

**-FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §1 1°, ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ**

**SENZA PREVIA DICHIARAZIONE** fatti commessi durante J anvier 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

**e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.**

**-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE** commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FRANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENALE.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

considerando che le indagini svolte nell'ambito di tale indagine giudiziaria consentono di sospettare che gli utenti delle soluzioni criptate fornite da SkyECC, i cui dati di utilizzi passano attraverso i server(softwar) messi a disposizione dalla società OVH, partecipino alla commissione di reati punibili con una pena detentiva di almeno tre anni, nella fattispecie atti di associazione a delinquere finalizzati in particolare alla preparazione di reati particolarmente l'importazione di stupefacenti da parte di una banda organizzata e di reati punibili con la reclusione di dieci anni, compresi l'acquisizione, la detenzione, il trasporto e il trasferimento di stupefacenti, nonché i reati connessi alla legislazione sulle armi,

considerando che è stato accertato che i due server inizialmente affittati da SkyECC a OVH comunicano tra loro e che il server principale comunica anche con Internet; che tali procedure operative costituiscono reti di comunicazione elettronica e di comunicazione elettronica e sono state intercettate sulla base delle summenzionate disposizioni giuridiche,

Che queste misure di intercettazione sono state successivamente rinnovate dal magistrato inquirente;

considerando inoltre che le indagini svolte in particolare dalle autorità olandesi hanno dimostrato che gli utenti della soluzione SkyECC si scambiavano in modo criptato, in particolare per quanto riguarda le modalità di acquisizione, trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale,

considerando che una relazione comunicata dalle autorità olandesi in seguito allo sfruttamento dei dati dell'intercettazione delle comunicazioni autorizzate nell'ambito dell'indagine preliminare ha confermato l'utilizzo da parte di attori di organizzazioni criminali di soluzioni SkyECC, in particolare evidenziando identificatori e gruppi legati ad attività criminali, "El chapo è tornato" "Generai in armi", gruppi relativi al recupero e al trasporto di stupefacenti;che le autorità belghe confermano l'intercettazione di questi dati necessari al fine di poter comprendere l'architettura dei server e la loro comunicazione .

considerando che il proseguimento delle intercettazioni poste in essere appare quindi necessario per la manifestazione della verità per proseguire le indagini sull'architettura dei server, sulle comunicazioni di dati relativi alle organizzazioni criminali. per raccogliere prove e identificare squadre criminali utilizzando la soluzione SkyECC, tali intercettazioni appaiono proporzionate alla gravità degli atti di associazione a delinquere ai fini della preparazione di reati e reati punibili con dieci anni di reclusione oggetto del presente procedimento in corso .

essere nell'impossibilità di eseguire noi stessi gli atti necessari allegati,

Diamo commissione rogatoria al Sig. Direttore

A:

Ufficio centrale per la lotta contro la criminalità connessa alle tecnologie dell'informazione e della comunicazione

106 RUE DES TROIS FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato al più presto, entro il 30 marzo 2020

Fatto nel nostro ufficio, 18 octobre2029

Gudice di istruzione

**Valèrie CULIOLI**

## INCARICO

Ho l'onore di chiederLe di fare tutte le richieste necessarie per procedere a tutte le requisizioni utile per procedere all'intercettazione, registrazione e trascrizione

1-Le comunicazioni elettroniche intervenienti tra i due server localizzati all'indirizzi IP seguenti , che Sono impiantati fisicamente presso l'host( ospite ) OVH situato a ROUBAIX:

- il server principale , lega direttamente a rete internet , D'indirizzo IP :5.135.135.94
- un server di backup ,d'indirizzo IP,188.165.14.8

2-Le comunicazioni elettroniche entranti e usciti dal server principale d'indirizzo IP 5.135.135.94 impiantati fisicamente presso l'host( ospite ) OVH situato a ROUBAIX:

e per una durata di quattro mese et 24 jours , dal 20 ottobre 2019 fino 20 febbraio 2020

Redigerai un rapporto di ciascuna delle operazioni di intercettazione e registrazione, il suddetto rapporto menzionando la data e l'ora in cui l'operazione è iniziata e quelli in cui si è conclusa.

Ci informerai regolarmente dei progressi della tua missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

Fatto nel nostro ufficio , 18 ottobre 2020

Gudice di istruzione

Gudice di istruzione

**Valèrie CULIOLI**

197

Corte d'appello di DOUAI

**CORTE DI GIUSTIZIA DI LLLE**

**Ufficio di Marc CHEMIN**

**Vicepresidente incaricato delle indagini**

25-10-2021

Il Cancelliere Esperto
Dr.ssa Ignota Incognito

Parquet 19043000263

Istruzioni: JI CJIRSBC19000006

identificatore di giustizia: 1900451491T

## ROGATORIO COMMISSIONE

INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA

Traffico esterno -server 1

Noi, Mare CHEMIN, vicepresidente responsabile delle indagini, siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

**- FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 aprile2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §Iii, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §Iii, §IV LEGGE 2004-575 DEL 21/06/2004.

**-PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE** fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE.

previsto dall'ART.450-1 AL.1, AL.2 C.PENAL.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENAL.

**-FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1 °, ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi durante J anvier 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENAL.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENAL.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

vista la relazione di M.GAUTHIER DE L'OCLCTIC del 27 novembre 2020.

considerando che le indagini svolte nell'ambito della presente informativa giudiziaria lo consentono sospettare che le rozze soluzioni fornite dalla società SKyECC, i cui dati utente passano attraverso i server messi a disposizione dalla società OVH a ROUBAIX, possano essere utilizzate per la commissione sul territorio nazionale di reati punibili con almeno tre anni di reclusione. In particolare l'importazione di stupefacenti in una banda organizzata, le violazioni della normativa sugli stupefacenti, nonché i reati relativi alla normativa sulle armi, che potrebbero costituire la fornitura di tali soluzioni di cifratura non autorizzate sul territorio nazionale ed il loro utilizzo da parte di organizzazioni criminali il reato di associazione per delinquere finalizzata alla preparazione di un reato punibile con 10 anni.

Considerando che è stato stabilito che i server noleggiati da SkyECC a OVH comunicavano tra loro ma anche con la rete Internet; che tali modalità operative costituenti comunicazioni elettroniche e reti di comunicazione elettronica siano state intercettate sulla base delle predette disposizioni di legge,

Che tali provvedimenti di intercettazione siano stati successivamente rinnovati dal Magistrati istruttori.

Considerando inoltre che le indagini svolte in particolare dalle autorità olandesi e belghe hanno confermato che gli utilizzatori della soluzione SkyECC si scambiavano in maniera criptata, in particolare sulle modalità di acquisizione e trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale, confermando il fatto che tale soluzione crittografata è stata utilizzata da organizzazioni criminali per proteggere le loro comunicazioni da possibili indagini di polizia o giudiziarie e per scambiare in forma anonima;

Che è stata posta in essere un'intercettazione di tutte le comunicazioni in entrata e in uscita dai server ubicati presso OVH previa autorizzazione del Giudice Libertà e Detenzione e poi del GIP

Considerando che l'implementazione delle intercettazioni sui server utilizzati ha consentito di fornire ulteriori elementi di analisi utili alla manifestazione della verità, che ha consentito in particolare di comprendere meglio l'architettura dei server, il funzionamento delle soluzioni crittografate e di intercettare dopo talvolta la decrittazione dei dati relativi all'utilizzo della soluzione di cifratura SkyECC a fini criminali;

Che il proseguimento delle intercettazioni poste in essere è necessario per la manifestazione della verità

Che tali intercettazioni appaiano proporzionate alla gravità dei fatti oggetto del presente procedimento, ed alle finalità perseguite nel caso di associazione di delinquenti finalizzata alla preparazione di delitti punibili con la reclusione di dieci anni

Non essendo in grado di compiere noi stessi gli atti annessi necessari,

Diamo commissione rogatorie al Signor Direttore

a: ufficio centrale per la lotta alla criminalità legata alle tecnologie di Informazione e comunicazione

106 VIA DEI TRE FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato quanto prima, entro il 15/04/2021

Fatto presso la nostra sede il 03 dicembre 2020

Il vicepresidente incaricato dell'istruzione

Marc Chemain

**Incarico**

Ho l'onore di chiedervi di procedere con tutte le richieste utili per continuare l'intercettazione, la registrazione e la trascrizione

-comunicazioni elettroniche in entrata e in uscita circolanti sul link esterno (internet) del server identificato con l'host name (nome DNS) ns62400.ip-

5.135-135eu (chiamato server 1-server principale)

fisicamente situato presso l'host OVH situato a ROUBAIX;

e questo per un periodo di 4 mesi,

Lei redigerà un verbale di ciascuna delle operazioni di intercettazione e registrazione, in detto verbale indicando la data e l'ora in cui l'operazione è iniziata e quelle in cui è terminata.

