P R O C U R A G E N E R A L E
DELLA CORTE DI CASSAZIONE

MEMORIA PER L'UDIENZA DELLE SEZIONI UNITE PENALI DEL 29 FEBBRAIO 2024 NEI RICORSI n. ***/2023 R.G. e n. *****/2023 R.G.**

IL PROCURATORE GENERALE

nelle persone dell'Avvocato Generale, dott. Pietro Gaeta, e del Sostituto Procuratore Generale, dott. Luigi Giordano, osservano quanto segue.

La presente memoria costituisce una sintesi scritta della requisitoria orale che sarà esposta all'udienza del 29 febbraio p.v. Essa ha il precipuo scopo di anticipare, a beneficio dei signori Avvocati difensori degli imputati, contenuti e conclusioni della requisitoria orale, per meglio sviluppare il contraddittorio di udienza.

Vengono all'esame di codesto Onorevole Consesso due distinti ricorsi, che, ancorché formalmente separati, ben possono essere trattati congiuntamente in ragione della sicura comunanza delle questioni di diritto prospettate. La presente memoria è organizzata secondo il seguente schema espositivo, di tipo modulare al fine di agevolarne la lettura: una prima parte riassume i motivi veicolati nei due ricorsi in trattazione, con esposizione sintetica delle rispettive vicende processuali; una seconda parte passa in rassegna i diversi orientamenti giurisprudenziali già prospettati sui profili problematici oggetto del contrasto; la terza parte, infine, espone una rassegna critica delle soluzioni possibili alle questioni di diritto ed argomenta sulla soluzione sostenuta dall'ufficio di Procura Generale.

PARTE PRIMA
Sintesi dei ricorsi e delle vicende processuali.

1. Ricorso rg n. ***** del 2023 nell'interesse di G---- E-----

Il primo ricorso in trattazione (RG *****2023) è proposto dai difensori di G---- E----- avverso l'ordinanza con cui il Tribunale del riesame di Potenza ha rigettato l'istanza di

riesame volta ad ottenere l'annullamento dell'ordinanza applicativa della misura coercitiva della custodia cautelare in carcere emessa dal giudice per le indagini preliminari, in relazione ai reati di cui agli artt. 73 e 74 del d.P.R. n. 309 del 1990. Con ordinanza n. *****/23 del 3/11/2023, depositata il 30/11/2023, la Terza Sezione penale della Corte di cassazione ha rimesso gli atti del procedimento indicato in epigrafe alle Sezioni Unite, formulando i seguenti quesiti di diritto:

a) Se l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato attraverso un ordine europeo d'indagine presso un'autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisca acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-bis cod. proc. pen. o di documenti ex art. 234 cod. proc. pen. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove.

b) Se l'acquisizione di cui sopra debba essere oggetto, ai fini della utilizzabilità dei relativi dati, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della Autorità Giurisdizionale nazionale.

Con decreto della Prima Presidente del 13/12/2023, le questioni sono state rimessa all'esame delle Sezioni Unite per l'udienza del 29/02/2024

1.1. - I motivi di ricorso.

L'indagato G---- E----- ha proposto ricorso per cassazione avverso l'ordinanza del Tribunale di Potenza depositata il 24/07/2023, che ha rigettato l'istanza di riesame volta ad ottenere l'annullamento dell'ordinanza applicativa della misura coercitiva della custodia cautelare in carcere emessa dal giudice per le indagini preliminari in relazione ai reati di cui agli artt. 73 e 74 del d.P.R. n. 309 del 1990.

1.1.1. Con il primo motivo, il ricorrente ha dedotto la violazione degli artt. 191 e 234-*bis* cod. proc. pen. Al riguardo, ha premesso che "*non può revocarsi in dubbio che l'acquisizione di dati informatici sui server della società Sky Global relativi alle conversazioni già intercorse mediante lo strumento Sky-Ecc non sia riconducibile alle intercettazioni, bensì a documenti informatici*". Tali documenti sono stati ottenuti mediante ordine europeo di indagine "*per la cui emissione è imposto dall'art. 6 della direttiva 2014/41/UE che l'atto di indagine richiesto debba essere emesso alle stesse condizioni di un caso interno analogo*". A questo proposito non sarebbe pertinente il riferimento alla previsione dell'art. 234-*bis* cod. proc. pen., che riguarda l'acquisizione dei dati direttamente presso il privato avente sede in altro Stato e con il suo consenso. Neppure sarebbe configurabile il presupposto del "*consenso del legittimo titolare*" degli stessi richiesto da questa disposizione. Pur se la norma non chiarisce la figura del legittimo titolare dei dati, tale soggetto, comunque, non sarebbe individuabile, né negli *internet service provider*, i quali non

hanno il potere di acconsentire alla divulgazione dei dati dei propri utenti ai sensi dell'art. 32 della Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001, né nel pubblico ministero francese.

1.1.2. Con il secondo motivo, è stata dedotta l'inutilizzabilità dei dati acquisiti mediante ordine europeo d'indagine per la violazione degli artt. 191 cod. proc. pen., 27 Cost. e 6 CEDU. Qualificando le *chat* come prova documentale, deve rilevarsi che sono stati messi a disposizione della difesa "*i soli esiti dell'attività svolta all'estero e non anche il percorso di acquisizione di quei dati*"; anzi, nel caso di specie, sono stati acquisiti solo "*gli esiti di una consulenza tecnica avente ad oggetto la decifratura delle chat criptate a mezzo di una chiave di cifratura*", senza permettere alle difese di verificare la fase di formazione della prova e , dunque, "*la legittimità delle risultanze assunte*". Nonostante la consegna di tale materiale sia passata attraverso ordini europei di indagine, "*tale procedura non può sostituirsi al controllo dell'autorità giudiziaria sulla legittimità del processo di formazione della prova*". È stato aggiunto che l'affermazione del Tribunale del riesame circa la superfluità della conoscenza dei file originari e della chiave di decifratura - assunta sul presupposto per cui l'utilizzo di un algoritmo non conforme avrebbe condotto all'elaborazione di espressioni prive di senso - avrebbe determinato una violazione del diritto di difesa perché, di fatto, avrebbe impedito la verifica delle modalità di acquisizione del dato, in contrasto "*con l'inviolabile diritto di difesa*".

1.1.3. Con il terzo motivo, è stata dedotta la mancanza della gravità indiziaria e la manifesta illogicità della motivazione dell'ordinanza impugnata per avere il Tribunale del riesame ingiustamente qualificato il ricorrente come "partecipe" dell'associazione di cui all'art. 74 del d.P.R. n. 309 del 1990, senza illustrare adeguatamente i dati investigativi da cui dovrebbe desumersi la sua presenza al momento della consegna del danaro ad un agente sotto copertura e, comunque, senza indicare ragioni sufficienti a dimostrare la provenienza illecita della somma e la consapevolezza della illiceità della transazione.

1.1.4. Con il quarto motivo, il ricorrente ha proposto, ai sensi dell'art. 267 del Trattato sul funzionamento dell'Unione europea (TFUE), una questione pregiudiziale da sollevare innanzi alla Corte di giustizia europea.

La premessa della questione è che "*non si dubita*", nel caso in esame, che, con ordine europeo d'indagine emesso dal pubblico ministero interno, sono stati acquisiti dati elettronici già in possesso dell'autorità estera di esecuzione. Tali dati, "*conservati nei server della società Sky Global*", sarebbero stati acquisiti dalla polizia o dall'autorità giudiziaria francese "*come dati già esistenti al momento delle attività poste in essere dalle squadre investigative comuni e non come flussi di comunicazione in atto*".

L'autorità di emissione dell'ordine europeo di indagine, ai sensi dell'art. 6, § e 2, della direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale, deve garantire il rispetto dei diritti della persona indagata o imputata e certificare che l'ordine emesso sia proporzionato e necessario.

Nel caso di specie, l'attività di acquisizione dei dati elettronici avviata dal pubblico ministero italiano sarebbe lesiva dei diritti fondamentali della persona e del principio di proporzionalità: l'adozione di ordine europeo di indagine ha reso possibile l'acquisizione dei dati senza verificare il presupposto del grave reato, ormai richiesto dall'art. 132 del d.lgs. n. 196 del 2003 e senza rispettare i limiti temporali dell'accesso da parte dell'autorità pubblica, con la conseguenza che "*come attualmente impiegato, l'ordine europeo di indagine consentirebbe di ottenere uno standard di tutela nettamente inferiore rispetto … agli strumenti interni …*".

La direttiva 2002/58/UE relativa alla vita privata e alle comunicazioni elettroniche e gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, infatti, consentono l'accesso dell'autorità pubblica a tali dati solo per l'obiettivo della lotta contro forme gravi di criminalità e di prevenzione di gravi minacce per la sicurezza pubblica come ormai precisato dalla giurisprudenza europea (il riferimento è a CGUE del 2 marzo 2021, H.K. c. Prokuratuur).

Ne consegue la formulazione del seguente quesito eventualmente da sottoporre alla Corte di Giustizia: "*Se l'art. 6 paragrafo 1 della direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale, letto alla luce degli artt. 7, 8, e 11 nonché 52 par. 1, della carta dei diritti fondamentali dell'Unione europea, deve esser interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'acquisizione di dati elettronici relativi al traffico e relativi all'ubicazione già in possesso della autorità di esecuzione e la acquisizione di dati elettronici relativi al traffico e relativi alla ubicazione contenuti in basi di dati della polizia o delle autorità giudiziarie, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sulla ubicazione di apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto nonché dalla quantità o dalla natura dei dati disponibili per tale periodo*".

Con il medesimo motivo, poi, è stato rappresentato un'ulteriore punto critico. Ritenendo utilizzabili i dati elettronici, concernenti il traffico, l'ubicazione dell'utenza, ma anche il contenuto delle comunicazioni, con ordine europeo di indagine da parte del pubblico

ministero si permetterebbe a quest'ultimo - parte nel processo, dunque, soggetto privo del necessario requisito di indipendenza ed imparzialità - di acquisire tali dati senza la previa autorizzazione del giudice. "*Il bilanciamento tra interessi e diritti fondamentali in gioco* [invece] *può essere garantito solo da un'autorità che abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati virgola di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo di qualsiasi influenza esterna*". Riconoscendo al pubblico ministero l'accesso diretto ai dati personali conservati dai fornitori dei servizi di comunicazione, pertanto, si riterrebbero utilizzabili nel processo penale prove ottenute in modo illegittimo, con pregiudizio dell'indagato o imputato.

Su queste premesse è stato formulato il seguente ulteriore quesito da porre alla Corte europea: "*Se dal diritto dell'Unione Europea, in particolare dal principio di effettività, discenda che le violazioni di tale diritto verificatesi nell'ambito dell'acquisizione di elementi investigativi o di prove in un procedimento penale nazionale non possono rimanere del tutto prive di conseguenze anche nel caso di reati gravi e devono quindi essere prese in considerazione a favore dell'imputato quantomeno sul piano della valutazione delle prove e della determinazione della pena*".

1.1.5. Con memoria depositata il 31/01/2024, sono stati depositati motivi nuovi nell'interesse del ricorrente.

1.2. - L'ordinanza di rimessione.

La Terza Sezione penale, con ordinanza n. *****/23 del 3/11/2023, depositata il 30/11/2023, per la rilevanza della questione e per l'esistenza di un contrasto giurisprudenziale sui temi controversi riguardanti l'acquisizione e l'utilizzabilità dei dati informatici scambiati con l'utilizzo di sistemi telematici definiti "criptofonini", ha rimesso gli atti alle Sezioni Unite ai sensi dell'art. 618 cod. proc. pen., al fine di stabilire:

a) Se in tema di mezzi di prova l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante Ordine europeo di indagine, presso Autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisca acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-*bis* cod. proc. pen. o di documenti ex art. 234 cod. proc. pen. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove;

b) Se, inoltre, tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte della Autorità giurisdizionale nazionale.

1.3. - La descrizione dell'attività investigativa compiuta.

Il presente procedimento riguarda l'attività di un'organizzazione criminale dedita al traffico internazionale di stupefacenti di vario tipo, costituita da una pluralità di persone per lo più di nazionalità albanese e legati da stretti vincoli parentali, insediatisi nel Comune di Scanzano Ionico ed in altre località nazionali (pag. 20 e ss. dell'ordinanza impugnata).

Le indagini, compiute anche con l'ausilio di un agente *undercover*, hanno svelato un numero notevole di transazioni aventi ad oggetto droga ed hanno condotto ad una pluralità di sequestri di stupefacenti, tra i quali anche alcuni quantitativi di 6-MAM (6-monoacetilmorfina), una sostanza che "*permette di avere un'efficacia psicoattiva maggiore rispetto all'esposizione all'eroina comune poiché agisce in maniera diretta sull'encefalo*" (pag. 28 dell'ordinanza), definita "*eroina killer*" o "*super eroina*" (cfr. pag. 23 dell'ordinanza del Gip di Potenza del 12/06/2024).

In particolare, "*l'attività investigativa esperita, concretizzatasi soprattutto in un'intensa attività di intercettazione ad ampio raggio, ha investito la totalità delle comunicazioni intrattenute tra i soggetti, avvenute sia secondo modalità tradizionali … ovvero mediante il traffico di informazioni a mezzo sms o chat, quest'ultimo intercorse tra parecchi telefonici del tipo iPhone mediante l'utilizzo dell'applicativo di cripto chat denominato Sky-Ecc"* (pag. 28 dell'ordinanza). Gli indagati, infatti, utilizzavano anche "*criptofonini anti-intercettazioni*" (pag. 31 dell'ordinanza).

La polizia giudiziaria, in un primo momento, ha raccolto indizi che dimostravano il coinvolgimento dei principali indagati - i fratelli H____ - nel circuito del narcotraffico internazionale. In questo contesto, dopo uno scambio di informazioni con la Procura distrettuale della Repubblica di Trento, è emersa la figura dell'attuale indagato G---- E-----, il quale, con H____, ha consegnato il 19 giugno 2020 a Scanzano Ionico ad un agente sotto copertura la somma di € 150.000 da destinare all'acquisto di sostanze stupefacenti destinata alla cessione anche ad altri gruppi criminali. Questa operazione è stata oggetto di una attività di osservazione della polizia giudiziaria (pag. 25 dell'ordinanza cautelare del Gip di Potenza).

Il Gip del Tribunale di Potenza, quindi, ha autorizzato intercettazioni telefoniche con provvedimento del 13 gennaio 2021, cui ha fatto seguito un altro provvedimento autorizzativo, oltre che di proroga delle captazioni. È così stato accertato l'utilizzo da parte degli indagati di "criptofonini".

È emerso, infatti, che H_____ utilizzava uno smartphone *iPhone* per l'accesso al network *Sky-ECC* (cfr. pag. 33 dell'ordinanza impugnata; pag. 27 dell'ordinanza genetica del Gip di Potenza).

È stato intercettato il dispositivo *iPhone* associato al pin E10F7C, ottenendo, peraltro, il solo *positioning* che, peraltro, permetteva di ricavare le direttrici di spostamento degli indagati (cfr. pag. 24 dell'ordinanza del Gip di Potenza del 12/06/2024).

All'attuale ricorrente G---- E-----, oggetto di servizi di osservazione, pedinamento e controllo, oltre che di intercettazione anche di SMS, invece, è stato attribuito in modo certo il "criptonimo" "I VOGLI", il piccolo (pag. 87 dell'ordinanza impugnata).

Con successivo ordine europeo di indagine del 9 luglio 2021 rivolto al *Tribunal Judiciarie de Paris*, sono state acquisite 23 *conversation* intrattenute nel periodo 12 dicembre 2019 - 8 marzo 2021 sul citato *iPhone*, dimostrando il coinvolgimento di diversi soggetti nell'ambito delle pratiche dei predetti indagati inerenti al traffico internazionale di stupefacenti (cfr. pag. 34 e ss. dell'ordinanza) (ALL. n. 3). Tali chat, pervenute alla Procura della Repubblica di Potenza il 6 settembre 2021, sono state tradotte da un interprete di lingua albanese.

Le *chat* intercorse sulla piattaforma criptata *Sky-Ecc* relative al presente procedimento, dunque, erano state già acquisite dall'autorità giudiziaria francese a seguito di una iniziale autorizzazione del giudice istruttore di Lille del 14 giugno 2019, cui avevano fatto seguito provvedimenti di proroga e nuove autorizzazioni tra cui quella del 17 dicembre 2020 del giudice istruttore di Parigi, nell'ambito di una complessiva operazione culminata con un intervento della polizia in data 9 marzo 2021. Tali *chat,* solo successivamente alla loro registrazione, sono state trasferite all'autorità giudiziaria italiana sulla base di un ordine europeo di indagine emesso dal Procuratore della Repubblica il 9 luglio 2021 e che ha riguardato le conversazioni di specifici utenti e un preciso arco temporale.

Tra gli atti delle indagini sono presenti i provvedimenti del giudice istruttore di Lille, a partire dal primo che risale al 14 giugno 2019, corredata con l'informativa della polizia giudiziaria e con la "*richiesta di intercettazione della corrispondenza*" del pubblico ministero presso il Tribunale di Lille, oltre che gli atti successivi (ALL. n. 1). Di questa documentazione il pubblico ministero presso il Tribunale di Potenza ha disposto, in data 6 ottobre 2022, la traduzione per mezzo di una consulenza (anch'essa contenuta in ALL. n. 1).

L'analisi della messaggistica pervenuta dall'Autorità francese ha permesso di determinare i volumi di stupefacenti importati dagli indagati; la polizia giudiziaria ha quantificato la sostanza stupefacente trafficata nel periodo temporale coerente con l'avvenuto utilizzo della piattaforma di comunicazione criptata, compreso tra il 12 dicembre 2019 e l'8 marzo 2021, **pari a 526,5 kg di stupefacente**, tra eroina cocaina e derivati dalla cannabis (cfr. pag. 31 dell'ordinanza del Gip di Potenza).

1.4. - La soluzione accolta dall'ordinanza del Tribunale di Potenza.

L'ordinanza impugnata, respingendo la tesi difensiva della assenza di autorizzazione del Gip alla effettuazione di intercettazioni con violazione dell'art. 266 e ss. cod. proc. pen. e quella, formulata in alternativa, della violazione dell'art. 234 cod. proc. pen per violazione del contraddittorio nella formazione della prova, ha ritenuto utilizzabili per la decisione i messaggi ottenuti con ordine europeo di indagine emesso dal pubblico ministero, sottolineando la natura documentale e non "captativa" delle *chat* in questione e richiamando, in tal senso, conforme giurisprudenza di legittimità, su cui di seguito ci si soffermerà. In particolare, secondo il tribunale, "*l'autorità giudiziaria estera si è resa garante del rispetto delle corrette procedure acquisitive del dato informatico volto ad impedirne l'alterazione*", sicché le prerogative difensive non risultano frustrate dalla scelta del pubblico ministero di mettere a disposizione i soli esiti delle attività svolte all'estero e non anche il percorso di acquisizione dei dati (cfr. pag. 122 dell'ordinanza).

Nel provvedimento, poi, è stato aggiunto che non è contestato dal ricorrente, come pure evidenziato illustrandone i motivi di ricorso, che si tratti di acquisizione di messaggi costituenti dati "freddi" ovvero estranei, nella loro acquisizione, ad un flusso di comunicazioni in corso e che "*il dato sia stato fornito dal Tribunale di Parigi"*, essendo, pertanto, intervenuta nell'acquisizione una autorità giurisdizionale.

1.5. – Il contrasto tra orientamenti giurisprudenziali.

La Sezione remittente ha rilevato come sia insorto un contrasto tra le Sezioni della Corte di cassazione in merito all'utilizzabilità come prova delle chat ottenute dal pubblico ministero nella forma già decriptata mediante ordine europeo di indagine rivolto all'autorità giudiziaria francese.

Dall'ordinanza impugnata, infatti, risulta che le chat intercorse sulla piattaforma criptata *Sky ECC*, gestita dalla società canadese *Sky Global*, sono state acquisite dall'autorità giudiziaria francese – in particolare, dal giudice francese - per fini di giustizia interni a seguito di una operazione internazionale eseguita dalla polizia belga in data 9 marzo 2021 e, successivamente, sono state trasmesse, in esecuzione di ordine europeo di indagine emesso dal pubblico ministero di Potenza, all'autorità giudiziaria italiana il 9 luglio 2021.

Appare opportuno segnalare, prima ancora di soffermarsi su diversi orientamenti emersi, che l'indirizzo prevalente ha ritenuto utilizzabili nel procedimento penale detti messaggi, pur dividendosi, come meglio si vedrà nel prosieguo, in merito all'individuazione della disciplina applicabile quale parametro di riferimento per sostenere tale giudizio.

Un diverso indirizzo giurisprudenziale, invece, con specifico riferimento al tema del rispetto del principio di equivalenza, escluso il ricorso alla previsione di cui all'art. 234-*bis* cod. proc. pen. per affermare l'utilizzabilità delle suddette *chat*, ha annullato con rinvio l'ordinanza cautelare fondata su dette prove, chiedendo al giudice del rinvio di chiarire quale sia stata la natura dell'attività svolta all'estero e di attribuire alla stessa la corretta qualificazione giuridica che sarebbe da ricondursi al sequestro di cui all'art. 254-*bis* cod. proc. pen. oppure alle intercettazioni previste dall'art. 266 cod. proc. pen. (Sez. 6, n. 44154 del 26/10/2023 Rv. 285284 01; Sez. 6, n. 44155 del 26/10/2023 Rv. 285284 –01).

2. Ricorso R.G. n. 41618/2023 nell'interesse di G** B*** e G**** S*****.**

Il secondo ricorso in trattazione (RG n. ****/2023) è proposto dai difensori di G____ B_____ e G____ S_____ avverso l'ordinanza con cui il Tribunale del riesame di Reggio Calabria ha rigettato l'istanza di riesame volta ad ottenere l'annullamento dell'ordinanza applicativa della misura coercitiva della custodia cautelare in carcere emessa dal giudice per le indagini preliminari, in relazione ai reati di cui agli artt. 73 e 74 del d.P.R. n. 309 del 1990. con ordinanza n. 2329/24 del 15/01/2024, depositata il 18/01/2024, la Sesta Sezione penale della Corte di cassazione ha rimesso gli atti del procedimento indicato in epigrafe alle Sezioni Unite, formulando i seguenti quesiti di diritto:

a) Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazione disposte dall'Autorità giudiziaria estera su una piattaforma informatica criptata integri, o meno, l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.

b) Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'autorità giudiziaria estera attraverso l'inserimento di un captatore informatico sul server di una piattaforma optata sia soggetta nell'ordinamento interno ad un controllo giurisdizionale, preventivo o successivo, in ordine l'utilizzabilità dei dati raccolti.

Con decreto della Prima Presidente del 22/01/2024, le questioni sono state rimesse all'esame delle Sezioni Unite per l'udienza del 29/02/2024

2.1. – I motivi di ricorso.

Gli indagati G____ B_____ e G____ S_____ hanno proposto ricorso per cassazione avverso l'ordinanza del Tribunale di Reggio Calabria depositata il 29/08/2023, che ha rigettato l'istanza di riesame volta ad ottenere l'annullamento dell'ordinanza applicativa della misura coercitiva della custodia cautelare in carcere emessa dal giudice per le indagini preliminari in relazione ai reati di cui agli artt. 73 e 74 del d.P.R. n. 309 del 1990.

2.1.1. Con il primo motivo, i ricorrenti hanno denunciato la violazione dell'art. 294 cod. proc. pen. ed il vizio di motivazione dell'ordinanza impugnata, lamentando che, nel corso dell'interrogatorio di garanzia e in sede di riesame, il pubblico ministero ha omesso la produzione di una serie di provvedimenti emessi all'interno del procedimento originario francese, con conseguente impossibilità per la difesa di comprendere le modalità di acquisizione e decrittazione dei messaggi scambiati su *Sky ECC* e transitati, dapprima, nel procedimento penale n. 1589/2019 della Procura della Repubblica di Reggio Calabria e, successivamente, nel procedimento penale n. 3886/2022 della medesima Autorità giudiziaria, relativo ad un'inchiesta denominata "*Eureka*".

2.1.2. Con il secondo motivo, è stata dedotta violazione di legge e vizio di motivazione in ordine al superamento dei termini di durata delle indagini preliminari di cui all'art. 407 cod. proc. pen., censurando, in particolare, l'affermazione del Tribunale secondo cui il procedimento non soggiace alla nuova disciplina dell'art. 335-*quater* cod. proc. pen.

2.1.3. Con il terzo motivo, i ricorrenti hanno dedotto violazione di legge e vizio di motivazione con riferimento alla procedura seguita dall'Autorità giudiziaria francese per l'acquisizione degli atti di indagine, poi trasferiti nel procedimento in oggetto a seguito di Ordine Europeo di Indagine penale (in seguito, OEI), nonché in relazione alla ritenuta utilizzabilità degli stessi da parte del Tribunale del riesame. Al riguardo, si assume che:

- sarebbe erroneo l'inquadramento giuridico dell'acquisizione delle chat nella previsione dell'art. 234-*bis* cod. proc. pen. come accolto dal Tribunale del riesame;

- l'attività svolta all'estero dovrebbe essere qualificata come "*intercettazione massiva, generalizzata e indiscriminata*" di tutte le conversazioni effettuate tramite la piattaforma criptata *Sky ECC*, in quanto tale non permessa nel nostro ordinamento;

- l'acquisizione non potrebbe essere consentita tramite OEI a mente del principio di equivalenza espresso dall'art. 6, par. 1, lett. b) della direttiva 2014/41/UE e, in ogni caso, deve ritenersi preclusa da specifiche disposizioni euro-unitarie (artt. 47, par. 2, della Carta dei diritti fondamentali, 6, par. 1 e 8, par. 2, Conv.EDU), come riconosciuto dalla Corte di Giustizia dell'Unione europea (da ultimo, sent. 2 marzo 2021, Prokuratuur, C-746/18, punto 42; sent. 6 ottobre 2020, Le Quadrature du Net e a., C-511/19, C-512/18, C/520/18, punto 223);

- non conoscendo l'ordinamento francese una disposizione analoga al nostro art. 270 cod. proc. pen., il "transito" di dette intercettazioni nel procedimento penale italiano violerebbe, sia la *lex loci*, sia le previsioni dell'art. 10, par. 5, della direttiva 2014/41/UE e

dell'art. 8, par. 2, CEDU (come ritenuto dalla Corte Edu nella pronuncia Matheron c. Francia) con ricadute nell'ordinamento interno ex artt. 117 Cost. e 191 cod. proc. pen.;

- non sussisterebbero i presupposti di utilizzabilità previsti dall'art. 270 cod. proc. pen., né sarebbero state rispettate le previsioni di cui all'art. 268, commi 6, 7 e 8, cod. proc. pen., che in relazione ai risultati delle intercettazioni prevedono l'instaurazione di un contraddittorio adeguato tra le parti dinanzi ad un organo giudicante terzo e imparziale, le indicate chat non possono ritenersi utilizzabili;

- le risultanze delle indagini espletate in Francia configurerebbero una prova atipica *ex* art. 189 cod. proc., la cui acquisizione, tuttavia, sarebbe in contrasto con i principi costituzionali e convenzionali sulla tutela del "domicilio informatico".

2.1.4. I ricorrenti hanno depositato un'istanza con cui hanno chiesto l'anticipazione del procedimento accompagnata da una memoria in cui si ricostruiscono, con ampia documentazione i termini della vicenda processuale intervenuti in Francia.

Una successiva memoria di discussione è stata poi depositata il 10/01/2024.

2.2. - L'ordinanza di rimessione.

La Sesta Sezione penale, con ordinanza n. 2329/24 del 15/1/2024, depositata il 18/1/2024, per l'esistenza di un contrasto giurisprudenziale sui temi controversi riguardanti l'acquisizione e l'utilizzabilità dei dati informatici scambiati con l'utilizzo di sistemi telematici definiti "criptofonini", ha rimesso gli atti alle Sezioni Unite ai sensi dell'art. 618 cod. proc. pen., al fine di stabilire:

1) Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'Autorità giudiziaria estera su una piattaforma informatica criptata integri, o meno, l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.;

2) Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'Autorità giudiziaria estera attraverso l'inserimento di un captatore informatico sul "server" di una piattaforma criptata sia soggetta nell'ordinamento interno ad un controllo giurisdizionale, preventivo o successivo, in ordine alla utilizzabilità dei dati raccolti.

2.3. - La descrizione dell'attività investigativa compiuta.

Il presente procedimento riguarda l'attività illecite di tre organizzazioni criminali dedite al traffico di sostanza stupefacenti e, in particolare, all'importazione in territorio calabrese di ingenti quantità di droga. Gli appartenenti alle associazioni si occupavano dello

svolgimento delle trattative per l'acquisto di carichi di stupefacenti che provenivano da Stati esteri (Sud America e Belgio) e che approdavano al porto di Gioia Tauro. Essi, poi, si occupavano di far uscire la sostanza dall'area portuale e di rivenderla a terzi. Gli affiliati ai gruppi criminali in esame, infine, provvedevano all'occultamento dei profitti illeciti, mediante investimento di questi in attività formalmente lecite o il trasferimento e il deposito in luoghi ritenuti sicuri (pag. 1 dell'ordinanza impugnata).

Nel corso delle indagini sono emersi gravi indizi di reità nei confronti degli attuali ricorrenti. In particolare, G____ B_____, nella qualità di organizzatore e finanziatore dell'associazione, dava direttive agli altri associati per far uscire lo stupefacente dal Porto di Gioia Tauro; coordinava il trasporto dello stesso su autovettura nella provincia di Reggio Calabria; finanziava parte delle importazioni di cocaina dal Sud America e gestiva la successiva commercializzazione dello stupefacente in Calabria. G____ S_____, invece, partecipava all'associazione, essendo addetto allo smercio ed al trasporto della sostanza stupefacente, nonché al trasferimento dei ricavi della vendita ai fornitori in Colombia e agli altri correi.

Il materiale indiziario derivava da complesse indagini, svolte in particolare con intercettazioni telefoniche e tra presenti, utilizzo di circuiti di videosorveglianza installati dalla polizia giudiziaria e decifrazione ed identificazione delle conversazioni della messaggistica in chat criptata utilizzata dagli associati (cfr. pag. 1 dell'ordinanza impugnata). Lo stesso ricorrente G____ S_____ ha riconosciuto di essere stato intercettato con provvedimenti eseguiti dall'agosto 2020 al 30 maggio 2022 (cfr. pag. 3 dell'ordinanza). Una caratteristica peculiare delle associazioni oggetto delle investigazioni è comunque rappresentata dall'utilizzo, per le comunicazioni riservate, di criptofonini di ultima generazione "*in quanto ritenuti, per la loro speciale sofisticate tecnologia, non captabili da parte delle forze di polizia"* (pag. 4 dell'ordinanza).

2.4. - La soluzione accolta dall'ordinanza del Tribunale di Reggio Calabria.

L'ordinanza impugnata ha ritenuto utilizzabili per la decisione i messaggi ottenuti con OEI emesso dal pubblico ministero, sottolineando la natura documentale e non "captativa" delle *chat* in questione e richiamando, in tal senso, conforme giurisprudenza di legittimità, su cui di seguito ci si soffermerà. In particolare, secondo il tribunale, "*gli OEI hanno avuto ad oggetto … la trasmissione di comunicazioni già pervenuta relativi destinatari e memorizzate nel server allocato in Francia*" (cfr. pag. 5 dell'ordinanza). Si tratta "*propriamente di atti investigativi assunti dall'autorità giudiziaria estera nel corso di autonome investigazioni dalla stessa intraprese per le quali vige la presunzione*

di legittimità dell'attività svolta" (pag. 8). Il legittimo titolare dei dati acquisiti è la persona che può giuridicamente disporne in forza di un titolo legittimo, secondo l'ordinamento giuridico del Paese estero, identificabile nella specie con l'Autorità giudiziaria francese.

Il Tribunale ha affermato, inoltre, che "*va ribadito il principio di diritto, già espresso in tema di rogatoria internazionale, secondo cui trovano applicazione, per il principio* locus regit actum *ed in conformità ai canoni di diritto internazionale della prevalenza della* lex loci *sulla* lex fori*, le norme dello stato in cui l'atto viene compiuto e non quelle del codice di rito del paese richiedente che disciplinano il processo*" (cfr. pag. 6 dell'ordinanza).

E stato sottolineato, tra l'altro, che la difesa si duole della mancata acquisizione della documentazione relativa a l'estrapolazione dei dati o informatici originali dal server "*senza tuttavia addurre elementi di una qualche consistenza (es. messaggi troncati, incompleti o dissonanti) tali da far dubitare della compromissione del dato, assumendo la censura carattere di genericità*", rivelandosi, pertanto, inidonea a "*superare la presunzione di legittimità della prova trasmessa tramite l'ordine di indagine europeo*" (cfr. pag. 7 dell'ordinanza).

2.5. – Il contrasto tra orientamenti giurisprudenziali.

La Sezione remittente ha rilevato come sia insorto un contrasto tra le Sezioni della Corte di cassazione in merito all'utilizzabilità come prova delle chat ottenute dal pubblico ministero nella forma già decriptata mediante ordine europeo di indagine rivolto all'autorità giudiziaria francese.

Dall'ordinanza impugnata, infatti, risulta che le chat intercorse sulla piattaforma criptata *Sky ECC*, gestita dalla società canadese *Sky Global*, sono state acquisite dall'autorità giudiziaria francese – in particolare, dal giudice francese - per fini di giustizia interni a seguito di una operazione internazionale eseguita dalla polizia belga in data 9 marzo 2021 e, successivamente, sono state trasmesse, in esecuzione di ordine europeo di indagine emesso dal pubblico ministero di Potenza, all'autorità giudiziaria italiana il 9 luglio 2021.

Appare opportuno segnalare, prima ancora di soffermarsi su diversi orientamenti emersi, che l'indirizzo prevalente ha ritenuto utilizzabili nel procedimento penale detti messaggi, pur dividendosi, come meglio si vedrà nel prosieguo, in merito all'individuazione della disciplina applicabile quale parametro di riferimento per sostenere tale giudizio.

Un diverso indirizzo giurisprudenziale, invece, con specifico riferimento al tema del rispetto del principio di equivalenza, escluso il ricorso alla previsione di cui all'art. 234-*bis* cod. proc. pen. per affermare l'utilizzabilità delle suddette *chat*, ha annullato con rinvio l'ordinanza cautelare fondata su dette prove, chiedendo al giudice del rinvio di chiarire quale

sia stata la natura dell'attività svolta all'estero e di attribuire alla stessa la corretta qualificazione giuridica che sarebbe da ricondursi al sequestro di cui all'art. 254-*bis* cod. proc. pen. oppure alle intercettazioni previste dall'art. 266 cod. proc. pen. (Sez. 6, n. 44154 del 26/10/2023 Rv. 285284 01; Sez. 6, n. 44155 del 26/10/2023 Rv. 285284 –01).

PARTE SECONDA

Gli orientamenti giurisprudenziali

1. – La qualificazione giuridica dell'acquisizione mediante OEI dei messaggi di chat già decriptati dall'autorità straniera: la tesi che fa riferimento all'art. 234-*bis* cod. proc. pen.

1.1. Come è stato anticipato, numerose sentenze della Corte di cassazione hanno già ritenuto utilizzabili nel procedimento penale i messaggi di chat acquisiti mediante OEI Queste pronunce, in particolare, si sono soffermate sul tema del rispetto del principio di equivalenza sancito dall'art. 6, par. 1 lett. b), della direttiva 2014/41/UE, secondo cui "*l'autorità di emissione può emettere un ordine europeo di indagine solamente quando l'atto o gli atti di indagine richiesti nell'ordine europeo di indagine avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*".

Secondo tale orientamento, il ricorso all'ordine europeo d'indagine per il conseguimento delle *chat* rispetta il suddetto principio, dovendo individuarsi nell'art. 234-*bis* cod. proc. pen. la norma interna di riferimento alla stregua della quale l'atto di indagine avrebbe potuto essere emesso in un caso analogo interno, in quanto si tratta di una acquisizione di "*documenti e di dati informatici*" (tra le tante, Sez. 4, n. 37503 del 30/05/2023 non mass.; Sez. 4, n. 38002 del 16/05/2023, non mass.; Sez. 4, n. 16345 del 05/04/2023, Liguori ed altri, non mass.; Sez. 4, n. 16347 del 05/04/2023, Rv. 284563 - 01; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Rv. 283998 - 01).

La premessa da cui muove questo indirizzo è che occorre distinguere tra operazioni di captazione del messaggio cifrato nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario - qualificabile come intercettazione di comunicazioni informatiche o telematiche ex art. 266-*bis* cod. proc. pen. - e operazioni di acquisizione del contenuto del messaggio già inoltrato, oltre che di decriptazione dello stesso, per le quali va esclusa l'applicazione della disciplina delle intercettazioni (cfr. tra le altre, in motivazione, Sez. 4, n. 16347 del 05/04/2023 Rv. 284563 - 01 cit.; Sez. 1, n. 34059 del 01/07/2022, non mass.; Sez. 6, n. 18907 del 20/04/2021, Rv. 281819 - 01 cit.; Sez. 6, n. 22417 del 16/3/2022, Rv.

283319; Sez. 6, n. 28269 del 28/05/2019 Rv. 276227 - 01; Sez. 3, n. 29426 del 16/4/2019, Rv. 276358; Sez. 5, n. 1822 del 21/11/2017, Rv. 272319).

In questo secondo caso, i messaggi integrano mera documentazione dei flussi comunicativi già avvenuti, costituendo rappresentazioni comunicative incorporate in una base materiale con un metodo digitale ovvero dati informatici che consentono la intelligibilità del contenuto di stringhe redatte secondo il sistema binario (Sez. 6, n. 18907 del 20/4/2021, Rv. 281819, cit., in motivazione; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Rv. 283998, in motivazione, e anche Sez. 1, n. 6363, non mass., in pari data). Il loro contenuto - se gli inquirenti hanno la disponibilità dell'algoritmo che consente di decriptarne il tenore ovvero se tale chiave di decodifica sia stata loro messa a disposizione dalla società che ne è proprietaria - può essere utilizzato come prova.

Nel caso di specie, peraltro, non assume rilevanza, ai fini del vaglio di legittimità del tipo di acquisizione in esame, la questione se i dati stessi siano stati acquisiti dalla magistratura straniera *ex post* o in tempo reale (quindi. come "dati freddi" o come comunicazioni in corso), perché i flussi di comunicazione, al momento in cui tali dati sono stati chiesti dall'autorità giudiziaria interna, non erano più in corso.

Secondo questa impostazione, pertanto, l'art. 234-*bis* cod. proc. pen. costituisce la norma interna che giustificherebbe il ricorso all'ordine europeo di indagine, perché viene in rilievo l'acquisizione non di un documento cartaceo o analogico, bensì di un documento inteso come "*rappresentazione comunicativa incorporata in una base materiale con un metodo digitale*" (in tal senso, tra le altre, v. in particolare Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Rv. 283998 - 01 cit.).

Il consenso all'acquisizione da parte del "legittimo titolare", previsto dalla disposizione citata come condizione per l'acquisizione dei dati o dei documenti conservati all'estero, è rinvenibile nell'assenso del soggetto che di tali dati o di tali documenti poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del Paese estero. Tale soggetto è identificabile non soltanto nella persona fisica e/o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria e nell'autorità giudiziaria, oltre che nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico o nell'*internet service provider* (in motivazione Sez. 1, n. 6364 del 13/10/2022 Rv. 283998 - 01 cit.).

1.2. L'orientamento giurisprudenziale illustrato, inoltre, ha escluso che, ai fini della utilizzabilità nel procedimento penale, occorra un ulteriore vaglio giurisdizionale interno,

anteriore o posteriore rispetto all'acquisizione dei suddetti documenti informatici, sviluppando argomentazioni che discendono dal principio del mutuo riconoscimento.

Al riguardo, è stato premesso che l'ordine europeo d'indagine - disciplinato dal d.lgs. 27 giugno 2017, n. 108, emanato per dare attuazione alla direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 - "*può anche essere emesso per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione*" (art. 1, par. 1, della direttiva), proprio come è avvenuto nella specie, perché il provvedimento del pubblico ministero italiano ha avuto ad oggetto l'acquisizione degli esiti documentali di attività d'indagine precedentemente svolta dall'autorità francese.

Quanto ai controlli che deve esperire l'autorità di esecuzione, è stato osservato che quest'ultima riconosce l'OEI, "*senza imporre ulteriori formalità e ne assicura l'esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione, a meno che non decida di addurre uno dei motivi di non riconoscimento o di non esecuzione ovvero uno dei motivi di rinvio previsti dalla presente direttiva*" (art. 9, par. 1, della direttiva).

L'utilizzazione degli atti trasmessi a seguito di attività di cooperazione internazionale, inoltre, non è condizionata da un accertamento svolto ad opera dell'autorità di emissione concernente la regolarità delle modalità di acquisizione esperite da quella di esecuzione, in quanto vige la presunzione di legittimità dell'attività svolta e spetta al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate nella fase delle indagini preliminari (in tal senso, Sez. 5, n. 1405 del 16/11/2016, dep. 2017, Rv. 269015 - 01; Sez. 2, n. 24776 del 18/05/2010, Rv. 247750 - 01; Sez. 1, n. 21673 del 22/01/2009, Rv. 243796 - 01).

L'OEI, infatti, deve eseguirsi in conformità a quanto previsto nello Stato di esecuzione per il compimento di un analogo atto di acquisizione probatoria e si deve presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo concreta verifica di segno contrario (tra le altre, sez. 6, n. 48330 del 25/10/2022, Rv. 284027, in motivazione).