Ci informerai regolarmente dello stato di avanzamento della tua missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

I dati crittografati possono essere consegnati direttamente al CTA che agisce su richiesta della loro decodificazione (descrizione )

I dati intercettati possono essere trasmessi ai servizi investigativi belgi e olandesi per essere utilizzati nell'ambito della squadra investigativa comune costituita;

Vi preghiamo di restituirmi questa lettera di richiesta insieme a un rapporto riepilogativo.

Fatto presso la nostra sede il 03 dicembre 2020

Il vicepresidente incaricato dell'istruzione

Marc Chemain

D 199

Corte d'appello di DOUAI

**CORTE DI GIUSTIZIA DI LLLE**

**Ufficio di Marc CHEMIN**

**Vicepresidente incaricato delle indagini**

25-10-2012
Il Cancelliere Esperto
Dr.ssa Katia Incognito

Parquet 19043000263

Istruzioni: JI CJIRSBC19000006

identificatore di giustizia: 1900451491T

**COMMISSIONE ROGATORIA**

INTERCETTAZIONE DELLA CORRISPONDENZA PER VIA ELETTRONICA

Traffico esterno -server 2

Noi, Marc CHEMIN, vicepresidente responsabile delle indagini, siamo nel nostro ufficio presso la Tribunal judiciaire de Lille; viste le informazioni relative a:

X

Accusato di capi:

- **FORNITURA DI SERVIZI DI CRITTOGRAFIA FINALIZZATI A GARANTIRE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME** fatti commessi nel mese di gennaio 2018 e fino al 20 aprile2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §III, ART.31§1, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5, ART.8 . DECRETO 2007-663 DEL 02/05/2007.

e punibile dall'ART.35 §III, §IV LEGGE 2004-575 DEL 21/06/2004.

**-PARTECIPAZIONE A UN'ASSOCIAZIONE CRIMINALE PER LA PREPARAZIONE DI UN CRIMINE** fatti commessi durante Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e nei dipartimenti di NORD e di PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLA.

previsto dall'ART.450-1 AL.1, AL.2 C.PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 CODICE.PENALE.

**-FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCA ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi nel mese di gennaio 2018 e fino al 20 agosto 2019 a ROUBAIX e nei dipartimenti di NORD e PAS-DE-CALAIS, nella giurisdizione del JIRS di LILLA

previsto dall'ART.35 §I 1 °, ART.30 §III, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON FORNISCE ESCLUSIVAMENTE FUNZIONI DI AUTENTICAZIONE O CONTROLLO DELL'INTEGRITÀ SENZA PREVIA DICHIARAZIONE** fatti commessi durante gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX e sui dipartimenti di NORD e PAS-DE-CALAIS, sulla giurisdizione del JIRS di LILLE

previsto dall'ART.35 §I 1°, ART.30 §111, ART.29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART.4, ART.5

DECRETO 2007-663 DEL 02/05/2007.

e punito dall'ART.35 §11°, §IV LEGGE 2004-575 DEL 21/06/2004.

**-PARTECIPAZIONE AD ASSOCIAZIONE A DELINQUERE PER LA PREPARAZIONE DI UN REATO PUNIBILE CON 10 ANNI DI RECLUSIONE commesso nel mese di Gennaio 2018 e fino al 20 Agosto 2019 a ROUBAIX** e sui dipartimenti del NORD e del PAS-DE-CALAIS( UNA REGIONE DEL NORD DELLA FANCIA ), sulla giurisdizione del JIRS di LILLE

previsto dall'ART.450-1 AL.1, AL.2 CODICE .PENALE.

e punito dagli ART.450-1 AL.2, ART.450-3, ART.450-5 C.PENAL.

visti gli articoli 18, 81, 100, 100-1, da 100-3 a 100-8, 151 e seguenti del codice di procedura penale,

vista la relazione di M.GAUTHIER DE L'OCLCTIC del 27 novembre 2020.

considerando che le indagini svolte nell'ambito della presente informativa giudiziaria lo consentono sospettare che le rozze soluzioni fornite dalla società SKyECC, i cui dati utente passano attraverso i server messi a disposizione dalla società OVH a ROUBAIX, possano essere utilizzate per la commissione sul territorio nazionale di reati punibili con almeno tre anni di reclusione. In particolare l'importazione di stupefacenti in una banda organizzata, le violazioni della normativa sugli stupefacenti, nonché i reati relativi alla normativa sulle armi, che potrebbero costituire la fornitura di tali soluzioni di cifratura non autorizzate sul territorio nazionale ed il loro utilizzo da parte di organizzazioni criminali il reato di associazione per delinquere finalizzata alla preparazione di un reato punibile con 10 anni.

Considerando che è stato stabilito che i server noleggiati da SkyECC a OVH comunicavano tra loro ma anche con la rete Internet; che tali modalità operative costituenti comunicazioni elettroniche e reti di comunicazione elettronica siano state intercettate sulla base delle predette disposizioni di legge,

Che tali provvedimenti di intercettazione siano stati successivamente rinnovati dal Magistrati istruttori.

Considerando inoltre che le indagini svolte in particolare dalle autorità olandesi e belghe hanno confermato che gli utilizzatori della soluzione SkyECC si scambiavano in maniera criptata, in particolare sulle modalità di acquisizione e trasporto di stupefacenti (cocaina, resina di cannabis), armi a livello internazionale, confermando il fatto che tale soluzione crittografata è stata utilizzata da organizzazioni criminali per proteggere le loro comunicazioni da possibili indagini di polizia o giudiziarie e per scambiare in forma anonima;

Che è stata posta in essere un'intercettazione di tutte le comunicazioni in entrata e in uscita dai server ubicati presso OVH previa autorizzazione del Giudice Libertà e Detenzione e poi del GIP

Considerando che l'implementazione delle intercettazioni sui server utilizzati ha consentito di fornire ulteriori elementi di analisi utili alla manifestazione della verità, che ha consentito in particolare di comprendere meglio l'architettura dei server, il funzionamento delle soluzioni crittografate e di intercettare dopo talvolta la decrittazione dei dati relativi all'utilizzo della soluzione di cifratura SkyECC a fini criminali;

Che il proseguimento delle intercettazioni poste in essere è necessario per la manifestazione della verità

Che tali intercettazioni appaiano proporzionate alla gravità dei fatti oggetto del presente procedimento, ed alle finalità perseguite nel caso di associazione di delinquenti finalizzata alla preparazione di delitti punibili con la reclusione di dieci anni

Non essendo in grado di compiere noi stessi gli atti annessi necessari,

Diamo commissione rogatorie al Signor Direttore

a: ufficio centrale per la lotta alla criminalità legata alle tecnologie di Informazione e comunicazione

106 VIA DEI TRE FONTANOT 92000 NANTERRE

ai fini dello svolgimento delle operazioni qui indicate.