Il giudice italiano dinanzi al quale fosse chiesta l'utilizzazione della prova acquisita all'estero, pertanto, non può e non deve conoscere della regolarità degli atti di esecuzione di attività di indagine compiuta dall'autorità giudiziaria straniera (nel caso di specie quella francese), giacché detta l'attività investigativa è eseguita secondo la legislazione dello Stato estero; e, a maggior ragione, ciò vale ove l'originaria attività investigativa non sia stata compiuta su richiesta dell'autorità giudiziaria italiana, ma sia stata eseguita, nell'ambito di altro

procedimento instaurato nel detto Stato, su iniziativa di quell'autorità nella sua piena autonomia, nel rispetto della sua legislazione in relazione ad altri reati.

1.3. Neppure può essere posta in dubbio la competenza all'emissione dell'ordine di acquisizione delle chat già decriptate da parte del pubblico ministero interno.

Gli artt. 6 e 9 della direttiva citata, infatti, precisano che l'OEI può avere ad oggetto solo atti d'indagine richiesti che "*avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*". L'ordinamento interno prevede la piena ed esclusiva competenza all'acquisizione di tali esiti documentali da parte del pubblico ministero, organo peraltro competente nella fase di indagine all'emissione dello stesso OEI, salve specifiche eccezioni, quali la richiesta di effettuazione di intercettazioni all'estero (art. 43 del d.lgs. n. n. 108 del 2017).

Non può essere dedotta dinanzi al giudice italiano, inoltre, la necessità di verificare che all'attività investigativa di cui si tratta nello Stato estero abbia provveduto un giudice e non un pubblico ministero in ragione della sopravvenuta disciplina interna introdotta con il d.l. n. 132 del 2021 convertito nella legge n. 178 del 2021, perché ciò che viene acquisito sono documenti informatici e non dati esteriori di una comunicazione come definiti dalla giurisprudenza (il riferimento è a Sez. U, n. 21 del 13/07/1998, Gallieri, Rv. 211196).

1.4. L'indirizzo illustrato, infine, esclude, salvo allegazione di specifici e concreti elementi di segno contrario, la sussistenza di lesioni al diritto di difesa e, in particolare, la sussistenza di alterazioni o manipolazioni dei testi captati anche in assenza della fornitura dell'algoritmo necessario, in quanto, secondo la scienza informatica, risulterebbe impossibile, ove la chiave di decrittazione non fosse corretta, ottenere un testo avente un significato intellegibile sebbene difforme da quello reale, potendosi, al più, imbattersi in una sequenza alfanumerica o simbolica (detta "stringa") priva di senso alcuno (in motivazione Sez. 4, n. 30395 del 21/04/2022 Rv. 283454 - 01; sullo stesso tema e sul diritto di difesa in tema di decrittazione di dati informatici anche Sez. 6, n. 14395 del 27/11/2018, dep. 2019, Rv. 275534 - 01).

2. - La tesi che rinvia alle previsioni dell'art. 254-*bis* o degli artt. 266 e ss. cod. proc. pen. per l'acquisizione all'estero della messaggistica criptata in chat *Sky ECC*.

2.1. Come è stato anticipato, un diverso indirizzo giurisprudenziale - espresso da due sentenze - ha escluso che possa farsi ricorso alla previsione di cui all'art. 234-*bis* cod. proc. pen. per ritenere rispettato il principio dell'equivalenza rispetto ad un caso analogo interno ed affermare l'utilizzabilità delle *chat* trasmesse dall'autorità giudiziaria straniera. Queste

sentenze hanno annullato con rinvio l'ordinanza cautelare fondata su dette prove, chiedendo al giudice del rinvio di attribuire all'attività svolta all'estero la corretta qualificazione giuridica.

Al riguardo, secondo l'impostazione accolta da queste decisioni, l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma *Sky Ecc*, se riguardante comunicazioni avvenute nella fase "statica", deve essere inquadrata nelle disposizioni in materia di perquisizione e sequestro e, in particolare, in quella di cui all'art. 254-*bis* cod. proc. pen., mentre, se avente ad oggetto comunicazioni registrate nella fase "dinamica", deve essere ricondotta alla disciplina degli artt. 266 e ss. cod. proc. pen. in materia di intercettazioni telefoniche (Sez. 6, n. 44154 del 26/10/2023, Rv. 285284 01; Sez. 6, n. 44155 del 26/10/2023 Rv. 285284 – 01).

Le sentenze citate hanno manifestato perplessità in ordine alla natura dell'attività svolta dall'Autorità giudiziaria straniera, che è consistita nell'avere "*instradato*" le "*chat su un server*" e, quindi, nel compimento di attività captative anche con l'impiego di *software* del tipo "*trojan*", che consistevano in intercettazioni che richiedono l'adozione di specifici provvedimenti da parte del giudice e non del pubblico ministero (Sez. 6, n. 44154 del 26/10/2023, cit).

È stato sostenuto che la disposizione dettata dall'art. 234-*bis* cod. proc. pen., comunque, non è applicabile se riferita ai risultati di una attività acquisitiva che, anche in attuazione della richiesta di assistenza formulata dall'autorità giudiziaria italiana, si sia concretizzata nella apprensione occulta del contenuto archiviato in un *server* ovvero nel sequestro di relativi dati ivi memorizzati o presenti in altri supporti informatici, nella disponibilità della società che gestiva quella piattaforma di messaggistica.

Siffatta attività acquisitiva va piuttosto inquadrata nelle disposizioni dettate in materia di perquisizione e sequestri, in specie nella norma dettata dall'art. 254-*bis* cod. proc. pen., riguardante le ipotesi di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni.

L'operatività dell'art. 234-*bis* cod. proc. pen. "*può ritenersi giustificata esclusivamente nell'ipotesi di acquisizione di documenti e dati informatici, intesi come elementi informativi "dematerializzati*", che preesistevano rispetto al momento dell'avvio delle indagini da parte dell'autorità giudiziaria francese ovvero che erano stati formati al di fuori di quelle investigazioni: nel caso concreto, invece, risulta in maniera sufficientemente chiara che quella acquisita è stata documentazione di attività di indagine della autorità straniera (Sez. 6, n. 44155 del 26/10/2023).

La fattispecie ex art. 234-*bis* cod. proc. pen., dunque, va delimitata alla sola acquisizione di dati informatici in ogni caso estranei, nella loro formazione, a qualsivoglia coinvolgimento di autorità investigative.

2.2. Questo indirizzo, tra l'altro, sul piano della individuazione dell'autorità legittimata ad emettere l'ordine di acquisizione della prova, ha evidenziato che, nel diritto interno, dopo alcune decisioni della Corte di giustizia dell'Unione Europea (in particolare CGUE, Grande Camera, 2 marzo 2021 H.K., C-746/18, cit.), è intervenuto in via d'urgenza il legislatore (d.l. n. 132 del 2021, convertito nella legge n. 178 del 2021) che, riformando l'art. 132 Cod. privacy, ha previsto che la procedura di acquisizione dei dati esterni di traffico telefonico e telematico esige un provvedimento autorizzatorio motivato del giudice. Ne deriverebbe che "*l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione debba essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero*".

2.3. È stato osservato, infine, che la Corte costituzionale ha esteso l'applicazione delle garanzie previste dall'art. 15 Cost., in materia di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione, anche ai messaggi elettronici (Corte Cost., sent. n. 170 del 2023). Questa decisione va considerata anche in collegamento con le posizioni assunte in materia dalla Corte Europea dei diritti dell'uomo, che ha ricondotto "sotto il cono di protezione dell'art. 8 CEDU" - ove pure si fa riferimento alla "corrispondenza" *tout court* - i messaggi di posta elettronica (Corte EDU, sent. 5/09/2017, Barbulescu c. Romania, p. 72; Corte EDU, sent. 3/04/2007, Copland c. Regno Unito, p. 41), gli SMS (Corte EDU, sent. 17/12/2020, Saber c. Norvegia, p. 48) e la messaggistica istantanea inviata e ricevuta tramite internet (Corte EDU, sent. Barbulescu, cit., p. 74). Dalla qualificazione dei messaggi come corrispondenza deriva che "*ove si delineasse un'ipotesi di sequestro, sembra poter aprire la riflessione sul necessario intervento, anteriore o postumo del giudice, per l'acquisizione all'estero dei dati comunicativi in parola*" (Sez. 6, n. 44154 del 26/10/2023, Rv. 285284 01).

3. – L'orientamento secondo cui la corrispondenza, anche informatica, già decriptata all'estero, acquisita con OEI, rientra nella previsione dell'art. 234 cod. proc. pen.

3.1. Dopo la decisione della Corte di rimettere il presente ricorso alle Sezioni Unite e nelle more della redazione dell'ordinanza di rimessione, sono state depositate ulteriori

sentenze della Corte di cassazione che hanno affrontato il tema. Queste sentenze hanno concluso per l'utilizzabilità nel procedimento penale della corrispondenza, anche informatica, già decriptata all'estero, acquisita con OEI, individuando nell'art. 234 cod. proc. pen., e non nella disposizione successiva, il parametro normativo di riferimento (Sez. 6 n. 46482 del 27/09/2023; Sez. 6 n. 46833 del 26/10/2023).

In particolare, questa impostazione ha ribadito che la disciplina delle intercettazioni non è applicabile per l'acquisizione, con ordine europeo di indagine, di specifici "dati freddi", cioè di documenti costituenti l'esito delle comunicazioni memorizzate su *server*, già acquisiti e decriptati dai giudici stranieri, in un loro procedimento autonomamente avviato e concluso.

E' stato poi osservato che, alla luce della sentenza della Corte Costituzionale n. 170 del 2023, anche la messaggistica informatica conservata, dopo la ricezione, mantiene il suo carattere di corrispondenza (dovendosi ritenere permanere, secondo la Consulta, l'interesse alla riservatezza di tale messaggistica, "*almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento storico*", così Corte cost. n. 170 del 2023).

La corrispondenza, anche informatica, nondimeno, secondo la prospettiva accolta da queste sentenze, rientra nel fuoco dell'art. 234 cod. proc. pen., dovendo, invece, escludersi il riferimento all'art. 234-*bis* cod. proc. pen. Quest'ultima norma consente l'acquisizione all'estero di documentazione digitale accessibile al pubblico (o con il consenso del titolare del documento, se non in libera disponibilità) senza ricorso alle procedure di collaborazione con lo Stato in cui i documenti sono collocati. Nella specie, invece, i dati sono stati acquisiti all'esito di una attività di collaborazione internazionale.

3.2. Quanto all'individuazione dell'Autorità che può provvedere alla emissione dell'ordine di acquisizione delle *chat*, è stato sostenuto che, nel caso in cui la prova sia già stata acquisita con atto del giudice nel Paese di esecuzione, il suo semplice trasferimento nel procedimento in Italia, può essere disposto sulla base della sola richiesta del pubblico ministero. Del resto, il trasferimento di prove tra procedimenti, anche se costituenti esito di intercettazioni (art. 270 cod. proc. pen.), nell'ordinamento interno avviene con provvedimento del pubblico ministero (Sez. 6 n. 46832 del 26/10/2023, cit.).

Sul punto, è stato giudicato non pertinente il richiamo della direttiva 2002/58/UE che "*non riguarda … la acquisizione di documentazione elettronica posta nei dispositivi personali dell'utente (o negli spazi virtuali su server in suo accesso esclusivo)*", ma concerne solo il trattamento dei dati conservati dai fornitori di servizi di comunicazione elettronica (cfr. Sez. 6 n. 46832 del 26/10/2023, che richiama CGUE, Grande Camera, 6/10/2020, Q.N. C 511/18, C 512/18

e C 520/18). La disciplina europea pretende l'intervento del giudice per l'acquisizione dei dati conservati dai gestori dei servizi per fornire garanzie sufficienti contro il rischio di abusi nell'accesso a tali dati.

3.3. Quanto agli ulteriori aspetti che il tema in esame impone di affrontare, l'indirizzo giurisprudenziale in esame ha sostenuto che, in materia di OEI, "*è pacifico che l'autorità nazionale non possa mettere in discussione la legittimità degli atti dell'autorità giudiziaria del paese richiesto anche quando si voglia ottenere il trasferimento di una prova già raccolta in un procedimento penale dello Stato di esecuzione*" (cfr. Sez. 6 n. 46832 del 26/10/2023, cit.).

I dubbi sulla violazione di diritti fondamentali della difesa, infine, sono stati reputati inconsistenti, essendo dei fondati sulla "*suggestione*" di una presunta non ostensibilità di informazioni in ragione di un preteso segreto militare abdotto dallo Stato di esecuzione. La normativa francese, invece, "*applica per l'acquisizione della messaggistica già trasmessa e conservata nei dispositivi personali regole sostanzialmente corrispondenti a quelle italiane sulle intercettazioni*" sicché, con gli OEI, *"le autorità inquirenti italiane hanno chiesto e ottenuto copie di prove raccolte in un procedimento francese con provvedimento del giudice sotto il suo diretto controllo*" (cfr. Sez. 6 n. 46832 del 26/10/2023, cit.).

4. – L'orientamento secondo cui le *chat* sono corrispondenza acquisita in una forma riconducibile nel diritto interno alla previsione dell'art. 270 cod. proc. pen.

Una successiva (almeno quanto a deposito delle motivazioni) sentenza della Corte di cassazione (Sez. 6, n. 48838 del 11/10/2023, Brunello) ha ribadito che l'acquisizione delle *chat* a seguito di OEI emesso dal pubblico ministero non sia ascrivibile al dettato dell'art. 234-*bis* cod. proc. pen., né - sebbene alle stesse debba essere riconosciuta la natura di corrispondenza e non già di meri "*documenti e di dati informatici*" - la loro acquisizione debba essere assoggettata alla disciplina delle intercettazioni informatiche o telematiche ex art. 266-*bis* cod. proc. pen., stante l'assenza di contestualità tra la trasmissione della comunicazione e l'atto acquisitivo (come rilevato, *ex plurimis*, da Sez. 4, n. 16347 del 05/04/2023, Papalia, Rv. 284563 - 01, relativa ad una fattispecie analoga).

Secondo questa prospettiva, l'attività svolta nello Stato di esecuzione consiste in intercettazioni. La richiesta del pubblico ministero con ordine europeo di indagine di trasferimento della corrispondenza e delle conversazioni intercettate tra due procedimenti penali – dunque, degli esiti del mezzo di ricerca della prova - è riconducibile in un caso analogo nell'ordinamento italiano alla previsione dell'art. 270 cod. proc. pen. per la cui

applicazione, nel caso di specie, sussistono tutti i presupposti (la rilevanza e l'indispensabilità per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza).

E' stato osservato, in particolare, come la Corte di Giustizia abbia statuito che, una volta che una prova sia stata acquisita nello spazio comune europeo e in conformità al diritto dell'Unione, la sua ulteriore circolazione, con trasferimento ad altro procedimento, non richieda una nuova autorizzazione del giudice, ma solo che sia rispettato il limite della utilizzabilità per sicurezza pubblica e repressione di gravi reati (CGUE 7 settembre 2023, A.G. - C-162/22, relativa all'utilizzazione della documentazione acquisita dal giudice presso gli operatori di telecomunicazioni in processi diversi da quello originario; CGUE 16 dicembre 2021, H.P., C-724/19, 10 in tema di ordine europeo di indagine emesso da un pubblico ministero per l'acquisizione in altro Paese di dati dagli operatori di telecomunicazione).

L'acquisizione delle chat, inoltre, non è avvenuta in contrasto con i principi fondamentali dell'ordinamento italiano. Essa costituisce l'esito di una forma di cooperazione giudiziaria in materia penale di cui all'articolo 82, § 1, TFUE, che si fonda sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie, a sua volta fondato sulla fiducia reciproca nonché sulla presunzione relativa che gli altri Stati membri rispettino il diritto dell'Unione e, in particolare, i diritti fondamentali (v., in tal senso, CGUE 11/11/2021, Gavanozov, § 54; CGUE 8/12/2020, Staatsanwaltschaft Wien, § 40; CGUE 24/10/2019, Gavanozov, § 35).

La violazione dei diritti fondamentali, del resto, è di difficile verificazione in relazione all'attività giudiziaria di uno Stato membro dell'Unione Europea, tenuto a condividere i principi fondamentali dell'ordinamento europeo, (Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, Rv. 283998; Sez. 1, n. 19082 del 13/01/2023; Costacurta, Rv. 284440, non massimate sul punto), ma la presunzione relativa ben può essere confutata in un caso specifico mediante l'allegazione di specifici e concreti elementi di segno contrario dinanzi al giudice competente.

L'utilizzabilità delle prove acquisite o il trasferimento delle prove già raccolte in uno Stato membro in esecuzione di un ordine europeo di indagine è, dunque, allo stato interamente rimessa alle scelte legislative dello Stato di emissione.

Quanto all'ordinamento italiano, viene in rilievo il disposto dell'art. 78 disp. att. cod. proc. pen., che, al primo comma, prescrive che "*la documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera può essere acquisita a norma dell'art. 238 del codice*". Tale ultima disposizione, a sua volta, consente il trasferimento da un procedimento estero ad uno

nazionale delle sole prove formate nel rispetto delle garanzie difensive previste dall'ordinamento italiano.

La sentenza illustrata, infine, ha ribadito che la direttiva unionale relativa alla vita privata e alle comunicazioni elettroniche non trova applicazione con riguardo ad intercettazioni effettuate direttamente dagli Stati membri, con accesso diretto alle utenze con provvedimento mirato, senza che sia imposto alcun obbligo di trattamento dei dati ai fornitori di servizi di telecomunicazione.

PARTE TERZA

Le osservazioni della Procura generale.

1. - Il sistema di comunicazione elettronica realizzato da *Sky Global*.

Esaurita la panoramica generale delle soluzioni offerte dalla giurisprudenza di legittimità sulle questioni in esame, occorre porre in evidenza come, per affrontare le questioni giuridiche poste alle Sezioni unite, non si possa prescindere da una sommaria descrizione del meccanismo di funzionamento dei "criptofonini" operanti sulla piattaforma *Sky ECC*, gestita dalla società canadese *Sky Global*.

Essa utilizza sofisticati metodi crittografici a più livelli di sicurezza, attivi sia sui dispositivi mobili, sia sui server intermediari, per resistere ai tentativi di intercettazione[1].

Come è stato specificato nelle ordinanze di rimessione alle Sezioni unite e nelle ordinanze impugnate in entrambi i procedimenti, gli indagati facevano uso di "criptofonini anti-intercettazione" da intendersi come *smartphone* che impiegano un *hardware* standard (in genere *Apple*, *Android* o *Black Berry*), ma che, rispetto agli apparecchi mobili tradizionali, si connotano per l'installazione di un'apposita scheda SIM e di un sistema operativo dedicato, avente particolari requisiti di sicurezza, in quanto disabilita i servizi di localizzazione (GPS, *Bluetooth*, fotocamera, scheda SD e porta USB)[2].

Le chiamate rimangono attive solo in modalità *Voice over IP* (VoiP), non avvalendosi della rete GSM, ed impiegano applicazioni di cui sono proprietarie le piattaforme stesse

---

[1] *Sky Global* era una rete di comunicazioni e un fornitore di servizi con sede a Vancouver, in Canada: uno dei suoi prodotti più importanti era l'applicazione di messaggistica sicura *Sky ECC*. Nel 2021 erano oltre 171.000 gli apparati registrati, principalmente in Europa, Nord America, diversi Paesi del Centro e Sud America – principalmente Colombia – e Medio Oriente. Un quarto degli utenti attivi si trovava in Belgio (6.000) e nei Paesi Bassi (12.000) (dati tratti da W. Nocerino, L'*acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, in *Cass. pen*. 2023, 2786).

[2] Sky ECC non è l'unico sistema di comunicazione criptata in commercio. Si pensi, solo per citarne alcuni, ad *Ennetcom, Exclu, Silent phone, Zphone, X1 e X1 black* della *Secure Group* e le piattaforme dall'azienda *Sikur* (*ivi*., pag. 2788).

(*Encrochat*, *Sky ECC, Anom, No1bc*, etc.), che permettono lo scambio di dati crittografati con una cifratura a più livelli[3].

I "criptofonini", per assicurare la riservatezza delle comunicazioni, necessitano di una dotazione di "*server*", messi a disposizione dalla compagnia che gestisce il servizio in abbonamento e che abilita gli utenti a scambiare messaggistica o chat, secondo una architettura informatica del tipo "*peer-to-peer*", che archivia i dati – oltre che sul dispositivo criptato – anche sui *server,* dedicati e protetti da algoritmi ad elevata sicurezza[4].

Sky ECC è costruito mediante architettura "*client-server*", con la conseguenza che qualunque messaggio telematico basato su tale applicativo, per poter approdare dal terminale del mittente sul "criptofonino" del destinatario, deve necessariamente transitare attraverso il *server* centrale. I dati in cui si risolvono le chat scambiate su *Sky ECC* viaggiano cifrati sulla rete internet.

Nelle ordinanze impugnate sono descritte una serie di funzioni che i criptofonini consentono e che appare opportuno evidenziare:

- utilizzo di sistemi di cifratura avanzata, sia dei dati memorizzati, sia del canale di comunicazione;

- volatilità dei messaggi con la possibilità, anche da parte di un terzo, di effettuare da remoto sul dispositivo l'autodistruzione del contenuto del messaggio, che comunque interviene dopo un certo lasso di tempo (per esempio dopo sette giorni dall'ultima accensione o impiego) ovvero in occasione del riavvio del sistema in alcune configurazioni o ancora dopo un certo lasso di tempo di disconnessione dalla rete telefonica o telematica;

- l'impiego di "*fake up*" per simulare l'uso di un apparato ordinario e trarre in inganno l'operatore di polizia in caso di eventuale controllo del dispositivo;

- la possibilità di rilevare la presenza di *IMSI Catcher*[5] e di non ricevere i cosiddetti

---

[3] La crittografia, come è noto, è la tecnica che permette, con l'aiuto di un algoritmo matematico, di trasformare un messaggio leggibile da tutti, in una forma illeggibile per quegli utenti che non possiedano una chiave segreta di decifrazione. La funzione è reciproca, per cui l'applicazione dello stesso algoritmo e della chiave segreta al testo cifrato restituisce il testo originale.

[4] L'espressione inglese *peer-to-peer* (abbreviata anche come P2P), cioè rete paritaria/paritetica, nelle telecomunicazioni indica un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi ('clienti' e 'serventi'), ma anche sotto forma di nodi equivalenti o 'paritari' (peer), potendo fungere al contempo da client e server verso gli altri nodi terminali (*host*) della rete. Nel caso di specie, sembra sia stato realizzato un servizio non riconducibile a un P2P puro, ma ad un P2P con *Discovery Server* o con *Lookup Server*, cioè un sistema di comunicazioni che presuppone una interlocuzione con un server centrale prima del contatto tra due nodi.

[5] Un *IMSI-catcher* (*International Mobile Subscriber Identity*) è un dispositivo che si finge una cella di una rete mobile. Quando un telefono cellulare cerca una rete nelle vicinanze, l'*IMSI-catcher* si presenta come la cella più attraente per il dispositivo, che si connetterà automaticamente a essa. Una volta stabilita la connessione, l'*IMSI-catcher* è in grado di intercettare le comunicazioni tra il dispositivo e la rete, incluse chiamate vocali, messaggi di testo e dati internet e finanche di interrompere il servizio, rivelandosi strumento molto utile soprattutto per le indagini relative a reati di terrorismo e di criminalità organizzata.

sms "silenti o occulti";

- la possibilità di inserire un cd. *panic code*, che consente di azzerare l'intero contenuto del dispositivo;

- la possibilità di prevedere l'impiego di codici di sblocco sia del sistema operativo di sia di ogni singola applicazione;

- la possibilità di impiegare schede straniere non intestate a soggetti giuridici.

La considerazione di tutte queste caratteristiche ha condotto nelle ordinanze impugnate i Tribunali a ritenere che i criptofonini "*risultano … particolarmente versatili per le esigenze operative ed elusive delle organizzazioni criminali*", giungendo alla conclusione che "*si tratta di apparecchi non intercettabili, progettati per le attività criminali e normalmente utilizzati - tenuto conto anche degli esorbitanti costi e della necessità di conoscere i nickname delle persone con cui si vuole conversare - da strutturate organizzazioni criminali*" (cfr. 4 – 5 dell'ordinanza del Tribunale di Reggio Calabria).

Complesse indagini della polizia francese, in collaborazione con quella olandese e belga e con il coordinamento di Europol[6], hanno svelato progressivamente l'architettura informatica del sistema di comunicazione impiantato dalla società canadese *Sky Global*, facendo emergere l'utilizzo, per assicurare la massima riservatezza degli utenti, di ben quattro chiavi di cifratura, due presenti nel server e due nel singolo cellullare dell'utilizzatore[7].

Appare utile osservare immediatamente che **le comunicazioni che avvengono con un sistema criptato così congegnato possono essere intercettate in modo utile, cioè in un modo che permetta di raccogliere dati comprensibili, solo conoscendo (e, dunque, attuando quanto necessario per conoscere) le chiavi di cifratura, le quali** – va rimarcato - **sono presenti, sia negli apparecchi mobili, sia nel *server***.

L'alternativa ipotizzabile è solo quella di rinunciare al mezzo di ricerca della prova: vale a dire, di non procedere ad intercettazione dei "criptofonini", attuale strumento di elezione per le comunicazioni aventi ad oggetto il traffico internazionale di stupefacenti e

---

[6] Dalla lettura degli atti della polizia giudiziaria, dei pubblici ministeri e dei giudici istruttori francesi emerge con estrema chiarezza che, in una realtà in cui il crimine ha assunto una dimensione transnazionale, operazioni di polizia di un certo rilievo sono possibili solo con la collaborazione tra le autorità preposte nei diversi Stati membri, permettendo di cogliere il senso più profondo della cooperazione giudiziaria nell'Unione.

[7] Nella "*Commissione di rogatoria*" del giudice istruttore francese dell'8 gennaio 2021 (in ALL. n. 1) sono illustrate le quattro chiavi:

"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 chiave segreta memorizzata sul server (e dunque impedendo ai gestori del server di decodificarla.)

2- secret key. Questa chiave è trasmessa al server e cancellata dalla memoria del telefono, 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 memorizzata 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)".

l'attività di terrorismo internazionale.

2. - I mezzi di ricerca della prova eseguiti in Francia.

Nel caso in esame, le attività d'indagine, più specificamente, sono state effettuate in Francia con riferimento ad ipotesi di reato relative alla fattispecie di **associazione per delinquere finalizzata al traffico di stupefacenti**, condotte punibili con 10 anni di reclusione, e alla violazione della legge sui mezzi di crittografia e sono state autorizzate dal giudice istruttore secondo il codice di rito francese.

Il giudice istruttore di Lille, in sintesi, in data 14 giugno 2019, ha adottato la prima "*autorizzazione all'intercettazione di corrispondenza per via elettronica*", autorizzando la collocazione di un dispositivo[8] per "*l'intercettazione, la registrazione e la trascrizione delle comunicazioni effettuate mediante comunicazioni elettroniche*" tra due server e delle "*comunicazioni elettroniche in entrata e in uscita dal server principale*"[9]. In questo modo, è stato captato il flusso telematico in transito tra due server di una società di *hosting* denominata OVH[10], uno dei quali di *backup*. I server erano stati noleggiati dalla società *Sky Global,* siti a Roubaix. A questo primo provvedimento hanno fatto seguito altre autorizzazioni e decreti di proroga (cfr. gli atti contenuti nell'ALL. n. 1).

In particolare, dall'informativa sull'andamento delle indagini del "Brigadiere di polizia" al pubblico ministero del 18 luglio 2019, emerge che "*un'analisi preliminare del flusso di rete ha rivelato elementi promettenti: parte del traffico di rete non è stato crittografato; alcune informazioni sono passate in chiaro; un'analisi sintetica dei primi pacchetti di rete intercettati ha consentito di risalire ai clienti delle email di conferma dell'attivazione dell'account SKY ECC compreso il numero IMEI, il numero*

---

[8] Nel provvedimento con cui la polizia francese ha dato esecuzione all'autorizzazione del giudice istruttore, per mezzo del contributo di una società provata che si occupa di servizi informatici, è stato disposto di "*impostare una sonda per l'intercettazione e la registrazione dei flussi di dati in un Datacenter dell'azienda OVH … per procedere all'intercettazione del flusso di rete in entrata e in uscita tra i 2 server …. permettendo a questi due server di comunicare i cui indirizzi IP sono: - 5.135.135.94 (back-end) - 188.165.14.8 (server di backup) così come una sonda sul server principale verso l'esterno al fine di analizzare il traffico di rete in entrata e in uscita. Il traffico in entrata e in uscita da questi server verrà reindirizzato alla sonda dal OVH che era richiesto per questo scopo. … Al termine delle intercettazioni, sarà inoltre necessario fornirci su hard disk tutte le registrazioni*".

[9] L'informativa della polizia giudiziaria francese posta a fondamento della prima autorizzazione, pur nella sintesi tipica di questi atti d'indagine, dà contezza della genesi dell'inchiesta, riferendo che "*Nel 2016 è stata aperta un'indagine nei Paesi Bassi e in Belgio riguardante la società canadese SKY ECC. … 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 SKY ECC 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 SKY ECC. Più di 350 numeri SKY ECC sono stati coinvolti solo per l'area di Anversa. Questa cifra è salita a 1000 numeri relativi ad attività criminali in tutto il paese belga.* ***Le autorità belghe hanno anche specificato che SKY ECC non ha collaborato con le forze di sicurezza, dopo aver ottenuto un mandato dal giudice***".

[10] OVH SAS è una grande società di *hosting* con diversi *data center* in tutto il mondo, che offre servizi a grandi e piccoli clienti.

seriale del telefono attivato, l'identificativo SK YECC, ecc.). ***Per vedere i messaggi degli utenti e i loro metadati passa in forma crittografata*** *…*".

Le indagini svolte in Francia, comunque, hanno permesso di svelare gradualmente il meccanismo di funzionamento dell'infrastruttura utilizzata per le comunicazioni – "*l'architettura tecnica dei server che consente e il funzionamento di tale applicazione consentendo a molti trafficanti di droga … di garantire la riservatezza dei loro scambi cospirativi*" (così, il pubblico ministero di Lille in una richiesta di proroga di autorizzazione di intercettazione di corrispondenza del 22 luglio 2019, contenuta in ALL. n. 1) – man mano che gli investigatori penetravano in essa, appurando i complessi sistemi di crittografia adoperati negli scambi di flussi dati tra i criptofonini e i *server* utilizzati dalla società.

Nel prosieguo dell'attività investigativa, nel dicembre del 2020, è stato emesso un ulteriore provvedimento di autorizzazione, questa volta dal giudice istruttore di Parigi, con cui è stato impiantato un programma informatico ("*un dispositif de captation de données sur le lien externe du serveur*"), che, ancorché inserito sul *server,* è servito per cogliere la chiave di cifratura presente in ciascun apparecchio telefonico. **Trattasi di provvedimento emesso dall'autorità giudiziaria francese, con ampia e specifica motivazione e secondo *standard* addirittura superiori a quelli previsti nell'ordinamento nazionale italiano: infatti, nella motivazione – ben oltre i requisiti minimi di cui all'art. 267 c.p.p. – è argomentata l'indispensabilità del mezzo** (cfr. ALL. n. 5)[11]. A questo provvedimento, nel febbraio 2021, ha fatto seguito un altro provvedimento, sempre del giudice istruttore di Parigi, per l'installazione di un secondo *"dispositif de captation de données"* (cfr. ALL. n. 6).

A questo punto, acquisite grazie alle intercettazioni le chiavi di cifratura che erano conservate nei *server* e recuperati a mezzo di *trojan* gli algoritmi di decodifica che erano riposti nei criptofonini, la polizia giudiziaria francese ha potuto decodificare i messaggi già registrati e apprendere il significato di quelli che intervenivano successivamente (cfr. atti in ALL. 1).

In seguito, il 9 marzo 2021, la polizia giudiziaria ha eseguito una operazione su base internazionale, così rendendo pubblica l'avvenuta violazione del sistema criptato, con l'accesso ai "*flussi di informazione di oltre 70.000 utenti*" (cfr. pag. 33 dell'ordinanza del Tribunale del riesame di Potenza).

In questa data è stato eseguito il sequestro dei server della società *OVH*, su cui il *provider* del servizio *Sky ECC* conservava copia della cronologia delle conversazioni

[11] Nel provvedimento del giudice istruttore si legge: "*le déchiffrement des messages individuels ne peut être réalisé à partir des seules données interceptées dans la mesure où seule la partie des éléments cryptographiques acheminée par les téléphones sur les serveurs est susceptible d'être récupérée au travers des données interceptées ; l'autre partie des éléments cryptographies étant uniquement stockée sur les téléphones* ".

intrattenute. Di tali server è stata fatta copia forense ed il loro contenuto è stato decrittato, così creando un archivio di conversazioni "in chiaro" (ALL. 2). Eurojust ha stilato una tavola riepilogativa delle decisioni riguardanti i server OVH (ALL. 4).

I Procuratori della Repubblica italiani, successivamente, con la emissione di una pluralità di OEI indirizzati all'Autorità giudiziaria francese, hanno richiesto la consegna dei messaggi scambiati, **in specifici periodi da specifici utenti,** con *Sky ECC*. I messaggi, consegnati già decriptati, sono stati ritenuti utili per dimostrare la perpetrazione di gravi reati riconducibili agli artt. 73 e 74 del d.P.R. n. 309 del 1990 (ALL 3).

3. – Il contrasto tra orientamenti giurisprudenziali.

In merito all'utilizzabilità come prova delle *chat* ottenute dal pubblico ministero nella forma già decriptata mediante OEI rivolto all'autorità giudiziaria francese, come è stato illustrato, è insorto un contrasto giurisprudenziale.

L'indirizzo prevalente nella giurisprudenza di legittimità ha ritenuto utilizzabili nel procedimento penale detti messaggi, pur dividendosi in merito all'individuazione della disciplina applicabile quale parametro di riferimento per sostenere tale giudizio.

Un diverso indirizzo giurisprudenziale, invece, con specifico riferimento al tema del rispetto del "principio di equivalenza" di cui all'art. 6, § 1, escluso il ricorso alla previsione di cui all'art. 234-*bis* cod. proc. pen., ha annullato con rinvio l'ordinanza cautelare fondata su dette prove, chiedendo al giudice del rinvio di chiarire quale sia stata la natura dell'attività svolta all'estero e di attribuire alla stessa la corretta qualificazione giuridica da ricondursi al sequestro di cui all'art. 254-*bis* cod. proc. pen. oppure alle intercettazioni previste dall'art. 266 cod. proc. pen. (Sez. 6, n. 44154 del 26/10/2023 Rv. 285284 01; Sez. 6, n. 44155 del 26/10/2023 Rv. 285284 –01).

Il contrasto interpretativo si è manifestato sia in ordine alla individuazione dello strumento processuale "interno" da porre a parametro per l'importazione delle chat decriptate e richieste con OEI, sia con riguardo all'ambito del controllo giurisdizionale da svolgere nel nostro ordinamento sull'utilizzabilità dei dati probatori raccolti all'estero.

Come già detto *supra*, la Terza Sezione della Corte di cassazione ha deciso di rimettere il ricorso alle Sezioni Unite (Sez. 3, ord. n. 47798/23 del 3/11/2023, dep. il 30/11/2023).

Nelle more della redazione dell'ordinanza di rimessione, inoltre, sono state depositate ulteriori sentenze della Corte di cassazione che hanno affrontato il tema, concludendo per l'utilizzabilità nel procedimento penale della corrispondenza, anche informatica, già decriptata all'estero, acquisita con OEI, individuando in altre disposizioni del codice di rito

il parametro normativo di riferimento (Sez. 6 n. 46482 del 27/09/2023; Sez. 6 n. 46833 del 26/10/2023).

Si è già evidenziato, nella parte prima, che una ulteriore ordinanza di rimessione, infine, è stata adottata dalla Sesta Sezione della Corte di cassazione, con la quale sono stati evidenziate ulteriori profili critici (Sez. 6, n. 2329 del 15/1/2024, dep. il 18/1/2024).

Le osservazioni di questo Ufficio affrontano congiuntamente le questioni poste da entrambe le ordinanze di rimessione.

4. - Il ricorso all'OEI per ottenere "prove esistenti" nello Stato di esecuzione.

La complessità delle questioni suggerisce l'opportunità di seguire **l'intero percorso procedimentale che ha condotto all'acquisizione della prova costituita dalla messaggistica criptata**.

È pacifico che, agli atti del procedimento penale, vi siano le trascrizioni di conversazioni in chat avvenute sulla piattaforma criptata *Sky ECC,* acquisite a seguito di autorizzazione del giudice istruttore francese per fini di giustizia interni.

Una parte di esse, concernenti determinati soggetti, sono state trasmesse al pubblico ministero presso il Tribunale di Potenza nel luglio del 2021 in esecuzione di OEI emesso da questi emesso e sono oggetto del procedimento n. 33544/2023 R.G. (ALL. 3).

Nello stesso ricorso, sul punto, si assume come circostanza certa che "*il dato sia stato fornito* [al pubblico ministero di Potenza] *dal Tribunale di Parigi*".

Analogamente, il pubblico ministero presso il Tribunale di Reggio Calabria ha acquisito, con ordine europeo d'indagine, le chat raccolte dall'autorità francese relative a specifici soggetti indagati in un procedimento iscritto presso la Procura di Reggio Calabria.

L'art. 1, § 1, della direttiva 2014/41/UE stabilisce che un ordine europeo di indagine possa essere emesso non solo per compiere uno o più atti di indagine in un altro Stato membro, ma anche "*per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione*".

L'art. 10, § 2, lett. a), della direttiva, inoltre, disciplina l'ordine che ha ad oggetto "*l'acquisizione di informazioni o prove che sono già in possesso dell'autorità di esecuzione*" (cfr. anche il considerando n. 7 che si riferisce "*all'acquisizione di prove già in possesso dell'autorità di esecuzione*").

Adoperando una terminologia invalsa nella prassi, deve rilevarsi che un OEI può essere emesso, sia per raccogliere "prove nuove", sia per trasferire "prove esistenti" nello Stato di esecuzione.

Nella specie, ricorre, pacificamente, il secondo caso, non risultando dubbio alcuno che l'ordine europeo di indagine si riferisse ad elementi di prova già completamente formati nello Stato di esecuzione al momento in cui gli ordini in questione venivano emessi.

5. - L'ammissione della prova indicata nell'OEI

5.1. Il procedimento probatorio, anche nel caso di ricorso all'OEI, si snoda in tre momenti essenziali: L'**ammissione** degli atti istruttori indicati nell'OEI; la **raccolta** della prova; l'**utilizzazione** della stessa.

Il vaglio di ammissibilità della prova, nell'impalcatura della direttiva 2014/41/UE, è devoluto all'autorità dello Stato di emissione ed è svolto secondo le previsioni di cui all'art. 6 della stessa direttiva, che consistono nella valutazione della "*necessità*" e della "*proporzionalità*" della prova (art. 6, § 1, della direttiva) e della possibilità di disporre l'atto istruttorio "*alle stesse condizioni in un caso interno analogo*" (art. 6, § 2, della direttiva).

I presupposti di ammissibilità della prova possono essere posti in discussione contestando, nello Stato di emissione, il provvedimento di ammissione tramite una impugnazione (CGUE, 11/11/2021, Gavanozov, C-852/19). L'art. 14, § 2, della direttiva, infatti, stabilisce che "*le ragioni di merito dell'emissione dell'OEI possono essere impugnate soltanto mediante un'azione introdotta nello Stato di emissione*".

La fattispecie non sembra diversa da quella che riguarda, per esempio, l'impugnazione del sequestro probatorio disposto all'estero tramite rogatoria (cfr. Sez. U, n. 21420 del 16/04/2003, Rv. 224184 - 01).

L'art. 28 del d.lgs. n. 108 del 2017, Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale, disciplina l'impugnazione dell'ordine di indagine avente ad oggetto il sequestro a fini di prova.

5.2. Tra le questioni sull'ammissione della prova, in particolare, va ricompresa quella relativa all'individuazione dell'autorità di emissione dell'OEI. Nel caso concreto, **se l'autorità di emissione possa essere individuata anche nel pubblico ministero**.

Su tale punto, deve segnalarsi che, secondo un orientamento giurisprudenziale, la questione della illegittima emissione dell'OEI da parte del pubblico ministero italiano non può essere dedotta dinanzi al giudice italiano nel caso in cui tale ordine sia stato emesso per acquisire una prova già disponibile nello Stato di esecuzione e la stessa sia stata definitivamente trasmessa da detto Stato (Sez. 6, n. 44155 del 26/10/2023, Kolgjokaj Indrit,

Rv. 285362 - 02). "*Tale profilo risulta definitivamente assorbito dalla trasmissione della prova ad opera di quest'ultimo (verificandosi un caso analogo a quello in cui la prova è stata spontaneamente messa a disposizione di un altro Stato, secondo un meccanismo oramai consolidato nella normativa internazionale nelle prassi delle relazioni tra Stati)*" (così, Sez. 6, n. 44154 del 26/10/2023, Iaria, cit.).

Come si vedrà, tale questione - anche se la si ritenesse proponibile dopo la fase dell'ammissione, quale causa di inutilizzabilità della prova - è da reputarsi, a parere di questo Ufficio, comunque infondata.

5.3. Il vaglio di ammissibilità della prova, invero, non è ad appannaggio esclusivo dello Stato di emissione. Tra i profili che la difesa potrebbe far valere presso lo Stato di esecuzione, per esempio, si pone quello della competenza dell'autorità di emissione ad adottare lo specifico atto richiesto (CGUE 16/12/2021, HP, C-724/19).

L'autorità di esecuzione, inoltre, ha la possibilità di adottare un atto istruttorio alternativo rispetto a quello indicato dall'autorità di emissione e capace di produrre il medesimo risultato.