Diciamo che il verbale redatto ci verrà inviato quanto prima, entro il 15/04/2021

Fatto presso la nostra sede il 03 dicembre 2020

Il vicepresidente incaricato dell'istruzione

Marc Chemain

**Incarico**

Ho l'onore di chiedervi di procedere con tutte le richieste utili per continuare l'intercettazione, la registrazione e la trascrizione

**-comunicazioni elettroniche in entrata e in uscita circolanti sul link esterno (internet) del server identificato con l'ospite nome (nome DNS) ns62400.ip-5.135-135eu (chiamato server 1-server principale)**

**fisicamente situato presso l'ospite OVH situato a ROUBAIX;**

e questo per un periodo di 4 mesi,

Lei redigerà un verbale di ciascuna delle operazioni di intercettazione e registrazione, in detto verbale indicando la data e l'ora in cui l'operazione è iniziata e quelle in cui è terminata.

Ci informerai regolarmente dello stato di avanzamento della tua missione e di eventuali difficoltà incontrate nell'esecuzione di questa missione.

I dati crittografati possono essere consegnati direttamente al CTA che agisce su richiesta della loro decodificazione (descrizione )

I dati intercettati possono essere trasmessi ai servizi investigativi belghe e olandesi per essere utilizzati nell'ambito della squadra investigativa comune costituita;

Vi preghiamo di restituirmi questa lettera di richiesta insieme a un rapporto riepilogativo.

Fatto presso la nostra sede il 03 dicembre 2020

Il vicepresidente incaricato dell'istruzione

Marc Chemain

AO. 6

Corte d'Appello di Parigi
Tribunale giudiziario di Parigi

D207/1

Ufficio di
Brice HANSEMANN
Vice presidente responsabile dell'istruzione

N° Procura: 20342 00697
N° dossier: JUI82520000010

# Ordinanza

## Recante autorizzazione di predisposizione di un dispositivo tecnico di acquisizione di dati informatici

Noi, Brice HANSEMANN vice presidente responsabile dell'istruzione, essendo nel nostro ufficio presso il Tribunale giudiziario di Parigi,

Vista l'inchiesta seguente contro: X

dei capi :

1) Associazione di criminali per la preparazione di reati o delitti punito con 10 anni di carcere (reati di importazione di sostanze stupefacenti commessi in bande organizzate, reati di traffico di sostanze stupefacenti)

fatti previsti e puniti dagli art. 450-1, 450-3, 450-5 c. penale (Natura di Infrazione 7188, 12214);

2) Fornitura di prestazioni di crittografia con lo scopo di assicurare delle funzionalità' di riservatezza senza dichiarazione conforme;

fatti previsti e puniti dagli 35 par. III e IV, ART 31 PAR. I, ART. 29 LEGGE 2004-575 DEL 21/06/2004. ART.3, ART. 4, ART. 5, ART. 8 DECRETO 2007-663 DEL 02/05/2007(Natura di Infrazione 32529);

3) Fornitura di un mezzo di crittografia che non assicura esclusivamente delle funzioni di autenticità e di controllo d'integrità senza dichiarazione preventiva
Fatti previsti e puniti dagli ART. 35 par. I 1°, IV ART 30 par. III, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, DECRETO 2007-663 DEL 02/05/2007 (Natura di Infrazione 32537);

4) Importazione di un mezzo di crittografia che non assicura esclusivamente delle funzionalità di autenticità o di controllo d'integrità senza dichiarazione preventiva.
Fatti previsti e puniti dagli Art. 35 par. I 1°, par. IV, ART 30 par. III, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, DECRETO 2007-663 DEL 02/05/2007(Natura di Infrazione 32539);

Fatti commessi in particolare a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione di Lilla, in ogni caso sul territorio nazionale, da gennaio 2018 fino al 20 agosto 2019, comunque dopo il periodo non coperto dalla prescrizione dell'azione pubblica.

Visti gli articoli 706-95-11 e 706- 95-19 del Codice di procedura penale,

Visti gli articoli 706-102-1 e 706- 102-5 del Codice di procedura penale,

Visto l'articolo D15-6-1 del Codice di Procedura penale,

Visto il Decreto n° 2015-1700 del 18 dicembre 2015 relativo all'acquisizione dei trattamenti di dati informatici acquisiti in applicazione dell'articolo 706-102-1 del codice di procedura penale,

Vista la commissione rogatoria del 20 agosto 2019 consegnata dalla dott.ssa Valérie CULIOLI, giudice dell'istruzione presso il tribunale giudiziario di LILLA al Direttore dell'Ufficio centrale della lotta contro la criminalità legata alle tecnologie dell'informazione e della comunicazione sotto i riferimenti seguenti: N° Procura: 19043000263- N° istruttoria: JI CJIRSBC19000006- identificativo giustizia: 1900451491T.

Vista la commissione rogatoria complementare consegnata il primo aprile 2020 dalla dott.ssa Valérie CULIOLI, giudice di istruzione presso il tribunale giudiziario di LILLA al Direttore centrale della Polizia giudiziaria sotto i seguenti riferimenti: N° Procura: 19043000263- N° istruttoria: JI CJIRSBC19000006- identificativo giustizia: 1900451491T.

Vista la decisione di proroga della commissione rogatoria consegnata da M Marc CHEMIN, vicepresidente responsabile dell'istruttoria presso il tribunale giudiziario di LILLA il 22 ottobre 2020;

Visti i trasmessi di Brice HANSEMANN, Aline BATOZ, Matthieu BONDUELLE, vice-presidenti responsabili dell'istruzione presso il tribunale giudiziario di Parigi e Marine FONTANGE, giudice d'istruzione presso il tribunale giudiziario di Parigi, indirizzato al Direttore della Direzione centrale della polizia giudiziaria in data dell'11 dicembre 2020 ai fini di prosieguo delle indagini;

Visto il rapporto del comandante di polizia Fabrice GAUTHIER in relazione all'OCLCTIC in data del 16 dicembre 2020;

Vista la nostra ordinanza di comunicazione al Procuratore della Repubblica in data del 17 dicembre 2017;

visto il parere del Procuratore della Repubblica in data del 17 dicembre 2020 in vista dell'installazione del dispositivo di acquisizione;

Dato che le indagini condotte sia dalle autorità belghe e olandesi sia dai servizi di inchiesta francesi dimostrano il carattere particolarmente opaco e selettivo del sistema di vendita di dispositivi del sistema crittografato SKYECC; che in effetti è emerso dalle transazioni per l'acquisto di un dispositivo che si effettuavano mediante un costo molto elevato se non proibitivo per una clientela ordinaria ( parecchie migliaia di euro per una durata limitata di alcuni mesi : un tale prezzo per rendersi anonimi non può essere manifestamente consentito che solo per persone che percepiscono dei redditi conseguenti (cfD8), e ciò, dopo una presa di contatto tramite il sito internet della società canadese SKY GLOBAL Technologies Inc, funzionante come una semplice casella postale; che inoltre, la vendita effettiva dei dispositivi che possiedono il sistema criptato SKY ECC è stata in seguito realizzata in delle condizioni clandestine che garantiscono da una parte l'anonimato del venditore e dell'acquirente e impedendo d'altra parte ogni tracciabilità in ragione dei pagamenti in contanti; che queste condizioni di acquisizione illecite si iscrivono in un metodo "commerciale" più globale avviato dalla società che offre il sistema di crittografia SkyECC tendente a tutelare i suoi utilizzatori da qualsiasi indagine suscettibile di essere avviata nei loro confronti dalle autorità giudiziarie, che è in effetti espressamente menzionato sul sito internet della società canadese SKY GLOBAL Technologies Inc., a destinazione delle forze dell'ordine suscettibili di richiederla per ottenere informazioni sui suoi utilizzatori e sul contenuto dei messaggi, che essa non ne conserva nessuno ad eccezione della data di creazione del conto e quella della sua ultima utilizzazione; che si tratta di un sistema estremamente sofisticato; che in effetti, il telefono genera alla sua inizializzazione 4 chiavi di cifratura:

1 – password key. Questa chiave è generata a partire dalla password dell'utilizzatore. Essa resta sul telefono e non è mai trasmessa. Serve a crittografare la secret key memorizzata sul server (e dunque impedendo i gestori del server di decodificarla.)
2- secret key. Questa chiave è trasmessa al server e cancellata dalla memoria del telefono, essa non è mai memorizzata sul telefono. Ogni vota che il telefono ne ha bisogno, la chiede al server, l'utilizza poi la cancella. La secret key serve a decifrare la master key.
3- master key- questa chiave serve a decifrare degli elementi della base dei dati dell'applicazione memorizzati sul telefono e contenente tutte le informazioni di funzionamento e i dati utilizzatori. La master key serve a crittografare alcuni dati memorizzati nella base di dati dell'applicazione di cui la private key.
4- private key. La chiave che serve a crittografare i messaggi ricevuti da un corrispondente (messaggi crittografati dalla chiave pubblica inviata al corrispondente). (D58/49 a D58/54);

Che questi mezzi di crittografia sono la prerogativa di una criminalità di altissima intensità; che l'insieme di questi elementi portano a sospettare che questi telefoni sono destinati ad uso nell'ambito di attività criminali; che questi elementi oggettivi conducono logicamente a considerare che il sistema di telefonia possa essere venduto intenzionalmente a dei fini criminali che possono caratterizzare un'associazione di malfattori; che di fatto, l'inchiesta giudiziaria ha messo in evidenza che il sistema di telefonia crittografata SkyECC era utilizzata da organizzazioni criminali che agiscono in particolare nei PAESI BASSI in BELGIO e in FRANCIA e, per alcuni, ad un livello internazionale (cf D30 in particolare);

Che a questo titolo, in particolare un telefono crittografato SkyECC è stato sequestrato nel porto di Anversa in Belgio nell'ambito di un affare di traffico di stupefacenti; che le autorità di polizia giudiziaria di Anversa hanno ugualmente fatto sapere che la soluzione crittografata SkyECC era utilizzata da parecchie organizzazioni criminali; che le richieste delle autorità giudiziarie belghe presso la società SkyECC hanno dimostrato la sua assenza di collaborazione con la giustizia; che dalle indagini realizzate presso gli operatori di comunicazioni elettroniche francesi, è emersa un'ampia utilizzazione di questo sistema crittografato sul territorio nazionale che può essere il fatto di organizzazioni criminali; che d'altronde, l'utilizzazione di questa crittografia con scopi criminali, da individui desiderosi di assicurare la perfetta sicurezza dei loro scambi cospirativi è stata constatata in un dossier di traffico di sostanze stupefacenti sulla giurisdizione interregionale specializzata di Lilla (D33)

Dato che le indagini in corso nel quadro della squadra comune di inchiesta istituita tra le autorità olandesi, belghe e francesi hanno permesso di confermare che gli utilizzatori della soluzione crittografata SkyECC agivano nel quadro di traffico di stupefacenti ad un livello internazionale grazie al lavoro di telefonia realizzato in particolare (D58/59 a D58/83); che più particolarmente per la Francia, le inchieste hanno permesso di stabilire che questi telefoni, di cui il numero di utilizzatori varia tra 1674 e 3276 sul primo semestre dell'anno 2020 (D58/108-109), potevano essere utilizzati in vista della commissione sul territorio nazionale di reati i e delitti che entrano nel campo delle disposizioni dell'articolo 706-73 del codice di procedura penale, in particolare l'associazione di criminali con lo scopo di preparazione di reati e delitti puniti con 10 anni di carcere ( reati di importazioni e prodotti stupefacenti commessi in bande organizzate, delitti di traffico di prodotti stupefacenti) (cf D9);

Dato che le inchieste condotte nell'ambito della presente informativa giudiziaria hanno stabilito che una parte dell'infrastruttura informatica necessaria all'avvio di questo sistema di crittografia era affittata presso il provider di hosting di servers OVHCLOUD e situata nei centri di elaborazione dati nella sede di questa impresa sita in via Kellermann n. 2 a ROUBAIX (59); ne emerge che questa società è composta da parecchi servers identificati con il nome di host ns62400.ip-5.135-135.eu ( detto server principale o server 1), ns6019808.ip-188-165-14.eu ( detto server di backup o server 2) e ns61191227.ip-51-91-129.eu (detto server 3); che questi servers sono piazzati sotto intercettazione; che le attività di intercettazione di comunicazioni elettroniche circolanti sui collegamenti esterni (da e verso Internet) e interni ( collegamenti

che mettono in comunicazione queste macchine direttamente su una rete interna di VRACK) di questi servers così che l'analisi del sistema di crittografia avviato dall'applicazione SkyEGC permettono di stabilire che:

- Le comunicazioni, dopo aver lasciato la rete dell'operatore mobile del roaming utilizzato dai telefoni in funzione della loro localizzazione geografica, sono indirizzati da internet verso il server 2 (ns6019808.ip-188-165-14.eu);
- I messaggi di gruppo della soluzione SkyECC anche intercettati possono essere crittografati tramite l'intercettazione delle chiavi di crittografia comunicati dal creatore del gruppo a tutti i partecipanti del detto gruppo;
- La cifratura dei messaggi individuali non può essere realizzata a partire dai soli dati intercettati nella misura in cui solo la parte degli elementi crittografati indirizzati dai telefoni sui servers è suscettibile di essere recuperata attraverso dei dati intercettati; l'altra parte degli elementi crittografati essendo unicamente memorizzate sui telefoni,

Dato che nell'ambito della squadra comune di inchiesta, gli investigatori e i tecnici olandesi hanno messo a punto una tecnica suscettibile di permettere di ottenere gli elementi crittografati memorizzati su ciascun telefono che utilizza l'applicazione SkyECC; che questa tecnica, basata sull'installazione di un server che svolge il ruolo di "Man in The Middle" "Uomo nel Mezzo" ( server detto MITM) posizionato sul collegamento esterno del server 2 (ns6019808.ip-188-165-14.eu), consiste nel ricevere tutto il traffico dei telefoni a destinazione del server 2 e tutto il traffico del server 2 a destinazione dei telefoni: che ne risulta che quando un telefono SkyECC si autentica sul server 2, il MITM genera a destinazione di questo telefono un messaggio di notifica di tipo push, specialmente realizzato e normalmente invisibile, che ha per solo scopo di incitare il telefono a comunicare in ritorno gli elementi crittografati necessari alla decifratura dei messaggi individuali ricevuti da questo telefono; che questi elementi sono acquisiti dal dispositivo MITM ma non rinviati al server 2; che tutte le altre comunicazioni dei telefoni sono trasmessi verso il server 2 e vice versa senza alcuna modifica in modo che il servizio di comunicazioni crittografate continua a funzionare normalmente;

Dato che questo dispositivo ha ricevuto l'autorizzazione n° 2011 F 1434 ( valida fino al 30/11/2026) consegnata dalla commissione consultativa incaricata di emettere un parere sui materiali suscettibili di recare violazione alla riservatezza della vita privata e al segreto delle corrispondenze (articolo R.226-2 del Codice penale) durante la sessione del 12 novembre 2020; che gli inquirenti già indirizzati confermavano dunque che i dispositivi SkyECC erano utilizzati a dei fini criminali. L'analisi dei dispositivi essendo impossibile, solo l'avvio di un dispositivo di intercettazione di dati informatici permetterebbe di eludere la crittografia dei dati scambiati dagli utilizzatori, questi transitando tutti dal server impiantato a ROUBAIX; che il ricorso a questo dispositivo, ad integrazione dell'intercettazione dei servers già avviati, costituisce l'unico mezzo di decifrare i messaggi individuali degli utilizzatori della soluzione di crittografia SkyECC dedicandosi a delle attività illecite e pervenire anche alla manifestazione della verità; che la misura di acquisizione appare infatti necessaria per determinare il livello di utilizzazione criminale che è fatto di questo sistema e di identificare tutti i dirigenti della società SKY GLOBAL Technologies Inc., il loro legame tra loro e con le più importanti organizzazioni criminali; che questa misura sembra dunque necessaria per determinare la volontà degli organizzatori di fornire in tutta conoscenza di causa un mezzo di comunicazione riservato che permetta di esercitare delle attività illecite; che l'utilizzazione di questa procedura tecnica è perfettamente proporzionata alla gravità delle infrazioni evocate sopra;