Nel caso di specie, tuttavia, tali profili non hanno alcun rilievo, sia perché simili questioni non sono state proposte nello Stato francese di esecuzione, sia perché, trattandosi di acquisizione di una prova esistente, l'atto istruttorio era già stato ammesso in tale Stato quando è stato inviato l'OEI dall'autorità di emissione.

5.4. Le condizioni di ammissione dell'OEI previste dall'art. 6 della direttiva, peraltro, **incidono sul regime di utilizzabilità della prova raccolta** con tale strumento. La loro mancanza, pertanto, può essere successivamente dedotta nello Stato di emissione ai fini della utilizzabilità della prova pervenuta dallo Stato di esecuzione.

Lo Stato di emissione, infatti, come ha chiarito la Corte di giustizia, indipendentemente dai rimedi esperibili presso lo Stato di esecuzione, deve consentire alla difesa di contestare "*la necessità e la regolarità di un ordine europeo di indagine*", assicurando il diritto a un ricorso effettivo (CGUE sent. 11/11/2021, Gavanozov, C-852/19).

Nel caso di emissione di un ordine d'indagine per acquisire una prova già disponibile nello Stato di esecuzione, ad avviso di questo Ufficio (ed in conformità alla condivisibile giurisprudenza di codesta Suprema Corte sul punto), anche se la stessa sia stata definitivamente trasmessa da detto Stato, la difesa può far valere **la mancanza delle condizioni di ammissibilità della prova** secondo l'ordinamento processuale italiano (Sez.

6, n. 44154 del 26/10/2023, Iaria, cit.; Sez. 6, n. 44155 del 26/10/2023, Kolgjokaj Indrit, cit.).

6. - L'assunzione della prova nello Stato di esecuzione secondo la *lex loci*.

6.1. L'art. 9, § 1, della direttiva citata sancisce che l'autorità d'esecuzione debba assumere la fonte di prova richiesta dall'autorità d'emissione nella osservanza della propria disciplina processuale. Secondo detta norma, difatti, l'autorità di esecuzione "*assicura l'esecuzione* [dell'ordine] *nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione*".

Nel sistema delineato dalla direttiva 2014/41/UE:

- la prova è formata nello Stato di esecuzione, secondo le previsioni della *lex loci*;

- eventuali censure relative alla concreta assunzione di tali mezzi di ricerca della prova non possono essere proposte all'autorità giudiziaria di emissione dell'ordine europeo di esecuzione, ma esclusivamente allo Stato di esecuzione;

- l'autorità di emissione non può sindacare la legittimità delle misure mediante le quali lo Stato di esecuzione ha raccolto le prove, in quanto spetta ai giudici dello Stato di esecuzione conoscere dei ricorsi giurisdizionali avverso tali atti.

Queste regole costituiscono **diretto portato del principio del riconoscimento reciproco che implica la fiducia reciproca** e la presunzione di conformità degli atti con cui è stata raccolta la prova al diritto dell'Unione e ai diritti fondamentali.

Tra Stati membri dell'Unione non sussistono regole uguali per l'assunzione della prova; **si presume**, invece, **un analogo livello di protezione dei diritti individuali**.

6.2. La fase della raccolta della prova, più precisamente, è solo tendenzialmente di competenza dello Stato di esecuzione.

L'autorità di esecuzione, infatti, secondo l'art. 9, § 2, della direttiva, "*si attiene alle formalità e alle procedure espressamente indicate dall'autorità di emissione, salvo qualora la presente direttiva disponga altrimenti, sempre che tali formalità e procedure non siano in conflitto con i principi fondamentali del diritto dello Stato di esecuzione*".

Il d.lgs. n.108 del 2017 di attuazione dell'ordine europeo d'indagine, all'art. 33, quanto al nostro ordinamento, precisa che "*l'autorità giudiziaria che ha emesso l'ordine di indagine concorda con l'autorità di esecuzione le modalità di compimento dell'atto di indagine o di prova, specificamente indicando i diritti e le facoltà riconosciuti dalla legge alle parti e ai loro difensori*".

Nel caso in cui lo Stato di emissione non indica alcuna "*formalità*" o "*procedura*", pertanto, lascia spazio alla piena operatività alla *lex loci*.

Nel caso di specie, **lo Stato italiano, emettendo l'ordine di indagine, non ha dato indicazioni in merito alle formalità e alla procedura da seguire per l'acquisizione della prova**; più semplicemente, ha indicato una determinata utenza, relativa a soggetto già raggiunto da sufficienti indizi, e, nel rispetto del principio di proporzionalità, ha chiesto l'acquisizione di specifiche conversazioni che ruotavano intorno a tale utenza, in un certo arco temporale, ipotizzando la commissione di gravi reati.

6.3. Le regole illustrate, comunque, non sembrano diverse da quelle che disciplinano le rogatorie.

Secondo l'indirizzo giurisprudenziale consolidato, in tema di rogatorie verso l'estero, l'autorità rogante, che nella domanda di assistenza giudiziaria non abbia indicato specifiche formalità per il compimento dell'atto istruttorio richiesto, non può compiere alcun vaglio circa la legittimità delle modalità di acquisizione esperite dall'autorità straniera, tanto più ove l'atto di indagine sia stato compiuto in precedenza, nel corso di investigazioni da quest'ultima autonomamente avviate, in quanto vige la **presunzione di legittimità dell'attività svolta in forza del principio di reciproca fiducia**, fermo restando che l'atto, una volta introdotto nel procedimento penale italiano, soggiace a tutte le regole sostanziali e processuali quanto alla sua valutazione e alla possibilità, da parte dell'imputato, di esercitare le prerogative difensive (Sez. 3, n. 1396 del 12/10/2021, dep. 2022, Rv. 282886 - 01).

Tali regole operano a maggior ragione nel caso in cui la cooperazione internazionale sia realizzata mediante l'ordine europeo d'indagine.

6.4. Quando emette un OEI diretto al trasferimento di prove esistenti, **l'autorità di emissione è vincolata al principio del mutuo riconoscimento, che costituisce la "pietra angolare" su cui si fonda la cooperazione in materia penale nell'Unione europea**: **l'autorità di emissione che chiede una "prova esistente" in un altro Stato membro non può sindacare la legittimità dell'atto formato in un procedimento giudiziario nello Stato di esecuzione**. Può dare indicazioni in merito a "*formalità*" o a "*procedure*" alle quali l'autorità di esecuzione deve attenersi, salvo che queste ultime non siano in conflitto con i "principi fondamentali" del diritto dello Stato di esecuzione. Se non fornisce espressamente dette indicazioni, lo Stato di emissione lascia campo libero alla *lex loci*.

6.5. Quanto appena illustrato, ad avviso di questo Ufficio, non significa che, all'autorità giudiziaria di emissione, non spetti, nella fase di utilizzazione della prova, verificare:

- se l'ordine europeo di indagine sia stato legittimamente emesso secondo le previsioni della direttiva 2014/41/UE e della disciplina interna di recepimento (nel caso italiano, il d.lgs. 21 giugno 2017, n. 108);

- se le prove acquisite mediante la cooperazione internazionale siano utilizzabili nel procedimento penale interno, in quanto sussistano, come meglio si vedrà nel prosieguo, le "*condizioni di emissione*" fissate dall'art. 6 della direttiva citata e concernenti **l'osservanza dei principi di equivalenza** rispetto ad un caso analogo interno e **di proporzionalità e necessità** dell'ingerenza sui diritti fondamentali, da valutarsi, come meglio si dirà, nella prospettiva del procedimento penale nazionale.

Ribadendo quanto già affermato, **lo Stato di emissione, indipendentemente dai rimedi esperibili presso lo Stato di esecuzione, deve consentire alla difesa di contestare "la necessità e la regolarità di un ordine europeo di indagine"** (CGUE, sent. 11/11/2021, Gavanozov, C-852/19).

6.6. Calando queste regole nel caso di specie, deve concludersi che **il giudice italiano non possa e non debba compiere una valutazione di conformità dei provvedimenti e dei metodi di acquisizione delle prove acquisite dallo Stato di esecuzione (Francia)** e trasmesse mediante l'OEI rispetto alla disciplina estera di riferimento per tale tipologia di attività, poiché un vaglio di questo genere rappresenterebbe una violazione del principio del riconoscimento reciproco, che è sotteso alla cooperazione in materia penale nell'Unione europea (conf., in termini analoghi, Sez. 6, n. 48330 del 25/10/2022, Borrelli, Rv. 284027; Sez. 1, n. 6364 del 13/10/2022, Calderon, Rv. 283998).

A maggior ragione, in una fattispecie in cui lo Stato italiano non ha dato indicazioni su "formalità" e su "procedure" da seguire per l'assunzione della prova.

Neppure il giudice italiano potrebbe sindacare, secondo la propria disciplina nazionale, la legittimità dei provvedimenti adottati dall'autorità giudiziaria dello Stato di esecuzione per la raccolta della prova, pretendendo l'osservanza di una sorta di principio di reciprocità. Tra Stati membri dell'Unione - si ribadisce - non sussistono regole uguali per l'assunzione della prova: si presume invece un analogo livello di protezione dei diritti individuali.

Nel caso di specie, comunque, è pacifico tra le parti che l'intercettazione e l'acquisizione delle chat intervenute sulla piattaforma criptata *Sky ECC* sono state eseguite in conformità alla *lex loci*. Come si vedrà, vi è stato finanche un ricorso alla locale Corte costituzionale su un profilo molto delicato del procedimento probatorio (ALL. n. 7).

È altresì pacifico, inoltre, che il mezzo di ricerca della prova sia stata esperito in forza di autorizzazione e sotto il controllo del giudice istruttore francese, proprio come sarebbe avvenuto in Italia per l'autorizzazione alla esecuzione di intercettazioni (ove si ritenesse che quest'ultimo rappresenti il mezzo di ricerca della prova che sarebbe stato utilizzato in un caso interno analogo).

Può dunque concludersi sul punto che in Italia (Stato di emissione) sono stati trasmessi risultati di prove già esistenti e **validamente raccolte in Francia** (Stato di esecuzione).

7. - Il rispetto del principio di equivalenza (art. 6, par. 1, lett. b), della direttiva 2014/41/UE).

L'ultimo momento del procedimento probatorio è rappresentato dal **vaglio di utilizzabilità della prova** raccolta tramite OEI che va compiuto nel processo instaurato nello Stato di emissione. Tale Stato, infatti, indipendentemente dai rimedi esperibili presso lo Stato di esecuzione, deve consentire alla difesa di contestare "*la necessità e la regolarità di un ordine europeo di indagine*", come ha chiarito la CGUE (CGUE 11/11/2021, Gavanozov, § 54).

Ritiene questo Ufficio che si tratti del momento in cui l'ordinamento interno garantisce il diritto a un ricorso effettivo, sancito dall'art. 47, primo comma, della Carta dei diritti fondamentali dell'Unione europea. Tale diritto, che costituisce una riaffermazione del principio della tutela giurisdizionale effettiva, **è assicurato con la previsione di un adeguato sistema impugnatorio direttamente nei confronti dell'OEI suscettibile di impattare sui diritti fondamentali** (art. 28 d.lgs. n.108 del 2017) e con **l'impugnazione dei provvedimenti che si fondano su tali prove, di cui può essere contestata la regolarità ("legittimità") e la necessità** (come è effettivamente avvenuto nei casi in esame).

Il controllo giurisdizionale sull'emissione dell'OEI è dunque assicurato nel diritto interno, ancorché non in via preventiva.

La CGUE, d'altra parte, **non richiede necessariamente un controllo giurisdizionale *ex ante*** (cfr. CGUE 11/11/2021, Gavanozov).

I parametri concreti del controllo giurisdizionale sono stabiliti dalla direttiva 2014/41/UE. Essa non ha disciplinato l'utilizzabilità della prova acquisita con l'OEI, rinviando per tale aspetto al diritto dello Stato di emissione. L'art. 14, § 7, peraltro, ha previsto che "*gli Stati membri assicurano che nei procedimenti penali dello Stato di emissione siano rispettati i* ***diritti della difesa*** *e sia garantito un* ***giusto processo*** *nel valutare le prove acquisite tramite l'OEI*", facendo altresì salve "*le norme procedurali nazionali*".

Ai fini del controllo sulla utilizzabilità della prova, poi, rileva l'art. 6 della direttiva 2014/41/UE, che fissa le condizioni di emissione e di trasmissione dell'OEI, richiamando il **principio di proporzionalità e necessità** del mezzo di prova rispetto e quello **di equivalenza**. Quest'ultimo prescrive che "*l'autorità di emissione può emettere un ordine europeo di indagine solamente quando l'atto o gli atti di indagine richiesti nell'ordine europeo di indagine avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*". Questa condizione va valutata "*per ogni caso*" (art. 6, § 2, della direttiva 2014/41/UE) e, come si vedrà, permette l'applicazione delle eventuali cause di esclusione della prova.

In forza del principio di equivalenza, in particolare, l'autorità giudiziaria dello Stato di emissione non può demandare a quella dello Stato di esecuzione il compimento di un atto di indagine che non sia contemplato dalla *lex fori*, né tantomeno richiedere la trasmissione di prove che non avrebbero potuto formare di acquisizione in un procedimento penale interno.

L'autorità giudiziaria dello Stato di emissione, analogamente, non può utilizzare prove che, ancorché trasmesse dallo Stato di esecuzione, non siano contemplate dalla *lex fori*.

La disposizione della direttiva mira ad evitare che le prove raccolte dall'autorità giudiziaria dello Stato di esecuzione, in conformità al proprio ordinamento, possano servire per **eludere i divieti** di acquisizione probatoria stabiliti dalla legge processuale dello Stato di emissione, divenendo utilizzabili ai fini decisori (in violazione delle clausole di esclusione probatoria stabilite dalla *lex fori*).

Appare opportuno, pertanto, partire dal principio di equivalenza, per verificare se sia stato rispettato nel caso di specie e, segnatamente, se messaggi di chat come quelli acquisiti con provvedimento del giudice istruttore francese possano essere utilizzati come prova in un procedimento penale italiano (in un "*caso interno analogo*").

8. - *segue*: La non condivisibilità dell'indirizzo che richiama l'art. 234-*bis* cod. proc. pen.

Ritiene questo Ufficio che non sia condivisibile l'indirizzo giurisprudenziale prevalente che richiama la previsione di cui all'art. 234-*bis* cod. proc. pen. quale istituto che,

in un caso analogo interno, permetterebbe l'acquisizione delle chat (tra le tante, Sez. 3, n. 47201 del 19/10/2023, Rv. 285350 – 01; Sez. 4, n. 37503 del 30/05/2023; Sez. 4, n. 38002 del 16/05/2023; Sez. 4, n. 16345 del 05/04/2023, Liguori ed altri; Sez. 4, n. 16347 del 05/04/2023, Rv. 284563 - 01; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Rv. 283998 - 01).

La norma citata, introdotta dal legislatore in riferimento al contrasto del terrorismo di matrice internazionale, consente "*sempre*" l'acquisizione dei documenti e dei dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, "*del legittimo titolare*", **senza ricorrere alla disciplina rogatoriale** (Sez. 6, n. 18907 del 20/04/2021, Civale, Rv. 281819 - 01, non massimata sul punto; Sez. 3, n. 36381 del 09/05/2019, Zinghinì, non massimata sul punto, entrambe relative all'ammissibilità dell'acquisizione della messaggistica, scambiata mediante sistema *BlackBerry* senza ricorso alle forme della rogatoria internazionale sulla base della collaborazione, spontaneamente prestata, del produttore del sistema operativo avente sede all'estero).

Nel caso di specie, l'acquisizione non ha riguardato direttamente dati digitali disponibili in rete o presenti presso un *server*, ma dati già previamente acquisiti dall'autorità giudiziaria francese per fini di giustizia interni.

A sua volta, l'autorità giudiziaria francese non ha acquisito tali dati con il consenso della società fornitrice del servizio di comunicazione elettronica, ma direttamente, per mezzo di mezzi di ricerca della prova come intercettazioni e sequestri.

L'acquisizione di tali chat, pertanto, non è avvenuta in deroga alla disciplina rogatoriale, ma in attuazione della disciplina dell'ordine europeo di indagine e, quindi, all'esito di una procedura di collaborazione internazionale.

È stato efficacemente rilevato che **la disciplina dell'ordine europeo di indagine e quella enunciata dall'art. 234-*bis* cod. proc. pen. non sono complementari, ma alternative** (Sez. 6, n. 48838 del 11/10/2023, Brunello).

Non essendo l'acquisizione delle chat di cui si controverte regolata dall'art. 234-*bis* cod. proc. pen., nessun rilievo può acquisire, pertanto, il difetto del consenso del titolare dei dati, eccepito anche nella specie dal ricorrente; parimente, non è necessario chiarire se il "*legittimo titolare*" delle stesse sia, nel caso di specie, il gestore della piattaforma criptata (*hosting service provider*), il titolare del criptofonino (*cloud consumer*) o l'autorità giudiziaria che ha proceduto alla loro acquisizione.

Per mera completezza, si osserva che, ai fini dell'acquisizione diretta di documenti e dati informatici diversi da quelli disponibili al pubblico, l'art. 234-*bis* cod. proc. pen. fissa il presupposto del consenso del "*legittimo titolare*" del dato, mentre, ad esempio, l'art. 254-*bis* cod. proc. pen. consente il sequestro – dunque, un mezzo ricerca della prova esperito senza il consenso dell'interessato - presso i fornitori di servizi dei dati informatici "*da questi detenuti*". Le due discipline, pertanto, diverse già quanto al presupposto del consenso che è necessario solo per una, fanno riferimento significativamente a due parametri normativi diversi: la "titolarità" dei documenti; la "detenzione" di dati su cui si esercita un potere di fatto, anche se la titolarità degli stessi appartiene ad altri.

9. - *segue*: La qualificazione delle *chat* come corrispondenza.

Il riferimento all'art. 234-*bis* cod. proc. pen. non pare pertinente anche perché deve ormai ritenersi che le chat di messaggistica costituiscano forme di corrispondenza e non già meramente "*documenti e dati informatici*".

La Corte costituzionale, con la sentenza n. 170 del 7 giugno 2023, ha infatti affermato che il concetto di "corrispondenza" ricomprende "*ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza*". La tutela accordata dall'art. 15 Cost. - che assicura a tutti i consociati la libertà e la segretezza "*della corrispondenza e di ogni altra forma di comunicazione*", consentendone la limitazione "*soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*" – "*si estende, quindi, ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti al momento del varo della Carta costituzionale*" (così, sent. n. 170 del 2023, par. 4.2. del *Considerato in diritto*).

La Corte, pertanto, ha ritenuto che lo scambio di messaggi elettronici - e-mail, SMS, *WhatsApp* e *similia* - rappresenta una forma di corrispondenza che ricade nella previsione dell'art. 15 Cost.

Mantengono la natura di corrispondenza, inoltre, anche i messaggi elettronici già ricevuti e letti dal destinatario, ma conservati nella memoria dei dispositivi elettronici del destinatario stesso o del mittente.

La Corte costituzionale ha optato per l'interpretazione secondo cui la tutela della corrispondenza di cui all'art. 15 Cost., iniziata nel momento in cui l'espressione del pensiero è affidata ad un mezzo idoneo a trasmetterlo, non si esaurisce con la ricezione del messaggio, né con la sua lettura. Si tratta, in verità, di una soluzione che pare obbligata perché "*Degradare la comunicazione a mero documento quando non più in itinere è soluzione che, se confina in ambiti angusti*

la tutela costituzionale prefigurata dall'art. 15 Cost. nei casi, sempre più ridotti, di corrispondenza cartacea, finisce addirittura per azzerarla, di fatto, rispetto alle comunicazioni operate tramite posta elettronica e altri servizi di messaggistica istantanea, in cui all'invio segue immediatamente - o, comunque sia, senza uno iato temporale apprezzabile - la ricezione" (così Corte cost. sentenza n. 170 del 2023, par. 4.4. del *Considerato*).

Il messaggio elettronico, dunque, costituisce corrispondenza anche dopo la ricezione da parte del destinatario "*fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse e alla sua riservatezza, trasformandosi in un mero documento storico*" (così ancora Corte cost. sentenza n. 170 del 2023, par. 4.4. del *Considerato*).

Anzi, il carattere di corrispondenza deve "*presumersi sino a prova contraria quando si discuta di messaggi scambiati … a una distanza di tempo non particolarmente significativa rispetto al momento in cui dovrebbero essere acquisiti …*" (così sempre Corte cost. sentenza n. 170 del 2023, *ivi*)[12].

Dalle statuizioni della Corte costituzionale deriva che le *chat* acquisite dall'autorità giudiziaria francese debbano essere qualificate come corrispondenza.

Le conclusioni della Corte, tuttavia, **non implicano che, per l'acquisizione della messaggistica, il pubblico ministero italiano debba sempre fare ricorso alla disciplina delle intercettazioni**. L'acquisizione di tali dati, infatti, non può essere assoggettata alla disciplina delle intercettazioni, anche di quelle informatiche o telematiche ex art. 266-*bis* cod. proc. pen., se manca la contestualità tra la trasmissione della comunicazione e l'atto acquisitivo (come rilevato, *ex plurimis*, da Sez. 4, n. 16347 del 05/04/2023, Papalia, Rv. 284563 - 01).

La stessa Corte costituzionale, infatti, nella sentenza illustrata, richiamando un principio giurisprudenziale consolidato (Sez. U, n. 36747 del 28/05/2003, Torcasio, Rv. 225465 - 01), ha ribadito che, affinché si abbia intercettazione, debbono ricorrere due condizioni: la comunicazione deve essere in corso nel momento della sua captazione da parte dell'*extraneus*, essendo colta nel suo momento "dinamico"; l'apprensione del messaggio comunicativo da parte del terzo deve avvenire in modo occulto, ossia all'insaputa dei soggetti tra i quali la comunicazione intercorre.

[12] La Corte costituzionale, invero, pur specificando che il carattere di corrispondenza si deve presumere, non precisa il lasso di tempo trascorso il quale il messaggio elettronico si trasforma in "*mero documento storico*" ("*i limiti temporali finali della tutela accordata dall'art. 15 Cost.*", volendo adoperare le espressioni della sentenza n. 170 del 2023). Esso dipende dalla sussistenza di un "*interesse alla riservatezza*" dal quale possa desumersi che il messaggio conservi, nella considerazione dei soggetti coinvolti, "*carattere di attualità*". Tale interesse sembrerebbe legato alla attualità delle vicende rappresentate e non al timore che il messaggio sia utilizzato come prova in un procedimento penale.

Entrambe le condizioni, pacificamente, non sussistono nel caso di specie in cui l'autorità giudiziaria italiana, con ordine europeo di indagine, ha ottenuto messaggi di chat già acquisiti dall'autorità giudiziaria straniera.

10. - *segue*: La qualificazione delle *chat* come "oggetto" di un provvedimento di sequestro.

10.1. L'operazione investigativa posta in essere dalle Autorità estere ha certamente avuto diversi momenti, consistiti nella iniziale captazione di flussi di dati in corso e nel sequestro finale dei server utilizzati dalla società *Sky Global* per fornire il servizio di comunicazione elettronica (cfr. ALL. 2).

Il percorso è stato articolato anche perché **l'architettura informatica realizzata dall'impresa *Sky Global* è stata progressivamente svelata dal progredire delle investigazioni**.

Nel corso dell'indagine, come si è visto, il giudice istruttore di Lille ha autorizzato "*l'intercettazione, la registrazione e la trascrizione delle comunicazioni effettuate mediante comunicazioni elettroniche*" tra due server ed in uscita da uno dei server (cfr. il provvedimento del giudice istruttore di Lille del 14 giugno 2019 ed i successivi provvedimenti proroga contenuti nell'ALL. 1), permettendo di apprendere le chiavi di decrittazione contenute nel *server*.

Nel prosieguo dell'attività investigativa, nel dicembre del 2020, è stato emesso un ulteriore provvedimento di autorizzazione, questa volta dal giudice istruttore di Parigi, con cui è stato impiantato un programma informatico del tipo *trojan* che, ancorché inserito sul *server,* è servito per cogliere la chiave di cifratura presente in ciascun apparecchio telefonico. A questo provvedimento, nel febbraio 2021, ha fatto seguito un altro provvedimento, sempre del giudice istruttore di Parigi, per l'installazione di un secondo *trojan*.

Solo a questo punto, acquisite grazie alle intercettazioni le chiavi di cifratura che erano conservate nei *server* e recuperati a mezzo di *trojan* gli algoritmi di decodifica che erano riposti nei criptofonini, la polizia giudiziaria francese ha potuto decodificare i messaggi già registrati e apprendere il significato di quelli che intervenivano successivamente (cfr. gli atti in ALL. 1).

Al termine dell'indagine, è seguito il sequestro dei tre server della società OVH, su cui il *provider* del servizio *Sky ECC* conservava copia della cronologia delle conversazioni intrattenute. Di tali *server* è stata fatta la copia forense (ALL. 2).

L'utilizzo del *trojan* per l'acquisizione delle chiavi di cifratura è avvenuto "*quale attività tecnica propedeutica al buon esito dell'attività di acquisizione delle comunicazioni … attività tecnica*

propedeutica allo svolgimento del fisiologico atto che le autorità giurisdizionali francesi si proponevano di effettuare, cioè appunto l'acquisizione delle chat tra gli utenti Sky ECC" (cfr. ordinanza del Tribunale di Reggio Calabria, pag. 16)

Il contenuto delle conversazioni acquisito è stato decrittato, così creando un archivio "in chiaro" in forza dei provvedimenti di intercettazione, come flusso in corso su due di tali server, comunque in precedenza non decrittabile in mancanza delle chiavi contenute sugli apparecchi mobili.

Dalla copia forense dei server della società OVH (e non da una copia ottenuta mediante registrazione "live") sono state estratte le conversazioni poi oggetto dell'OEI.

L'esecuzione dell'OEI italiano da parte dell'autorità francese, pertanto, è consistita esclusivamente nel fornire prove cristallizzate, frutto di sequestro, cioè, in gergo **dati cd. "freddi"**.

10.2. Seguendo questa prospettiva - e dunque ritenendo che, con OEI del 9 luglio 2021, il pubblico ministero italiano di Potenza (ma analogamente quello di Reggio Calabria nell'altro procedimento rimesso alle Sezioni unite) abbia acquisito corrispondenza elettronica non intercettata dall'autorità straniera nel momento in cui il flusso dati era *in itinere*, ma sequestrata in quanto rinvenuta nei *server* della società che fornisce i servizi di comunicazione elettronica o nei diversi dispositivi intercettati (dunque, "*dati freddi*") - deve concludersi per il pieno ed assoluto rispetto del principio di equivalenza di cui all'art. 6, § 1, lett. b), della direttiva più volte citata.

Il sequestro di corrispondenza, infatti, **costituisce un provvedimento che, in un "*caso interno analogo*", avrebbe potuto essere emesso alle stesse condizioni**.

In particolare, come è stato già evidenziato, la Corte costituzionale ha affermato che i messaggi scambiati tramite applicativi informatici o posta elettronica già ricevuti e letti dal destinatario, ma conservati nella memoria dei dispositivi elettronici del destinatario o del mittente mantengono la natura di corrispondenza (Corte cost., sentenza n. 170 del 2023).

La stessa Corte costituzionale, nella sentenza citata, con riguardo al mezzo con cui i messaggi già trasmessi possono essere acquisiti nel processo penale, ha fatto espresso riferimento al sequestro di telefoni cellulari, di computer o di altri dispositivi elettronici, indicati come "contenitori" di dati informatici.

Al riguardo, è stato rilevato che "*gli organi inquirenti debbono ritenersi abilitati a disporre … il sequestro del contenitore*"; tuttavia, "*nel caso di sequestro probatorio informatico il "vero" oggetto del sequestro non è tanto il dispositivo elettronico (il "contenitore") - il quale, di per sé, non ha di norma alcun*

interesse per le indagini - quanto piuttosto i suoi dati (il "contenuto"), nella parte in cui risultano utili alle indagini stesse …" (così, Corte cost., sentenza n. 170 del 2023, par. 5.1. del *Considerato*).

10.3. L'art. 253, comma 1, cod. proc. pen., invero, facendo riferimento alle "*cose pertinenti al reato necessarie per l'accertamento dei fatti",* non si riferisce esplicitamente alla corrispondenza.

La giurisprudenza di legittimità, tuttavia, ha precisato che la nozione a cui si riferisce la norma è più ampia di quella di corpo del reato, ricomprendendo, oltre al *corpus delicti*, tutte le cose, mobili o immobili, che servono, anche indirettamente, ad accertare la consumazione dell'illecito, il suo autore e le varie altre circostanze rilevanti ai fini di causa quali quelle inerenti alla modalità di preparazione ed esecuzione del reato ed ai suoi moventi (Sez. 5, del 21/10/1996, Rv. 206639).

Nel codice di rito, nondimeno, **alcune disposizioni si riferiscono specificamente al sequestro della corrispondenza**, anche quella che viene trasmessa **con mezzi telematici**.

L'art. 254 cod. proc. pen. disciplina espressamente il sequestro della corrispondenza. Questa norma, pur confermando che, in un "*caso analogo interno*", la corrispondenza può essere sequestrata, prevede l'adozione di un provvedimento che può riguardare anche la corrispondenza inoltrata "*per via telematica*", ma che deve essere eseguito "*presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazion*i", presupponendo, secondo l'interpretazione della giurisprudenza, un'attività di spedizione in corso (Sez. 3, n. 928 del 25/11/2015, dep. 2016, Rv. 265991 – 01; cfr. il punto 4.3. della sentenza Corte cost. n. 170 del 2023). Si tratta, pertanto, di una fattispecie, che non parrebbe pienamente sovrapponibile a quella oggetto del presente procedimento.

Non sembra, d'altra parte, che al sequestro della messaggistica "pregressa" si possa pervenire applicando la disciplina tipica del sequestro di dati informatici presso i fornitori di servizi informatici telematici e di telecomunicazione di cui all'art. 254-*bis* cod. proc. pen. che può riguardare i dati "*detenuti*" dal gestore.

I sistemi di messaggistica elettronica assicurano la riservatezza della comunicazione; mentre, nella corrispondenza epistolare, detta riservatezza è garantita dall'inserimento del plico cartaceo in una busta chiusa, nel caso dell'utilizzo della posta elettronica o di un sistema di messaggistica elettronica istantanea essa è garantita dal fatto che il messaggio o la e-mail viene inviata ad una specifica casella di posta, accessibile solo al destinatario tramite procedure che prevedono l'utilizzo di codici personali, mentre il messaggio, spedito tramite

tecniche che assicurano la riservatezza, è accessibile solo al soggetto che abbia la disponibilità del dispositivo elettronico di destinazione, normalmente protetto anche esso da codici di accesso o altri meccanismi di identificazione. Ne deriva che sembrerebbe debba essere considerato come detentore del messaggio elettronico soltanto colui che è titolare dei sistemi di identificazione (che, difatti, è l'unico che può cancellarlo quando vuole).

Qualificare i messaggi conservati nella memoria di un dispositivo elettronico, oggetto del decreto motivato di sequestro, come "*cose pertinenti al reato necessarie per l'accertamento dei fatti*" ovvero ricondurle alla corrispondenza sequestrabile con uno dei diversi mezzi di ricerca della prova disciplinati dal codice di rito che si riferiscono espressamente alla stessa, in ogni caso, **consente di ritenere rispettato il principio di equivalenza.**

Allo stesso tempo, il riferimento al sequestro finisce con il manifestare che la prova che è stata acquisita ha una natura non particolarmente diversa rispetto ai documenti ex art. 234 cod. proc. pen., se non riconducibile agli stessi.

Si tratta di cose che, pur avendo funzione probatoria, sono precostituite rispetto all'inizio del procedimento (nella specie, quello italiano) e appartengono, comunque, al contesto del fatto oggetto di accertamento.

La giurisprudenza di legittimità, difatti, ha ravvisato una relazione di genere a specie tra i documenti e la corrispondenza (cfr. Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, pag. 18), precisando che **la corrispondenza, anche informatica**, salvo la più peculiare tutela per il suo contenuto, **rientra nel fuoco dell'art. 234 cod. proc. pen.**, documento in generale (Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti).

La natura di corrispondenza, tuttavia, impone una tutela peculiare che comporta la necessità di acquisizione con decreto motivato dell'autorità giudiziaria, cui segue il riconoscimento di significative garanzie difensive (art. 257 cod. proc. pen.).

10.4. Il sequestro della corrispondenza, inoltre, è un istituto che, in un "*caso interno analogo*", sarebbe rimesso proprio all'iniziativa del pubblico ministero.

Tutte gli istituti disciplinati dal codice di rito a cui si è fatto cenno rinviano alla iniziativa del pubblico ministero.

Il pubblico ministero italiano, inoltre, ai sensi dell'art. 27, comma 1, del d.lgs. n. 108 del 2017 - normativa interna di recepimento della direttiva più volte citate - è l'organo legittimato a emettere, nell'ambito delle proprie attribuzioni, nella fase delle indagini preliminari, un ordine europeo di indagine volto all'acquisizione di una prova già disponibile,

perché oggetto di un sequestro già compiuto per ragioni di giustizia interna dall'Autorità di altro Stato membro, e a trasmetterlo direttamente all'autorità di esecuzione.

Sul tema della individuazione dell'autorità di emissione dell'OEI, comunque, si tornerà nel prosieguo.

10.5. Le investigazioni compiute in Francia sulla piattaforma criptata, d'altra parte, sono state avviate autonomamente sulla base di preesistenti *notitae criminis* relative, in via principale, al reato di associazione per delinquere finalizzata all'importazione di stupefacenti, come risulta dal provvedimento di sequestro dei tre server (ALL. n. 2), che richiama i provvedimenti esecutivi delle autorizzazioni all'intercettazione di comunicazioni elettroniche che lo hanno preceduto e reso possibile. In questi atti, il giudice istruttore francese ha affermato testualmente che "*la soluzione Sky ECC sembrava avere le caratteristiche di uno strumento utilizzato principalmente nel contesto delle attività della criminalità organizzata*" (cfr. il provvedimento del giudice istruttore di Lille del 14 giugno 2019 contenuto in ALL. 1). Questa affermazione è fondata su una serie di elementi indiziari precisamente riportati negli atti che, 'trasportati' nel nostro ordinamento, in un "caso interno analogo" integrerebbero il *fumus commissi deliciti* presupposto del sequestro.

10.6. Pur avendo riguardato il sequestro di *server* di una società che gestiva servizi di comunicazione, nondimeno, l'attività investigativa compiuta in Francia non è in nulla riconducibile ad una "sorveglianza di massa", così interpretando l'aggettivo "*massivo*" adoperato nell'ordinanza di rimessione Sez. 6, n. 2329 del 15/01/2024, con riferimento all'ipotesi in cui l'attività d'indagine sia qualificata come sequestro (pag. 17).

La sorveglianza di massa presuppone, come evidenziato in dottrina, che "*la persona, l'organizzazione o la caratteristica tecnica cui la raccolta dei dati è indirizzata non possono essere specificate preventivamente*".

Nella specie, le persone oggetto della misura dell'autorità francese sono state, invece, sufficientemente specificate e sono state oggetto di **tecniche investigative di sorveglianza "mirata"**, ossia quelle "*applicate dalle autorità competenti nel contesto di indagini penali* [o prima del loro formale inizio] *allo scopo di individuare e indagare su reati gravi e sospetti, e mirano a raccogliere informazioni in modo tale da non avvisare le persone bersaglio*" (Sul punto, Assemblea Generale, A/69/397, 23 settembre 2014, cfr. *www.europarl.europa.eu*). In questi casi, infatti, pur se l'investigazione ha condotto ad acquisire non flussi comunicativi di sistemi informatici determinati, ma tutti i flussi che transitano (o sono transitati) su un determinato *server*, esiste

un *target* di riferimento, così come esiste ed è sufficientemente individuato un "sistema" da monitorare.

Va sottolineato che il *target* individuato era rappresentato da soggetti che ritenevano necessario, per la riservatezza delle loro attività, interloquire con un meccanismo tecnologico fondato su ben quattro livelli di criptazione, così rendendo concreti i sospetti di svolgimento di gravi attività criminali di natura associativa.

La sufficiente specificamente del target, d'altra parte, **nel caso di una prova esistente, è una valutazione che spetta al giudice dello Stato di esecuzione che ha autorizzato l'atto**; la mancanza di tale presupposto può essere oggetto di impugnazione in detto Stato.

In Francia, sembra opportuno rimarcarlo, l'attività investigativa è stata compiuta su autorizzazione del giudice e nei confronti di soggetti che utilizzavano sofisticati sistemi di comunicazione per evitare l'intercettazione, ai quali sono stati riconosciuti efficaci rimedi impugnatori.

Il giudice istruttore francese, pertanto, ha ritenuto sufficientemente mirato l'obiettivo dell'intercettazione o del sequestro, affermando, come si è detto testualmente, che "*la soluzione Sky ECC sembrava avere le caratteristiche di uno strumento utilizzato principalmente nel contesto delle attività della criminalità organizzata*" (cfr. il provvedimento del giudice istruttore di Lille del 14 giugno 2019 contenuto in ALL. 1).

Basti solo pensare alle precauzioni che circondavano l'acquisto dell'abbonamento al servizio[13].

Il giudice istruttore francese, nel provvedimento del 17 dicembre 2020, difatti, ha sottolineato che "*les investigations menées tant par les autorités belges et néerlandaises que par les services d'enquête français démontrent le* ***caractère particulièrement opaque et sélectif*** *du système de vente de terminaux de la solution cryptée SkyECC …*", aggiungendo "*qu'il est en effet apparu que les transactions ayant trait à l'achat d'un terminal s'effectuaient moyennant un coût très élevé sinon prohibitif pour une clientèle ordinaire*" (cfr. ALL. n. 5).

Dunque, uno strumento che, già nel momento della vendita, si presenta "*opaco*", "*selettivo*", non rivolto, per i costi, ad una clientela "*ordinaria*".

Il Giudice istruttore francese, poi, ha affermato che "*Que ces moyens de chiffrement sont l'apanage d'une criminalité de très haute intensité; que l'ensemble de ces éléments inclinent à soupçonner que*

[13] Nella informativa della polizia giudiziaria francese si legge che "*era impossibile acquistare questo tipo di telefono direttamente sul sito web Sky ECC, 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 allora è stato dato, nel presente caso, in una retrobottega di un bar poco famoso, con un rivenditore. Quest'ultimo accettava solo soldi contanti e non chiedeva prove di indirizzo di identificazione. Inoltre, non sono state emesse fattura o documento di vendita*" (cfr. l'atto contenuto in ALL. 1).

ces téléphones sont destinés à un usage dans le cadre d'activités criminelles ; que ces éléments objectifs conduisent logiquement à envisager que la solution de téléphonie puisse être vendue intentionnellement à des fins criminelles pouvant caractériser une association de malfaiteurs ; que, de fait, l'information judiciaire a mis en évidence que la solution de téléphonie cryptée SkyECC était utilisée par des organisations criminelles agissant notamment aux PAYS BAS en BELGIQUE et en FRANCE et, pour certaines, à un niveau international" (cfr. ALL. n. 5)[14].

Mettere in discussione l'ampiezza del *target* o la determinazione del bersaglio dell'attività per come ritenuta dall'autorità francese, in provvedimenti argomentati che citano, per esempio "*Un elenco contenente quasi 9000 messaggi di utenti francesi di Sky ECC … fornito dalle autorità olandesi* [che] *ruotavano principalmente attorno al traffico di stupefacenti … e al regolamento di conti tra spacciatori*"[15] (cfr. ancora il provvedimento del giudice istruttore di Lille del 14 giugno 2019 contenuto in ALL. 1), **significherebbe entrare nel merito di tale giudizio** e, per questa via, **ledere in modo decisivo il principio del mutuo riconoscimento**.

La determinatezza del *target*, ad avviso di questo Ufficio, **non discende dal numero assoluto di utenze, ma dalla possibilità di distinguere sufficientemente coloro che sono oggetto della misura rispetto alla collettività indifferenziata dei fruitori di sevizi di comunicazione elettronica[16].**

Una indefinita acquisizione di dati contenuti in un sistema informatico in attesa dell'eventuale e futura comparsa del dato da acquisire a base delle indagini sarebbe compiuta se, per esempio, si adottasse un decreto di perquisizione e sequestro delle credenziali di accesso al sistema informatico di prenotazione dei voli *on line*, per identificare, nella massa di viaggiatori certamente non dediti al traffico di droga, i passeggeri sospettabili di fungere da

---

[14] "*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 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 crittografata SkyECC è stato utiilizzato da organizzazioni criminali che agiscono in particolare nei PAESI BASSI in BELGIO e in FRANCIA e, per alcuni, ad un livello internazionale*" (cfr. gli atti tradotti in ALL. n. 1).

[15] Nella richiesta del pubblico ministero presso il Tribunale di Lille del 14 giugno 2019, sul punto, è precisato che "*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 SK Y ECC. Il primo sfruttamento del contenuto di questi messaggi ha reso molto chiaro il sostegno all'utilizzo della soluzione SK Y ECC per scopi criminali, e in particolare nel contesto del traffico di droga, tema presente nella maggior parte dei messaggi raccolti*".

[16] E' stato già segnalato – a riprova che i fruitori del servizio non fossero una generica collettività di utenti di servizi di comunicazione elettronica – che dalla commissione rogatoria intercettazione della corrispondenza per via elettronica del giudice istruttore di Lille del 3 agosto 2020, risulta che, da metà giugno 2020 all'agosto 2020, il servizio ha registrato "*più di 30.000 nuovi utenti*" a seguito di migrazione di soggetti che in precedenza si avvalevano della soluzione crittografata *Encrochat* la quale è stata "*smantellata durante un'operazione* [di polizia] *congiunta tra Francia e Paesi* [Bassi]". L'esigenza di rendere anonime le conversazioni, dunque, era tanto pregante da determinare la rapida migrazione degli utenti (cfr. gli atti in ALL. 1).

corrieri internazionali di stupefacenti (c.d. ovulatori)[17]; diversamente, nella fattispecie in esame, il giudice francese ha emesso una misura che riguarda un determinato gestore di servizi, affermando che "*la soluzione Sky ECC sembrava avere le caratteristiche di uno strumento utilizzato principalmente nel contesto delle attività della criminalità organizzata*".