Pertanto, di conseguenza conviene autorizzare, ai sensi degli articoli 706-102-1 e 706-102-5 del codice di procedura penale, l'avvio di questo dispositivo nel centro di rielaborazione dati RBX2 del provider hosting OVHCLOUD all'indirizzo suddetto, sul collegamento esterno ( da e verso internet) del server identificato dal suo nome di host ns6019808.ip-188-165-14.eu ( detto server 2) al fine di intercettare gli elementi crittografati di ogni telefono utilizzando il sistema di crittografia SkyECC, che una volta combinati con gli elementi crittografati provenienti dalle intercettazioni permetteranno di decifrare i messaggi individuali ricevuti da questi telefoni;

## PER QUESTI MOTIVI

AUTORIZZIAMO tramite commissione rogatoria distinta in data odierna, il Direttore della Direzione centrale della Polizia giudiziaria, o qualsiasi ufficiale di polizia giudiziaria o sotto la propria responsabilità qualsiasi agente di polizia giudiziaria, da lui designato, a mettere qua e là nel centro rielaborazione dati RBX2 del provider hosting OVHCLOUD presso la sede di questa società situata in via Kellermann n. 2 a ROUBAIX (59) un dispositivo di acquisizione sulla linea esterna del server ns6019808.ip-188-165-14.eu;

In vista del suo avvio, AUTORIZZIAMO la trasmissione tramite una rete di comunicazioni elettroniche;

AUTORIZZIAMO ugualmente l'utilizzazione del detto dispositivo;

AUTORIZZIAMO questa tecnica speciale di inchiesta per una durata di **QUATTRO (04)** mesi dall'avvio effettivo del dispositivo;

Redatto nel nostro ufficio, il 17 dicembre 2020
Il vice presidente incaricato dell'istruzione
M. Brice HANSEMANN
Timbro del Tribunale giudiziario di Parigi
2020-0381

Copia della presente ordinanza è stata consegnata al Procuratore della Repubblica
Il 21/12/2020
Il cancelliere

D1 1
bis

Corte d'Appello di Parigi
Tribunale giudiziario di Parigi

D212/1

Ufficio di
Brice HANSEMANN
Vice presidente responsabile dell'istruzione

N° Procura: 20342 00697
N° dossier: JIJI82520000010

**Ordinanza**

**Recante autorizzazione di predisposizione di un dispositivo tecnico di**

**Acquisizione di dati informatici**

Noi, Brice HANSEMANN vice presidente responsabile dell'istruzione, essendo nel nostro ufficio presso il Tribunale giudiziario di Parigi,

Vista l'inchiesta seguente contro: X

dei capi:

PARTECIPAZIONE AD UN' ASSOCIAZIONE DI CRIMINALI PER LA PREPARAZIONE DI UN REATO episodi commessi da gennaio 2018 fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione INTERREGIONALE SPECIALIZZATA di Lilla
Previsti dall' ART. 450-1 AL.1, AL.2 C. PENALE.
E puniti dagli art. 450-1 AL.2, ART. 450-3, ART. 450-5 C. PENALE
PARTECIPAZIONE AD UN' ASSOCIAZIONE DI CRIMINALI PER LA PREPARAZIONE DI UN REATO PUNITO CON 10 ANNI DI CARCERE episodi commessi da gennaio 2018 fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione INTERREGIONALE SPECIALIZZATA di Lilla
Previsti dagli ART. 450-1 AL.1, AL.2 C. PENALE.
E puniti dagli art. 450-1 AL.2, ART. 450-3, ART. 450-5 C. PENALE.
FORNITURA DI PRESTAZIONI DI CRITTOGRAFIA CON LO SCOPO DI ASSICURARE DELLE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME episodi commessi da gennaio 2018 fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione INTERREGIONALE SPECIALIZZATA di Lilla
Previsti dall'ART. 35 par. III, ART 31 par. I, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, ART. 8 DECRETO 2007-663 DEL 02/05/2007
e puniti dall'Art. 35 par. III, par. IV Legge 2004-575 del 21/06/2004.
FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON ASSICURA ESCLUSIVAMENTE DELLE FUNZIONI DI AUTENTICITÀ E DI CONTROLLO D'INTEGRITÀ SENZA DICHIARAZIONE PREVENTIVA fatti commessi da gennaio 2018 fino al 20 agosto 2019 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione INTERREGIONALE SPECIALIZZATA di Lilla
Previsti dall'ART. 35 par. I 1°, ART 30 par. III, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, DECRETO 2007-663 DEL 02/05/2007
e puniti dall'Art. 35 par. I 1°, par. IV Legge 2004-575 del 21/06/2004.
IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON ASSICURA ESCLUSIVAMENTE DELLE FUNZIONI DI AUTENTICITÀ E DI CONTROLLO D'INTEGRITÀ SENZA DICHIARAZIONE PREVENTIVA fatti commessi da gennaio

2018 al 20 agosto 2019 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione interregionale specializzata di Lilla
Previsti dall'ART. 35 par. I 1°, ART 30 par. III, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, DECRETO 2007-663 DEL 02/05/2007
e puniti dall'Art. 35 par. I 1°, par. IV Legge 2004-575 del 21/06/2004.
PARTECIPAZIONE AD UN' ASSOCIAZIONE DI MALFATTORI PER LA PREPARAZIONE DI UN CRIMINE episodi commessi dal 21 agosto 2019 al 16 dicembre 2020 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione di JUNALCO
Previsti dall'ART 450-1 Al. 1, AL. 2 C. PENALE.
e puniti dall'ART 450-1 Al. 2, ART.450-3, ART. 450-5 C. PENALE.
PARTECIPAZIONE AD UN' ASSOCIAZIONE DI MALFATTORI PER LA PREPARAZIONE DI UN CRIMINE PUNITO CON 10 ANNI DI CARCERE episodi commessi dal 21 agosto 2019 al 16 dicembre 2020 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione di JUNALCO
Previsti dall'ART 450-1 Al. 1, AL. 2 C. PENALE.
e puniti dall'ART 450-1 Al. 2, ART.450-3, ART. 450-5 C. PENALE.
FORNITURA DI PRESTAZIONI DI CRITTOGRAFIA CON LO SCOPO DI ASSICURARE DELLE FUNZIONI DI RISERVATEZZA SENZA DICHIARAZIONE CONFORME episodi commessi dal 21 agosto 2019 al 16 dicembre 2020 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione di JUNALCO
Previsti dall'ART. 35 par. III, ART 31 par. I, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, ART. 8 DECRETO 2007-663 DEL 02/05/2007
e puniti dall'Art. 35 par. III, par. IV Legge 2004-575 del 21/06/2004.
FORNITURA DI UN MEZZO DI CRITTOGRAFIA CHE NON ASSICURA ESCLUSIVAMENTE DELLE FUNZIONI DI AUTENTICITÀ E DI CONTROLLO D'INTEGRITÀ SENZA DICHIARAZIONE PREVENTIVA fatti commessi dal 21 agosto 2019 al 16 dicembre 2020 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione di JUNALCO
Previsti dall'ART. 35 par. I 1°, ART 30 par. III, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, DECRETO 2007-663 DEL 02/05/2007
e puniti dall'Art. 35 par. I 1°, par. IV Legge 2004-575 del 21/06/2004.
IMPORTAZIONE DI UN MEZZO DI CRITTOGRAFIA CHE NON ASSICURA ESCLUSIVAMENTE DELLE FUNZIONI DI AUTENTICITÀ E DI CONTROLLO D'INTEGRITÀ SENZA DICHIARAZIONE PREVENTIVA fatti commessi dal 21 agosto 2019 al 16 dicembre 2020 a ROUBAIX e sui dipartimenti del NORD e di PASSO-DI-CALAIS, sulla giurisdizione di JUNALCO
Previsti dall'ART. 35 par. I 1°, ART 30 par. III, ART. 29 Legge 2004-575 del 21/06/2004. ART.3, ART. 4, ART. 5, DECRETO 2007-663 DEL 02/05/2007
e puniti dall'Art. 35 par. I 1°, par. IV Legge 2004-575 del 21/06/2004.