L'acquisizione indiscriminata di un'intera categoria di beni, nell'ambito della quale procedere successivamente alla selezione delle singole "*res*" strumentali all'accertamento del reato, d'altra parte, non costituisce di per sé una violazione del principio di proporzionalità. Il rispetto di detto principio può essere assicurato dalla motivazione di detta apprensione (come ha fatto il giudice francese) e dalla fissazione di efficaci criteri di selezione del materiale raccolto: come è avvenuto, nel caso in esame, da parte dei pubblici ministeri italiani che hanno chiesto determinate *conversation*, relative a specifiche persone, svolte in precisi ambiti temporali.

Il sequestro del server, in una ipotesi simile, in conclusione, **sarebbe consentita anche nel nostro ordinamento**, a condizione che il provvedimento non assuma una valenza meramente esplorativa e che il pubblico ministero adotti una motivazione che espliciti le ragioni per cui è necessario disporre un sequestro esteso e onnicomprensivo, in ragione del tipo di reato per cui si procede, della condotta e del ruolo attribuiti alla persona titolare dei beni e della difficoltà di individuare "*ex ante*" l'oggetto del sequestro (Sez. 6, n. 34265 del 22/09/2020 Rv. 279949 - 02).

10.7. Le stesse **funzionalità del criptofonino** dimostrano che l'attività di indagine svolta in Francia non è consistita in una indiscriminata apprensione di una massa di dati informatici, ma è stata rivolta ad uno specifico *target* costituito da affiliati ad organizzazioni criminali.

È stato già illustrato che gli apparecchi consentono funzioni come la **volatilità dei messaggi** con la possibilità, anche da parte di un terzo, di effettuare, da remoto sul dispositivo, l'**autodistruzione del contenuto del messaggio**, l'**impiego di "*fake up*"** (per simulare un apparato ordinario e trarre in inganno l'operatore di polizia in caso di eventuale controllo), la **possibilità di rilevare la presenza di *IMSI Catcher*** (il blocco dei cd. sms "silenti o occulti"), la **possibilità di inserire un cd. *panic code*** e la **possibilità di impiegare schede non intestate.**

Queste caratteristiche, oltre al prezzo e alle modalità di acquisto del servizio (prive di ogni tracciatura e riconducibilità formale ad un soggetto), circoscrivono precisamente

[17] L'esempio è tratto da Cass. Sez. 4, n. 19618 del 17/04/2012.

l'ambito degli utilizzatori. È, insomma, una 'riservatezza' univocamente ed esclusivamente finalizzata al compimento di attività criminali di acclarata ed assoluta gravità. Rispetto alla quale, dunque, non è eccentrica o blasfema, per l'ordinamento giuridico, (quantomeno) una problematica riflessione circa l'assolutezza della sua tutela e, più in generale, della sua sicura compatibilità con le archetipe e condivise affermazioni secondo cui la segretezza della comunicazione "è parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana" (così, Corte cost., sent. n. 366 del 1991). Detto senza ipocrisia, quale "armonia con i postulati della dignità umana" e quale attinenza con "il nucleo essenziale dei valori della personalità" (*ivi*) possa esprimere una riservatezza esclusivamente strumentale all'importazione di centinaia di kilogrammi di super-eroina o di cocaina rimane, in breve, interrogativo di non poco momento.

Nelle ordinanze impugnate, difatti, è stato affermato che i criptofonini "*risultano … particolarmente versatili per le esigenze operative ed elusive delle organizzazioni criminali*", giungendo alla conclusione che "*si tratta di apparecchi non intercettabili,* ***progettati per le attività criminali*** *e normalmente utilizzati - tenuto conto anche degli esorbitanti costi e della necessità di conoscere i nickname delle persone con cui si vuole conversare - da strutturate organizzazioni criminali*" (cfr. 4 – 5 dell'ordinanza del Tribunale di Reggio Calabria).

10.8. La Corte costituzionale, in particolare, ha rilevato che, in occasione del sequestro i dati informatici contenuti in un dispositivo elettronico, "*secondo le indicazioni della giurisprudenza di legittimità, vanno all'uopo selezionati e fatti possibilmente oggetto di una copia clone, con restituzione del dispositivo (e della disponibilità di tutti gli altri dati) al titolare*" (così, Corte cost., sentenza n. 170 del 2023, par. 5.1. del *Considerato*).

Si tratta di un profilo che, piuttosto che attenere alla condizione di cui all'art. 6, § 1, lett. b), della direttiva più volte citata, **riguarda la lett. a) della medesima disposizione, cioè la proporzionalità della misura nel procedimento penale interno** rispetto all'ingerenza sui diritti della persona sottoposta a indagini o imputata, su cui ci si soffermerà nel prosieguo di questa trattazione.

La Corte costituzionale, comunque, ha fatto esplicito riferimento all'elaborazione giurisprudenziale in tema di perquisizione e sequestro, ritenendo evidentemente che tale modulo procedurale garantisca un punto di equilibrio tra gli interessi in gioco, non impedendo agli organi investigativi di apprendere il dispositivo elettronico e di sequestrare i

dati informatici in esso contenuti nei limiti di quanto queste "*cose* [sono] *necessarie per l'accertamento dei fatti*" (art. 253, comma 1, cod. proc. pen.).

La Corte, nondimeno, ha fornito indicazioni chiare, desunte dall'elaborazione della giurisprudenza di legittimità. Il sequestro del contenitore è da ritenersi "strumentale" perché "*nel caso di sequestro probatorio informatico il "vero" oggetto del sequestro non è tanto il dispositivo elettronico (il "contenitore") - il quale, di per sé, non ha di norma alcun interesse per le indagini - quanto piuttosto i suoi dati (il "contenuto"), nella parte in cui risultano utili alle indagini stesse* …".

È allora solo il caso di anticipare che, nel caso di specie, il sequestro dei tre server disposto dall'autorità francese è stato l'unico modo per poter assicurare l'integrità del contenitore; **la specifica richiesta con OEI di determinate chat che riguardavano precisi soggetti indagati e relative ad un determinato arco temporale da parte dei pubblici ministeri italiani**, invece, **ha realizzato l'obiettivo della selezione del materiale utile alle indagini**.

Nel diritto interno è ormai acquisita la consapevolezza che **il sequestro di dispositivi elettronici comporta necessariamente una scansione operativa in più fasi**, rappresentate dal sequestro del sistema, dall'estrazione della copia forense dello stesso per garantirne l'integrità e dalla estrapolazione degli specifici dati in concreto rilevanti. Si tratta di una attività svolta per gradi, per consentire l'acquisizione dei dati contenuti nel sistema informatico e, allo stesso tempo, per assicurare la minor invasività dell'operazione nell'interesse della parte interessata (cfr. tra le altre, Sez. 5, n. 21488 del 18/01/2022).

10.9. Nel caso di specie, in conclusione, l'ordine europeo d'indagine adottato dal pubblico ministero presso il Tribunale di Potenza nel procedimento n. 33544/2023 RG in data 9 luglio 2021 ha riguardato **esclusivamente** le chat sequestrate originate da un determinato dispositivo attribuito ad un **certo** indagato, distinte in **23 *conversation*** intrattenute in uno **specifico arco temporale**, rispettando, come meglio si vedrà, il principio di proporzionalità richiamato dalla giurisprudenza della Corte di cassazione ai fini della legittimità del sequestro di dispositivi elettronici.

Si è trattato di un ordine di indagine relativo a prove esistenti in Francia, concernenti persone già indagate in Italia e già raggiunte da consistenti sospetti di traffico illecito di sostanze stupefacenti in grandi quantità, oltre che di appartenenza a un gruppo criminale organizzato.

Non diversamente è avvenuto nel procedimento n. 41618/2023 RG, nel quale, con OEI adottato dal pubblico ministero presso il Tribunale di Reggio Calabria, sono state

acquisite esclusivamente le chat sequestrate in Francia, siccome originate da determinati dispositivi attribuiti a specifici indagati.

11. - *segue*: La qualificazione delle *chat* come "risultati" di intercettazioni svolte in un diverso procedimento penale.

11.1. Questo Ufficio non nasconde che la qualificazione dell'attività svolta all'estero - dunque, **la** sua **sussunzione in un mezzo di ricerca della prova che sarebbe stato usato in un "*caso interno analogo*",** ai fini richiesti dall'art. 6, § 1, lett. b), della direttiva, in una vicenda investigativa di tale complessità da essere stata possibile solo con la collaborazione di forze di polizia di vari Stati dell'Unione - risulti in concreto complessa.

Tra gli atti delle indagini, in particolare, come è stato illustrato, sono presenti i provvedimenti del giudice istruttore di Lille, a partire dal primo, che risale al 14 giugno 2019, che consiste in una autorizzazione "*all'intercettazione, la registrazione e la trascrizione delle … comunicazioni elettroniche tra i due server situati … in Roubaix*", con l'informativa della polizia giudiziaria e con la "*richiesta di intercettazione della corrispondenza*" del pubblico ministero presso il Tribunale di Lille, oltre che gli atti di proroga successivi (ALL. 1).

Nonostante l'adozione di questi atti da parte del giudice istruttore francese, certamente il "caso interno analogo" non può essere rappresentato dall'autorizzazione delle intercettazioni ex art. 266 e ss. cod. proc. pen.

Non è stato emesso in concreto, né poteva essere emesso, un OEI di intercettazioni, né è stata elusa la relativa disciplina.

Nel modulo inviato alle autorità francesi non risulta compilata la sezione "H7" riservata all'intercettazione di comunicazione, né quella "H5" dedicata agli atti di indagine che implicano l'acquisizione di prove in tempo reale, in modo continuo e per un periodo determinato (così il Tribunale di Reggio Calabria, pag. 5). Né poteva essere diversamente: perché l'esecuzione di intercettazioni di comunicazioni elettroniche era già stata autorizzata in Francia; perché il flusso di comunicazioni non era più in corso quando è stato emesso l'OEI; perché nel nostro Paese **sono state trasmesse prove già esistenti** in quanto ***già*** raccolte autonomamente dallo Stato di esecuzione.

L'acquisizione delle chat registrate da altra autorità giudiziaria ha permesso **indagini "retrospettive"**, aventi ad oggetto "dati freddi" in quanto già raccolti in un procedimento diverso.

Quando lo scambio comunicativo non è più in corso, l'attività acquisitiva non rientra nel concetto di "intercettazione (Sez. U, n. 36747 del 28/05/2003, Torcasio, cit.).

11.2. Valorizzando la prima parte dell'attività d'indagine svolta in Francia e non il momento conclusivo della stessa rappresentato dal sequestro dei tre server, tuttavia, **potrebbe sostenersi che le conversazioni acquisite con ordine europeo di indagine costituiscano, in tutto o in parte, i risultati di una attività di intercettazione svolta dall'autorità giudiziaria straniera** (sebbene, come è stato chiarito, queste captazioni siano servite, in buona sostanza, per apprendere le quattro chiavi di cifratura, presenti sia sul server, sia sui singoli apparecchi mobili, e la prova trasmessa in Italia sia stata estratta, in forza di un criterio selettivo indicato dal pubblico ministero che ha emesso l'OEI, dal "contenitore" sequestrato).

Anche volendo seguire questa prospettiva, ad avviso di questo Ufficio, **deve ritenersi comunque rispettato il principio di equivalenza dapprima illustrato.**

Il trasferimento delle conversazioni intercettate nel procedimento penale che è stato svolto nello Stato di esecuzione dell'OEI, in tale ipotesi alternativa, va ricondotto alla disciplina dell'utilizzazione degli esiti delle intercettazioni in un altro procedimento e, dunque, alla previsione dell'art. 270 cod. proc. pen.

Un "*caso interno analogo*", dunque, **è quello in cui in Italia i risultati di intercettazioni** (cioè, il mezzo di prova) **sono trasferiti dal procedimento penale in cui sono state svolte ad un altro**.

È solo il caso di aggiungere che questa interpretazione risulta pienamente conforme al fatto che i flussi di comunicazione, al momento in cui tali dati sono stati chiesti dall'Autorità giudiziaria interna, non erano più in corso. L'art. 270 cod. proc. pen., infatti, consente, in presenza di determinate condizioni, l'utilizzazione degli esiti di intercettazioni già avvenute in un diverso procedimento.

11.3. La diversa prospettiva indicata, comunque, comporta che, ai fini del rispetto del principio di equivalenza fissato dall'art. 6, § 1, lett. b), della direttiva 2014/41/UE, devono sussistere i **presupposti che nel nostro ordinamento avrebbero giustificato il trasferimento dei risultati delle intercettazioni** disposte in un altro procedimento e, cioè, **la rilevanza e l'indispensabilità per l'accertamento** di delitti per i quali obbligatorio **l'arresto in fragranza di reato**.

Le cause di esclusione della prova previste dalla *lex fori*, che potrebbero venire in rilievo, difatti, sono quelle previste dall'art. 270 cod. proc. pen., che costituiscono diretta espressione del bilanciamento tra i diritti costituzionali confliggenti (cfr. Sez. U, n. 51 del 28/11/2019, dep. 2020, Cavallo, Rv. 277395 - 01).

Nel caso di specie, ricorrono pacificamente queste condizioni, trattandosi di procedimento relativo a reati che rientrano nel catalogo di cui all'art. 380 cod. proc. pen., la cui prova discende per una parte considerevole proprio dal tenore della corrispondenza intercettata.

Come si vedrà meglio nel prosieguo, le condizioni previste dall'art. 270 cod. proc. pen. rilevano anche ai fini della verifica della proporzionalità dell'ingerenza nei diritti della persona sottoposta ad indagini.

11.4. Anche accogliendo la soluzione illustrata, si deve ritenere corretto il riconoscimento in capo al pubblico ministero della prerogativa di richiedere il trasferimento degli esiti di intercettazioni, con ordine europeo di indagine, da un procedimento penale ad altro, in presenza di determinate condizioni, esattamente come sarebbe avvenuto in un "*caso interno analogo*".

Il pubblico ministero italiano, ai sensi dell'art. 27, comma 1, del d.lgs. n. 108 del 2017, come si è visto, è l'organo legittimato a emettere, nell'ambito delle proprie attribuzioni, nella fase delle indagini preliminari un OEI volto all'acquisizione di una prova già disponibile e a trasmetterlo direttamente all'autorità di esecuzione.

L'art. 270 cod. proc. pen., nel diritto interno, consente al pubblico ministero (o alla difesa) di chiedere l'utilizzo di esiti di intercettazioni realizzate *aliunde*, depositando verbali e registrazioni.

11.5. Non può sostenersi, peraltro, che l'OEI avrebbe dovuto essere preceduto da un provvedimento autorizzativo del giudice italiano sulla base dell'art. 43, comma 4, del d. d.lgs. n. 108 del 2017.

Quest'ultima norma, invero, disciplinando le modalità di intercettazione di telecomunicazioni da eseguirsi con l'assistenza tecnica dell'autorità giudiziaria di altro Stato membro dell'Unione europea, stabilisce che la richiesta contenuta in un ordine europeo di indagine "*possa avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate*". Tale previsione, tuttavia, riguarda i casi in cui l'autorità giudiziaria italiana chieda **congiuntamente** alla "*intercettazione delle conversazioni o comunicazioni o del flusso di comunicazioni*

relativo a sistemi informatici o telematici" (art. 43, comma 1, del d. d.lgs. n. 108 del 2017), anche ulteriori attività accessorie, quali "*la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate*" (art. 43, comma 4, del d. d.lgs. n. 108 del 2017).

Nel caso di specie, **l'autorità nazionale non ha chiesto l'intercettazione** e neppure la decriptazione della messaggistica captata, ma soltanto la trasmissione dell'esito di acquisizioni di comunicazioni già captate e già decriptate.

Difatti, per quanto risulta chiaramente dal titolo genetico e dall'ordinanza impugnata, l'intercettazione, l'acquisizione e la decrittazione delle comunicazioni intercettate erano operazioni già eseguite e completate dall'autorità francese prima che il pubblico ministero italiano procedesse all'emissione dell'OEI.

Secondo il costante orientamento della giurisprudenza di legittimità, del resto, la decriptazione del dato informatico è attività distinta dalla captazione di dati comunicativi *in itinere* dal mittente al destinatario (*ex plurimis,* Sez. 1, n. 6364 del 13/10/2022, Calderon, Rv. 283998-01; conf. Sez. 4, n. 16347 del 5/04/2023, Papalia, non massimata; Sez. 1, n. 34059 del 1/07/2022, n. 34059, Molisso, non massimata, pronunce tutte relative all'acquisizione della messaggistica scambiata con sistema cifrato "*Sky Ecc*" e "Encrochat"; Sez. 6, n. 18907 del 20/04/2021, Civale, Rv. 281819 - 01).

11.6. Secondo un percorso ricostruttivo illustrato nella seconda ordinanza di rimessione (Sez. 6, n. 2329 del 2024, pag. 20 e ss.), peraltro, l'individuazione nell'art. 270 cod. proc. pen. della norma che, in un "*caso interno analogo*", avrebbe giustificato l'importazione della prova raccolta *aliunde*, non esclude "*che occorrerebbe verificare, in ossequio al principio di equivalenza, se l'attività di utilizzo del trojan da parte dell'autorità giudiziaria francese non contrasti con i principi generali del nostro ordinamento processuale che disciplinano l'ambito di utilizzo di detto strumento di captazione delle comunicazioni*".

Detta valutazione, in particolare, "*andrebbe condotta alla luce della previsione dell'art. 271 cod. proc. pen.*". Nel giudizio *ad quem,* infatti, il giudice "*è tenuto a procedere ad un'autonoma valutazione circa la sussistenza dei presupposti e delle condizioni di legittimità delle operazioni di intercettazione disposte nel procedimento originario*" (Sez. 6, n. 36874 del 13/06/2017, Romeo, Rv. 270812). A tale ultimo riguardo, il riferimento è al principio secondo cui l'inutilizzabilità dei risultati di intercettazioni di conversazioni o comunicazioni è rilevata dal giudice del procedimento diverso da quello nel quale furono autorizzate solo quando essa risulti dagli atti di tale procedimento, non essendo tenuto il giudice a ricercarne d'ufficio la prova. Grava, infatti, sulla parte interessata a farla valere l'onere di allegare e provare il fatto dal quale

dipende l'eccepita inutilizzabilità, sulla base di copia degli atti rilevanti del procedimento originario che la parte stessa ha diritto di ottenere, a tal fine, in applicazione dell'art. 116 stesso codice (Sez. U, n. 45189 del 17/11/2004, PM in proc. Esposito, Rv. 229245 - 01).

Il tema, invero, sembra far emergere una questione di fondo che sembra pervadere tutte quelle poste alle Sezioni unite, così sintetizzabile: "*Se nell'ordinamento interno sia legittimo disporre ed effettuare il suindicato complesso sistema di acquisizione delle chiavi di decrittaggio nell'ambito della intercettazione effettuata su un server di una piattaforma informatica*" (così Sez. 6, ord. n. 2329 del 15/01/2024, G------, pag. 25).

La domanda posta, ad avviso di questo Ufficio, non sembra molto diversa da un interrogativo più intenso e diretto: se, cioè, il livello di garanzie assicurate dall'ordinamento francese – almeno quelle che sono state assicurate ai cittadini nel caso di specie - sarebbe equiparabile a quello riconosciuto dal diritto nazionale, posto che l'intercettazione del server è avvenuta in Francia e che nel nostro Paese sono state trasmesse specifiche conversazioni, relative a determinati indagati.

11.7. La prospettiva ricostruttiva illustrata, ad avviso di questo Ufficio, non risulta condivisibile.

Potrebbe in proposito, ed innanzitutto, rilevarsi al riguardo come l'art. 6 della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale non preveda, per la sua inosservanza, un'espressa causa di inutilizzabilità della prova già in possesso dell'autorità di esecuzione, né essa è contemplata dalle disposizioni del d.lgs. 21 giugno 2017, n. 108, che ha recepito la direttiva.

Come è stato già indicato, anche in tema di rogatorie l'utilizzazione degli atti trasmessi dalle autorità giudiziarie straniere in adesione alle richieste di rogatoria non è condizionata all'accertamento, da parte del giudice italiano, della regolarità degli atti compiuti dall'autorità straniera. Vige, cioè, una **presunzione di legittimità** dell'attività svolta e spetta al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate: la verifica cui è chiamato il giudice nazionale è quella della **compatibilità del diritto straniero**, sulla base del quale l'atto sia compiuto, **con i principi inderogabili dell'ordinamento interno**, spettando, comunque, a colui che eccepisca il difetto di compatibilità darne la prova, tanto più ove si tratti di Paese membro dell'Unione Europea (Sez. 4, n. 19216 del 06/11/2019, dep. 2020, Rv. 279246 – 01; Sez. 5, n. 45002 del 13/07/2016, Rv. 268457 - 01).