Visti gli articoli 706-95-11 a 706-95-19 del Codice di procedura penale,

Visti gli articoli 706-102 e 706-102-5 del Codice di procedura penale,

Visto l'articolo D15-6-1 del Codice di procedura penale,

Visto il Decreto n° 2015-1700 del 18 dicembre 2015 relativo all'acquisizione di dati informatici intercettati in applicazione dell'articolo 706-102-1 del codice di procedura penale,

Vista la commissione rogatoria del 20 agosto 2019 consegnata dalla dott.ssa Valérie CULIOLI, giudice d'istruzione al tribunale giudiziario di Lilla al Direttore dell'Ufficio centrale di lotta contro la criminalità legata alle tecnologie dell'informazione e della comunicazione sotto i riferimenti seguenti: N° Procura: 19043000263 – N° istruttoria: JICJIRSBC19000006-identificativo giustizia: 1900451491T

Vista la commissione rogatoria complementare consegnata il primo aprile 2020 dalla dott.ssa Valérie CULIOLI, giudice d'istruzione al tribunale giudiziario di Lilla al Direttore centrale della polizia giudiziaria sotto i riferimenti seguenti: N° Procura: 19043000263 – N° istruttoria: JICJIRSBC19000006-identificativo giustizia: 1900451491T

Vista la decisione di proroga del termine della commissione rogatoria consegnata dal dottor M Marc CHEMIN, vice presidente incaricato dell'istruttoria al tribunale giudiziario de LILLA il 22 ottobre 2020;

Visto il già trasmesso di Brice HANSEMANN, Aline BATOZ, Matthieu BONDUELLE, vice presidenti incaricati dell'istruttoria al tribunale giudiziario di Parigi e Marine FONTANGE, giudice d'istruttoria al tribunale giudiziario di Parigi, indirizzato al Direttore della direzione centrale della polizia giudiziaria l'11 dicembre 2020 ai fini del proseguimento delle indagini;

Vista la nostra ordinanza del 17 dicembre 2020 recante autorizzazione della predisposizione di un dispositivo tecnico di acquisizione di dati informatici;

Vista la nostra commissione rogatoria del 17 febbraio 2020 al Direttore della Direzione centrale della polizia giudiziaria ai fini dell'esecuzione della nostra ordinanza suddetta;

Vista la relazione del commissario di polizia Omar Merchi, capo aggiunto dell'OCLCTIC del 24 febbraio 2021;

Vista la nostra ordinanza di comunicazione al procuratore della Repubblica del 24 febbraio 2021;

Visto il parere favorevole del procuratore della Repubblica del 24 febbraio 2021 in vista della predisposizione del dispositivo di acquisizione;

Dato che l'attività del sito internet di SkyECC (disponibile in open-source) permette di raccogliere le informazioni seguenti:

- La società Sky ECC ha messo in linea una versione francese del suo sito, con lo scopo di indirizzarsi ad una clientela francofona (https://www.skyecc.store/index_fr.php?c=yes&l=fr);
- L'argomento principale è la riservatezza del sistema di comunicazione proposta;
- L'argomentazione del business porta su una sistema di comunicazione con crittografia da inizio alla fine -end to end-, affidabile nel resistere ai tentativi di cifratura tramite forza bruta – testo esaustivo delle combinazioni di una cifratura dall'utilizzazione di potenza di calcolo-, con chiavi di cifratura unicamente memorizzati nel dispositivo, e dati pertanto consultabili esclusivamente dal mittente e dal destinatario;
- È possibile fare domanda per entrare a far parte della rete di rivenditori di SkyECC trovandosi in Francia;
- Le coordinate disponibili sul sito per ordinare un dispositivo o beneficiare di un supporto passano tramite l'applicazione Wickr Messenger, essa stessa crittografata, o direttamente tramite un ID su SkyECC; la pagina di contatto è un formulario che non fornisce le coordinate dell'interlocutore;
- Le soluzioni di pagamento proposte integrano effettivamente delle monete virtuali (Bitcoin, Ethereum), o delle applicazioni di bonifico online (Paypal, Wire transfer);
- La politica di rispetto degli obblighi legali e in particolare di risposta alle sollecitazioni delle forze dell'ordine e delle autorità inquirenti è dettagliata in una pagina esclusivamente in inglese (https://www.skyecc.store/terms-of-use.php#law-enforcement-guidelines), che informa il lettore che le indicazioni riportate sono puramente informative e che l'operatore si riserva il diritto di cambiarle.(*" Questa guida è pubblicata solo per scopi informativi e nessuna dichiarazione deve essere costruita come una promessa o garanzia che SkyECC agirà in un determinato modo in*

*risposta a una richiesta delle forze dell'ordine. SkyECC si riserva il diritto di discostarsi dalle pratiche qui delineate qualora le circostanze lo richiedano");*

- La società si presenta come sottomessa alla legge canadese, e in particolare alle richieste emesse e convalidate dall'autorità nazionale canadese nell'ambito di richieste d'ingresso, ma annuncia di poter comunicare soltanto la data di creazione o dell'ultima utilizzazione di un conto identificato "dal suo account ID", ad esclusione di ogni dato crittografato e in particolare i messaggi o dati di contenuto, dati di identificazione, metadati, volume d'attività, indirizzi IP e geolocalizzazioni;
- Le condizioni di utilizzo stabiliscono sicuramente che il cliente abbia accesso e uso della soluzione di crittografia per "(i) la prevenzione di furti di identità, pirateria informatica, attacchi maligni o spionaggio; (ii) la tutela dei propri diritti alla riservatezza; e (iii) il funzionamento sicuro dei propri legittimi affari personali o d'affari, e non per qualsiasi uso illecito, illegale o criminale", sia che la comunicazione riservata deve permettere di proteggersi dagli attacchi informatici, di preservare la vita privata o le attività lecite dell'utilizzatore, ad eccezione di usi illeciti, illegali o criminali; pertanto, questa indicazione non si accompagna da nessun controllo effettivo percettibile;
Dato che la soluzione di crittografia SkyECC sembrava presentasse le caratteristiche di uno strumento utilizzato principalmente nell'ambito di attività rilevanti della criminalità organizzata e in particolare nel campo dell'articolo 706-73 del codice di procedura penale.

Dato che le inchieste condotte sia dalle autorità belghe e olandesi sia dai servizi di inchiesta francesi dimostrano il carattere particolarmente opaco e selettivo del sistema di vendita di dispositivi della soluzione crittografata SkyECC; che è in effetti emerso che le transazioni che hanno portato all'acquisto di un dispositivo si effettuavano mediante un costo molto elevato se non proibitivo per una clientela ordinaria ( parecchie migliaia di euro per una durata limitata di alcuni mesi: un tale prezzo per rendersi anonimi non può essere manifestatamente consentito che da persone che percepiscono dei redditi consistenti) (cf D8), e, ciò dopo una presa di contatto tramite il sito internet della società canadese SKY GLOBAL Technologies Inc, funzionante come una semplice casella postale: che inoltre, la vendita effettiva dei dispositivi che possiedono il sistema crittografato SkyECC era in seguito realizzata in delle condizioni clandestine che garantiscono da una parte l'anonimato di venditore e di acquirente e impedendo d'altra parte qualsiasi tracciabilità per i pagamenti in contanti; che queste condizioni oscure di acquisizione si iscrivono in una procedura "commerciale" più globale predisposta dalla società che offre il sistema di crittografia SkyECC che tende a tutelare i suoi utilizzatori da qualsiasi inchiesta delle autorità giudiziarie nei loro confronti, che infatti è menzionato espressamente sul sito internet della società canadese Sky GLOBAL Technologies Inc., a destinazione delle forze dell'ordine suscettibili di richiederla per ottenere informazioni sui suoi utilizzatori e sul contenuto dei messaggi, che essa non ne conserva alcuno ad eccezione della data di creazione del conto e quella della sua ultima utilizzazione; che si tratta di un sistema estremamente sofisticato, che in effetti, il telefono genera alla sua inizializzazione 4 chiavi di crittografia:

1 – password key. Questa chiave è generata a partire dalla password dell'utilizzatore. Essa resta sul telefono e non è mai trasmessa. Serve a cifrare la secret key memorizzata sul server (e dunque impedendo i gestori del server di decodificarla.)

2- secret key. Questa chiave è trasmessa al server e cancellata dalla memoria del telefono, essa non è mai memorizzata sul telefono. Ogni vota che il telefono ne ha bisogno, la chiede al server, l'utilizza poi la cancella. La secret key serve a decifrare la master key.

3- master key- questa chiave serve a decifrare degli elementi della base dei dati dell'applicazione memorizzati sul telefono e contenente tutte le informazioni di funzionamento e i dati utilizzatori. La master key serve a decifrare alcuni dati memorizzati nella base di dati dell'applicazione di cui la private key.

4- private key. La chiave che serve a decifrare i messaggi ricevuti da un corrispondente (messaggi crittografati dalla chiave pubblica inviata al corrispondente). (D58/49 a D58/54);

Che il Direttore dell'Agenza nazionale della sicurezza dei sistemi di informazione ha confermato che nessuna dichiarazione preventiva o richiesta di autorizzazione relativa al prodotto SKY ECC non è stata disposta presso dei servizi ai sensi del decreto n° 2007-663 del 2 maggio 2007adottato per l'applicazione degli articoli 30, 31 e 36 della legge n° 2004-575 dl 21 giugno 2004 per la sicurezza nell'economia digitale e relativa ai mezzi e alle prestazioni di crittografia (D6)

Che questi mezzi di crittografia siano la prerogativa di una criminalità di altissima intensità; che l'insieme di questi elementi portino a sospettare che questi telefoni siano destinati ad uso nell'ambito di attività criminali; che questi elementi oggettivi conducono logicamente a considerare che il sistema di telefonia possa essere venduto intenzionalmente a dei fini criminali che possono caratterizzare un'associazione di malfattori; che di fatto, l'inchiesta giudiziaria ha messo in evidenza che il sistema di telefonia crittografato SkyECC e' stato utilizzato da organizzazioni criminali che agiscono in particolare nei PAESI BASSI in BELGIO e in FRANCIA e, per alcuni, ad un livello internazionale (cf D30 in particolare);

Che a questo titolo, in particolare un telefono crittografato SkyECC è stato sequestrato nel porto di Anversa in Belgio nell'ambito di un affare di traffico di stupefacenti; che le autorità di polizia giudiziaria di Anversa hanno ugualmente fatto sapere che la soluzione crittografata SkyECC era utilizzata da parecchie organizzazioni criminali; che le richieste delle autorità giudiziarie belghe presso la società SkyECC hanno dimostrato la sua assenza di collaborazione con la giustizia; che dalle indagini realizzate presso gli operatori di comunicazioni elettroniche francesi, è emersa un'ampia utilizzazione di questo sistema crittografato sul territorio nazionale che può essere il fatto di organizzazioni criminali; che d'altronde, l'utilizzazione di questa crittografia con scopi criminali, da individui desiderosi di assicurare la perfetta sicurezza dei loro scambi cospirativi è stata constatata in un dossier di traffico di sostanze stupefacenti sulla giurisdizione interregionale specializzata di Lilla (D33)

Dato che le indagini in corso nel quadro della squadra comune di inchiesta istituita tra le autorità olandesi, belghe e francesi ( D58/30-48) hanno permesso di confermare che gli utilizzatori della soluzione crittografata SkyECC agivano nel quadro di traffico di stupefacenti ad un livello internazionale grazie al lavoro di telefonia realizzato in particolare (D58/59 a D58/83); che più particolarmente per la Francia, le inchieste hanno permesso di stabilire che questi telefoni, di cui il numero di utilizzatori varia tra 1674 e 3276 sul primo semestre dell'anno 2020 (D58/108-109), potevano essere utilizzati in vista della commissione sul territorio nazionale di crimini e delitti che entrano nel campo delle disposizioni dell'articolo 706-73 del codice di procedura penale, in particolare l'associazione di criminali con lo scopo di preparazione di reati e delitti puniti con 10 anni di carcere ( reati di importazioni e prodotti stupefacenti commessi in bande organizzate, delitti di traffico di prodotti stupefacenti) (cf D9);

Dato che le inchieste condotte nell'ambito della presente informativa giudiziaria hanno stabilito che una parte dell'infrastruttura informatica necessaria all'avvio di questo sistema di crittografia era affittato presso il provider di hosting di server OVHCLOUD e situata nei centri di elaborazione dati nella sede di questa impresa sita in via Kellermann n. 2 a ROUBAIX (59); che ne emerge che questa società è composta da parecchi servers identificati con il nome di host ns62400.ip-5.135-135.eu ( detto server principale o server 1), ns6019808.ip-188-165-14.eu ( detto server di backup o server 2) e ns61191227.ip-51-91-129.eu (detto server 3); che questi servers sono posti sotto intercettazione; che le attività di intercettazione di comunicazioni elettroniche circolanti sui collegamenti esterni (da e verso Internet) e interni ( collegamenti

che legano queste macchine direttamente su una rete interna di VRACK) di questi servers così che l'analisi del sistema di crittografia avviato dall'applicazione SkyECC permettono di stabilire che:

- Le comunicazioni, dopo aver lasciato la rete dell'operatore mobile del roaming utilizzato dai telefoni in funzione della loro localizzazione geografica, sono indirizzati da internet verso il server 2 (ns6019808.ip-188-165-14.eu);
- I messaggi di gruppo della soluzione SkyECC anche intercettati possono essere cifrati tramite l'intercettazione delle chiavi di crittografia comunicate dal creatore del gruppo a tutti i partecipanti del detto gruppo;
- La cifratura dei messaggi individuali non può essere realizzata a partire dai soli dati intercettati nel provvedimento in cui solo la parte degli elementi crittografati indirizzati dai telefoni sui servers è suscettibile di essere recuperata attraverso dei dati intercettati; l'altra parte degli elementi crittografati essendo unicamente memorizzata sui telefoni,

Dato che nell'ambito della squadra comune di inchiesta, gli investigatori e i tecnici olandesi hanno messo a punto una tecnica suscettibile di permettere di ottenere gli elementi crittografati memorizzati su ciascun telefono che utilizza l'applicazione SkyECC; che questa tecnica, basata sull'installazione di un server che svolge il ruolo di "Man in The Middle" "Uomo nel Mezzo" ( server detto MITM) posizionato sul collegamento esterno del server 2 (ns6019808.ip-188-165-14.eu), consiste nel ricevere tutto il traffico dei telefoni a destinazione del server 2 e tutto il traffico del server 2 a destinazione dei telefoni; che ne risulta che quando un telefono SkyECC si autentica sul server 2, il MITM genera a destinazione di questo telefono un messaggio di notifica di tipo push, specialmente realizzato e normalmente invisibile, che ha per solo scopo di incitare il telefono a comunicare in ritorno gli elementi crittografati necessari alla decifratura dei messaggi individuali ricevuti da questo telefono; che questi elementi sono intercettati dal dispositivo MITM ma non rinviati al server 2; che tutte le altre comunicazioni dei telefoni sono trasmessi verso il server 2 e vice versa senza alcuna modifica di modo che il servizio di comunicazioni crittografate continua a funzionare normalmente;

Dato che questo dispositivo ha ricevuto l'autorizzazione n° 2011 F 1434 ( valida fino al 30/11/2026) consegnata dalla commissione consultativa incaricata di emettere un parere sui materiali suscettibili di recare violazione alla riservatezza della vita privata e al segreto delle corrispondenze (articolo R.226-2 del Codice penale) durante la sessione del 12 novembre 2020; che gli inquirenti già indirizzati confermavano dunque che i dispositivi SkyECC erano utilizzati a dei fini criminali che essendo impossibile l'analisi dei dispositivi, solo l'avvio di un dispositivo di acquisizione di dati informatici permetterebbe di eludere la crittografia dei dati scambiati dagli utilizzatori, questi transitando tutti dal server impiantato a ROUBAIX; che il ricorso a questo dispositivo, ad integrazione dell'intercettazione dei servers già avviati, costituisce l'unico mezzo di decifrare i messaggi individuali degli utilizzatori del sistema di crittografia SkyECC dedicandosi a delle attività illecite e pervenire così alla manifestazione della verità; che la misura di acquisizione appare infatti necessaria per determinare il livello di utilizzazione criminale che è fatto di questo sistema e di identificare tutti i dirigenti della società SKY GLOBAL Technologies Inc., il loro legame tra loro e con le più importanti organizzazioni criminali; che questa misura appare dunque necessaria per determinare la volontà degli organizzatori di fornire in tutta conoscenza di causa un mezzo di comunicazione riservato che permetta di esercitare delle attività illecite; che l'utilizzazione di questa procedura tecnica è perfettamente proporzionata alla gravità delle infrazioni evocate sopra;

Dato che la suddetta seguente nostra ordinanza del 17 dicembre 2020, è stata autorizzata, ai sensi degli articoli 706-102-1 e 706-102-5 del codice di procedura penale, l'avvio di questo dispositivo nel

centro di rielaborazione dati RBX2 del provider hosting OVHCLOUD all'indirizzo suddetto sul collegamento esterno ( da e verso internet) del server identificato dal suo nome di host ns6019808.ip-188-165-14.eu ( detto server 2) al fine di acquisire gli elementi crittografati di ogni telefono utilizzando il sistema di crittografia SkyECC, che una volta combinati con gli elementi crittografati provenienti dalle intercettazioni permetteranno di decifrare i messaggi individuali ricevuti da questi telefoni;

Che questo dispositivo era connesso su questa linea il 18 dicembre 2020 dalla società OVHCLOUD e attivata lo stesso giorno; che dopo tre giorni di testi e memorizzazioni, l'acquisizione dei segreti crittografati dei telefoni IOS dotati del sistema di crittografia SkyECC e essendo stati acquisiti prima della portata alla luce del 03 dicembre 2020, raggiungeva il suo ritmo di crociera; che il 13 gennaio 2021 era attivata l'acquisizione dei segreti crittografati dei telefoni Android dotati del sistema di crittografia SKYECC; che l'11 febbraio 2021, l'acquisizione dei segreti crittografati dovendo permettere la cifratura dei messaggi di gruppo emessi e ricevuti dai telefoni IOS facendo uso dell'applicazione SkyECC era attivata a suo giro; che infine il 15 febbraio 2021 era attivata l'acquisizione dei segreti crittografati dei telefoni IOS dotati della soluzione di crittografia SKYECC e essendo stati acquisiti dopo la portata alla luce del 3 dicembre 2020, questi segreti dovevano permettere la cifratura dei messaggi individuali ricevuti da questi telefoni e estratti dai dati intercettati;

Dato che il 19 febbraio 2021, le squadre tecniche olandesi notavano un calo significativo e continuo del numero dei messaggi crittografati passando da 300 000 a 40 000 messaggi intercettati crittografati ogni ora; che parallelamente il tasso di acquisizione dei segreti crittografati dei telefoni IOS diminuiva di un fattore 10;

Che le indagini tecniche sui dati intercettati hanno permesso di stabilire che nell'infrastruttura ci sono state delle modifiche e che il flusso di messaggi crittografati non passava più unicamente dal server 2 (ns6019808.ip-188_165.eu) ma ugualmente dal server 1 ( **ns624000.ip-5.135.135.eu**); che questo server essendo ugualmente intercettato, i messaggi sono registrati ma a causa di questa modifica, la loro cifratura non è più compatibile con la catena dell'elaborazione predisposta;

Che questa modifica genera ugualmente un rallentamento importante dell'acquisizione dei segreti crittografati dal dispositivo di acquisizione installato sulla linea esterna del server 2;

Dato che la sola opzione possibile per correggere gli effetti di questa modifica d'infrastruttura consiste nell' installare un secondo dispositivo di acquisizione, identico al primo ( il cui dispositivo ha ricevuto l'autorizzazione n° 2011 F 1434, valida fino al 30/11/2026, dalla commissione consultativa incaricata di emettere un avviso sui materiali suscettibili di violare la riservatezza della vita privata e al segreto delle corrispondenze dalla sessione del 12/11/2020, come indicato sopra), sulla linea esterna del server 1;

Che conviene ricordare che l'acquisizione è l'unico mezzo per pervenire ai risultati scontati, tali che i menzionati sopra, che non potrebbero essere ottenuti dal solo aiuto delle intercettazioni ( di server, di linee telefoniche – n° MSISDN-, o ancora degli involucri telefonici -n° IMEI-); che l'avvio di questa tecnica di inchiesta digitale, utile alla manifestazione della verità, è perfettamente proporzionata alla gravità dei fatti indicati dalla procedura in corso, e ai fini perseguiti trattandosi di un'associazione di criminali in vista della preparazione di reati e delitti puniti con dieci anni di carcere.

Dato che conviene autorizzare l'installazione nel centro di elaborazione dati RBX2 del provider host OVHCLOUD situato in via Kellermann n. 2 a ROUBAIX (59), di questo secondo dispositivo di acquisizione sulla linea esterna ( da e verso internet) del server 1 di cui il nome host è **ns624000.ip-5.135.135.eu** e questo per un periodo che va fino alla fine del periodo autorizzato per il primo dispositivo di acquisizione, i due dispositivi dovendo essere collegati tra loro e sincronizzati;

## PER QUESTI MOTIVI

AUTORIZZIAMO tramite commissione rogatoria distinta in data odierna, il Direttore della Direzione centrale della Polizia giudiziaria, o qualsiasi ufficiale di polizia giudiziaria o sotto la propria responsabilità qualsiasi agente di polizia giudiziaria, da lui designato, a mettere qua e là nel centro rielaborazione dati RBX2 del provider host OVHCLOUD presso la sede di questa società situata in via Kellermann n. 2 a ROUBAIX (59) un dispositivo di acquisizione sulla linea esterna ( da e verso internet) del server 1 il cui nome d'host è **ns624000.ip-5.135.135.eu;**

In vista del suo avvio, AUTORIZZIAMO la trasmissione tramite una rete di comunicazioni elettroniche;

AUTORIZZIAMO ugualmente l'utilizzazione del detto dispositivo;

AUTORIZZIAMO questa tecnica speciale di inchiesta per una durata di **QUATTRO (04) mesi** dall'avvio effettivo del dispositivo;

Redatto nel nostro ufficio, Il 24 febbraio 2021
Il vice presidente incaricato dell'Istruzione
M. Brice HANSEMANN
Tribunale giudiziario di Parigi

Copia della presente ordinanza è stata consegnata al Procuratore della Repubblica
Il 25 febbraio 2021
Il cancelliere