Questo principio, secondo cui la prova che sia stata assunta all'estero sulla base della *lex loci* deve, per presunzione, considerarsi utilizzabile - sempre che non sia stata acquisita al termine di un procedimento probatorio che abbia importato la lesione di un principio fondamentale o di una norma inderogabile della *lex fori* - opera a maggior ragione nel caso ricorso all'ordine europeo di indagine (Sez. 1, n. 19082 del 13/01/2023, Rv. 284440 - 01).

Soprattutto, appare opportuno segnalare che, seguendo il percorso delineato, di fatto, **si consentirebbe la deduzione nel procedimento penale interno, come causa di inutilizzabilità, di un preteso vizio della raccolta della prova, che comunque è avvenuta all'estero secondo la *lex loci* e che non è stato oggetto di contestazione nello Stato di esecuzione** (pur potendo ivi essere dedotto con mezzi di impugnazione). **Ne verrebbe irrimediabilmente incrinato il principio del mutuo riconoscimento delle decisioni e la fiducia che ispira i rapporti tra gli Stati membri in tema di cooperazione penale**, ammettendo in sostanza che in Italia, tramite i principi di necessità, proporzionalità e equivalenza che governano le modalità di funzionamento dell'OEI, si possa valutare, in forza di regole interne, l'attività di raccolta della prova svolta in Francia su autorizzazione del giudice istruttore, ritenuta lesiva di prerogative fondamentali (per giunta, in una fattispecie in cui, nello Stato estero, è stata assicurata ampia tutela delle prerogative individuali, con impugnazioni culminate finanche in un procedimento dinanzi alla Corte costituzionale). Si precisa infatti che si deve lasciare ferma solo "… *la legittimità dell'emissione da parte della competente autorità giudiziaria italiana e della conseguente trasmissione dei relativi atti di indagini da parte dell'autorità estera …"* (così, Sez. 6, ord. n. 2329 del 15/01/2024, G_____, pag. 21) e non la legittimità dell'atto giudiziario francese.

L'autorità di emissione dell'OEI, invece, **non può sindacare la legittimità delle misure mediante le quali lo stato di esecuzione ha raccolto le prove**, in quanto spetta ai giudici di tale Stato conoscere dei ricorsi giurisdizionali avverso tali atti, con l'unico limite della *manifesta* lesione dei principi inderogabili dell'ordinamento interno (italiano), la cui prova spetta a colui che eccepisca il difetto di compatibilità della prova.

11.8. Peraltro, quand'anche si ritenesse possibile, in forza del principio di equivalenza e di proporzionalità, sindacare nel procedimento penale interno l'ammissione della prova e le modalità della sua raccolta in Francia (cioè, usando le parole adoperata da un precedente della Corte di cassazione, si ritenesse che, "*nel caso di risultati di operazioni di intercettazione già disponibili nello Stato di esecuzione, la norma di riferimento nella prospettiva nazionale non può essere soltanto l'art. 270 cod. proc. pen. che regola l'utilizzazione della prova acquisita in altro procedimento*",

così, Sez. 6, n. 44154 del 26/10/2023, Iaria, cit.), dovrebbe comunque, in un "*caso interno analogo*", reputarsi insussistente il profilo di inutilizzabilità della prova acquisita, dovendo escludersi, per una serie di ragioni, che le intercettazioni "*siano state eseguite fuori dei casi consentiti dalla legge*" (art. 271 cod. proc. pen.).

11.9. In particolare, la seconda ordinanza di rimessione (Sez. 6, n. 2329 del 15/01/2024, pag. 25) adombra il sospetto di inutilizzabilità delle operazioni captative volte ad acquisire l'algoritmo di cifratura (o 'decifratura') della messaggistica mediante inoculazione del *trojan* all'interno di uno o più *server* per comunicazioni telematiche e non all'interno di un dispositivo elettronico portatile (come, ad esempio, uno *smartphone* o un *tablet*).

In tal senso è specificamente rappresentato nell'ordinanza di rimessione (pag. 25) che "*l'utilizzo del captatore informatico è, nelle diverse disposizioni processuali previste dal codice di rito (art. 266, commi 2 e 2-bis, 267, commi 1 e 2-bis, disp. att. c.p.p.) autorizzato soltanto per l'inserimento su un "dispositivo elettronico portatile*" (in argomento, v. anche Sez. U., n. 26889 del 28/04/2016, Scurato, Rv. 266905 – 01).

Tale impostazione non può tuttavia essere condivisa.

La possibilità di utilizzare per scopo investigativo il *trojan* è espressamente disciplinata dal legislatore dall'art. 266 c.p.p., con specifico riferimento all'intercettazione di "*comunicazioni tra presenti*", ossia alla captazione di dialoghi e comunicazioni che avvengono "in presenza tra persone fisiche", che, per la pervasività del "captatore informatico", per il monitoraggio continuo del possessore del dispositivo infettato e per la mobilità del soggetto bersaglio, richiedono limiti e garanzie, in quanto il detentore può recarsi in luoghi di privata dimora.

Il caso in esame è del tutto diverso ed estraneo all'ambito applicativo dell'art. 266 c.p.p., atteso che viene in rilievo l'acquisizione di dati elettronici, programmi informatici, codici crittografici e informazioni scambiate telematicamente, che sono manifestamente estranei alla nozione di "*comunicazioni tra presenti*".

Non si tratta di comunicazioni tra persone fisiche che si muovono sul territorio e che, per comunicare, utilizzano smartphone o altri dispositivi mobili, sì da porre, eventualmente, un problema di limiti e garanzie in ragione dei luoghi di 'privata dimora' in cui tali conversazioni possono avvenire; quanto piuttosto si verte **in tema di dialogo circuitale e di scambio elettronico di dati informatici tra computer** (fissi e non mobili), per cui l'Autorità giudiziaria francese ha utilizzato un autonomo mezzo di ricerca della prova che non presenta 'interferenze' con le intercettazioni telefoniche e/o ambientali già disposte con i mezzi ordinari di captazione.

Nel diritto interno vengono in rilievo le "*intercettazioni informatiche o telematiche*" disciplinate dall'art. 266-*bis* cod. proc. pen., disposizione che consente "*l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi*", nei procedimenti relativi ai reati indicati nell'art. 266 c.p.p. ed **in quelli relativi a reati commessi mediante l'impiego di tecnologie informatiche o telematiche**.

Quest'ultima espressione merita particolare approfondimento, perché permette di ampliare la sfera del ricorso alle intercettazioni, non è più circoscritta ai soli procedimenti riguardanti ben determinate tipologie criminose, ma estesa a tutte le categorie di reato commessi con l'impiego di tecnologie di comunicazione digitale e di trattamento di informazioni.

La formula utilizzata dal legislatore è molto ampia. Essa non presuppone, come in Francia, la violazione della legislazione sui mezzi di criptografia, **ma si ricollega all'impiego di tecnologie avanzate e particolarmente insidiose per la commissione di reati**, che rende necessario il ricorso a tutti gli strumenti di ricerca della prova più innovativi per identificare i responsabili e per contrastare in modo adeguato l'emergenza criminale.

Lo strumento investigativo regolamentato dall'art. 266-*bis* cod. proc. pen., dunque, è utilizzabile anche nei casi in cui l'impiego delle tecnologie informatiche è funzionale al conseguimento del fine criminoso che si propone l'agente.

Il sistema codicistico non limita le intercettazioni soltanto ai reati ontologicamente elettronici introdotti dalla legge 23 dicembre 1993, n. 547 (sui c.d. *computer's crime*), ma le estende a qualsiasi fattispecie per la cui realizzazione l'autore del fatto ha utilizzato gli strumenti informatici o telematici.

Per legittimare l'esecuzione delle operazioni di captazione del flusso digitale è sufficiente che un reato sia stato consumato o, comunque, agevolato dalla tenuta di una banca dati o dallo scambio di file, di chat, di messaggi SMS e di posta elettronica.

L'intercettazione deve avere ad oggetto il "*flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrenti tra più sistemi*", ossia deve riguardare la trasmissione o lo scambio di dati, informazioni, suoni, immagini, simboli, o programmi tra due o più sistemi, tanto che nel provvedimento autorizzativo delle operazioni captative dei flussi di "bit" si fa usualmente espresso riferimento "all'intercettazione giudiziaria tra due server".

Un insieme di dati è il dialogo comunicativo, sotto forma di energie, all'interno di un elaboratore elettronico o tra più sistemi telematici interconnessi, che scambiano impulsi in grado di costituire una comunicazione al pari di una conversazione telefonica.

Il legislatore nazionale è intervenuto a regolamentare l'utilizzo del captatore informatico per la sua estrema pervasività e per la possibilità di agire e funzionare anche in luoghi di privata dimora (carpendo anche momenti di intimità), ma evidentemente queste esigenze di garanzia non sussistono per i server e per le postazioni informatiche fisse e non portatili.

Tali considerazioni spiegano la ragione per la quale il legislatore non è intervenuto a disciplinare l'utilizzo del captatore informatico – anche in occasione della recente modifica normativa dell'art. 266 cod. proc. pen. - in riferimento all'inoculazione di esso su "dispositivi elettronici fissi", che non interferiscono con la privacy e con la vita privata del soggetto bersaglio.

La possibilità di inserire il *malware* all'interno di un *server*, allora, **refluisce in una scelta investigativa del tutto ammissibile e utilizzabile, che è stata funzionale ad acquisire in qualsiasi modo il programma informatico o l'algoritmo di decifrazione dei flussi di dati già captati** (non essendo previste limitazioni o restrizioni operative nell'art. 266-*bis* c.p.p.).

Non pare pertanto che, per sostenere tale conclusione, vi sia necessità di richiamare la previsione di cui all'art. 189 cod. proc. pen. perché l'aspetto relativo all'utilizzo del *trojan* in un dispositivo fisso e per acquisire le chiavi di decrittaggio risulta affrontabile nell'ambito della previsione dell'art. 266-*bis* cod. proc. pen.

Per la legittimità dell'attività con cui sono stati prelevati e copiati dati memorizzati sul computer – nella specie, le chiavi di decrittaggio – come prova atipica, in ogni caso, si è già pronunciata la Corte di cassazione in una nota sentenza (Sez. 5, n. 16556 del 14/10/2009, dep. 2010, Virruso ed altri, Rv. 246954 - 01).

11.10. La previsione dell'art. 266, comma 2, c.p.p. – si ribadisce - non sarebbe in ogni caso di ostacolo, in un "*caso interno analogo*", all'intercettazione dei criptofonini, anche mediante l'inserimento di un captatore informatico in un *server* per cogliere la chiave di cifratura.

Tale disposizione, nella parte in cui stabilisce che "*Negli stessi casi* [quelli indicati nel comma 1 della norma, n.d.r.] *è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*", non limita l'uso dello strumento ai soli dispositivi portatili; piuttosto, ha ritenuto di dover disciplinare il profilo più delicato del bilanciamento dei diritti confliggenti, **permettendone**

l'uso anche in un dispositivo portatile, pure se, per sua natura itinerante, è in grado potenzialmente di compiere intercettazioni "*tra presenti*" in ambienti non determinabili.

La norma non esclude che il *trojan* possa essere inoculato in un dispositivo informatico fisso; piuttosto ne ammette l'utilizzo in un dispositivo portatile - l'ipotesi maggiormente messa in discussione sotto il profilo del bilanciamento tra i diritti confliggenti - per realizzare intercettazioni tra presenti. In questi termini si è già espressa la Corte di cassazione (Sez. 5, n. 48370 del 30/05/2017, Occhionero, Rv. 271412 – 01; Sez. 1, n. 3591 del 07/10/2021, dep. 2022).

Sarebbe paradossale, del resto, ritenere che la disposizione indicata permetta una intercettazione in astratto più invasiva, perché itinerante, ed impedisca una captazione che lo è certamente di meno perché concentrata in un dispositivo fisso.

11.11. Come è stato rilevato espressamente nella seconda ordinanza di rimessione (pag. 26), l'art. 1, comma 2-*bis*, introdotto dalla legge di conversione n. 137 del 2023 del decreto-legge n. 105 del 2023 ha previsto, riformando l'art. 267 cod. proc. pen., che l'autorità che autorizza l'impiego del captatore informatico deve assolvere un rigoroso onere motivazionale nella esposizione di un'autonoma valutazione della necessità "*in concreto*" del ricorso a tale modalità tecnica di espletamento del mezzo di ricerca della prova.

Con la nuova formulazione della norma, dunque, è stato ribadito che l'autorizzazione all'utilizzo, per la realizzazione di captazioni tra presenti, di uno strumento tanto invasivo della riservatezza della persona come il captatore informatico presuppone una motivazione "rafforzata" da parte del Gip, il quale è tenuto a dare adeguato conto, nel rispetto del principio di proporzionalità, del bilanciamento da egli operato tra i diritti costituzionali confliggenti.

Anche in questo caso, **la norma richiamata disciplina il decreto che autorizza l'intercettazione "*tra presenti*" per mezzo dell'inserimento di captatore informatico su dispositivo elettronico portatile e non l'intercettazione del flusso di comunicazioni relativo a sistemi informatici** ovvero intercorrente tra più sistemi di cui all'art. 266-*bis* cod. proc. pen.

Comunque, basta solo rinviare ai provvedimenti dell'autorità giudiziaria francese, per individuare la motivazione "*in concreto*" della necessità dello strumento adoperato, esattamente come ormai prescriverebbe il codice di rito in un caso interno analogo. Per esempio, nella "*Commissione rogatoria - Intercettazione di corrispondenze tramite via elettroniche",* il Vice-Presidente responsabile dell'istruzione ha precisato, tra l'altro, di essere "*sicuri del fatto che questo sistema*

criptato era utilizzato da organizzazioni criminali con lo scopo di mettere la loro comunicazione al riparo da eventuali investigazioni di polizia o giudiziarie e di scambiarsi messaggi in maniera anonima" (ALL. 1).

11.12. Le investigazioni compiute in Francia sulla piattaforma criptata, d'altra parte, pur avendo riguardato le comunicazioni tra due *server* di una società che gestiva servizi di comunicazione e le comunicazioni in uscita da un server, come è stato già illustrato, non sono riconducibili ad una "sorveglianza di massa", così interpretando l'aggettivo "*massivo*" adoperato nell'ordinanza di rimessione Sez. 6, n. 2329 del 15/01/2024, sia con riferimento all'ipotesi in cui l'attività d'indagine sia qualificata come sequestro (pag. 17), sia, nei motivi di ricorso, con riferimento all'ipotesi che le indagini svolte siano riconducibili alle intercettazioni.

Nella specie, le persone oggetto della misura dell'autorità francese sono state sufficientemente specificate e sono state oggetto di **tecniche investigative di sorveglianza "mirata"**, ossia quelle "*applicate dalle autorità competenti nel contesto di indagini penali* [o prima del loro formale inizio] *allo scopo di individuare e indagare su reati gravi e sospetti, e mirano a raccogliere informazioni in modo tale da non avvisare le persone bersaglio*" (Sul punto, Assemblea Generale, A/69/397, 23 settembre 2014, cfr. *www.europarl.europa.eu*). In questi casi, infatti, pur se l'investigazione non è diretta ad acquisire flussi comunicativi di sistemi informatici determinati, ma tutti i flussi che transitano (o sono transitati) su un determinato *server*, esiste un *target* di riferimento, così come esiste ed è sufficientemente individuato un "sistema" da monitorare.

Va sottolineato che il *target* individuato era rappresentato da soggetti che ritenevano necessario, per la riservatezza delle loro attività, interloquire con un meccanismo tecnologico fondato su ben quattro livelli di criptazione, così rendendo concreti i sospetti di svolgimento di gravi attività criminali.

È solo il caso di precisare che il presupposto per il ricorso alle intercettazioni, in considerazione del delitto ipotizzato, è rappresentato dalla sussistenza di sufficienti indizi di reato.

La sufficiente specificamente del target, d'altra parte, **nel caso di una prova esistente, certamente è una valutazione che spetta al giudice dello Stato di esecuzione che ha autorizzato l'atto**; la mancanza di tale presupposto può essere oggetto di impugnazione in detto Stato.

In Francia, sembra opportuno rimarcarlo, l'attività investigativa è stata compiuta su autorizzazione del giudice e nei confronti di soggetti che utilizzavano sofisticati sistemi di

comunicazione per evitare l'intercettazione, ai quali sono stati riconosciuti efficaci rimedi impugnatori.

Il giudice istruttore francese, pertanto, ha ritenuto sufficientemente mirato l'obiettivo dell'intercettazione o del sequestro, affermando testualmente che "*la soluzione Sky ECC sembrava avere le caratteristiche di uno strumento utilizzato principalmente nel contesto delle attività della criminalità organizzata*" (cfr. il provvedimento del giudice istruttore di Lille del 14 giugno 2019 contenuto in ALL. 1).

Mettere in discussione la determinazione del bersaglio dell'attività di intercettazione per come ritenuta dall'autorità francese, in provvedimenti argomentati, **significherebbe entrare nel merito di tale giudizio** e, per questa via **ledere in modo decisivo il principio del mutuo riconoscimento**.

Come già in precedenza evidenziato, la determinatezza del *target*, ad avviso di questo Ufficio, **non discende dal numero assoluto di utenze, ma dalla possibilità di distinguere sufficientemente coloro che sono oggetto della misura rispetto alla collettività indifferenziata dei fruitori di sevizi di comunicazione elettronica.**

11.13. Va sottolineato, d'altra parte, che **lo stesso meccanismo di funzionamento del sistema di comunicazione criptato è tale che, senza intercettare prima il *server* e, poi, inoculare in esso un *trojan*, non si può realizzare l'attività investigativa in modo utile sui singoli apparecchi, apprendendo le chiavi di cifratura necessarie a decodificare quanto acquisito**.

Il principio di proporzione, come meglio si vedrà nel prosieguo, deve orientare l'autorità giudiziaria anche nella individuazione dell'atto d'indagine che avrebbe potuto essere emesso in un caso interno analogo; va compiuta l'attività che implica la minore inerenza sulle prerogative individuali (cfr. l'art. 7 del d.lgs. n. 108 del 2017, seppur relativo alla disciplina della richiesta di OEI dall'estero). Una minore ingerenza, nella specie - **evitando di coinvolgere nell'attività eventuali estranei alle attività criminali, che peraltro non sono emersi e la cui esistenza costituisce solo un'ipotesi vaga -** non era possibile: l'unica alternativa era quella di non utilizzare il mezzo di ricerca della prova, pur in presenza di gravi indizi di criminalità grave.

Nella specie, dunque, il meccanismo tecnologico utilizzato per comunicare non permetteva di realizzare in modo utile l'attività investigativa utilizzando misure meno invasive.

Anche in un caso interno analogo una simile attività investigativa non avrebbe potuto svolgersi se non intercettando il server per apprendere le chiavi di cifratura.

Codesta Corte di cassazione, infatti, **ha già affermato che sono legittime le intercettazioni di comunicazioni informatiche o telematiche, di cui all'art. 266-*bis* cod. proc. pen., effettuate mediante l'istallazione di un captatore informatico** (c.d. "*trojan horse*") all'interno di un computer collocato in un luogo di privata dimora (Sez. 5, n. 48370 del 30/05/2017, Occhionero, Rv. 271412 – 01, cit.; Sez.1, n.3591 del 07/10/2021, dep. 2022).

La Corte, del resto, aveva già ritenuto legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati (Sez. 5, n. 16556 del 14/10/2009, dep. 2010, Virruso ed altri, Rv. 246954 – 01, cit.).

Né per escludere la legittimità del mezzo di ricerca della prova potrebbe genericamente farsi riferimento ad una violazione del domicilio informatico, inteso come spazio ideale in cui sono contenuti i dati informatici di pertinenza della persona, a cui viene estesa la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (cfr., tra le altre, Sez. 5, n. 27900 del 22/02/2023). Secondo indirizzo giurisprudenziale consolidato, la finalità di intercettare consente all'operatore di polizia la materiale intrusione, per la collocazione dei necessari strumenti di rilevazione, negli ambiti e nei luoghi di privata dimora, oggetto di tali mezzi di ricerca della prova (Sez. 6, n. 39403 del 23/06/2017, Nobile, Rv. 270941 – 01; Sez. 6, n. 41514 del 25/09/2012, Adamo, Rv. 253805 - 01).

Va rimarcato comunque **che l'intercettazione del *server* e l'inoculazione del *trojan* è stata servente o strumentale all'intercettazione dei criptofonini**[18].

In questi casi, necessariamente la platea degli intercettati si amplia, altrimenti non può svolgersi l'attività d'indagine: **il bilanciamento delle prerogative individuali**, tuttavia, **è stato adeguatamente assicurato nella fase dell'utilizzazione della prova**, nella quale si procede alla selezione del materiale probatorio.

---

[18] Nel provvedimento del giudice istruttore del 17 dicembre 2020, come è stato già indicato, si legge che "*le déchiffrement des messages individuels ne peut être réalisé à partir des seules données interceptées dans la mesure où seule la partie des éléments cryptographiques acheminée par les téléphones sur les serveurs est susceptible d'être récupérée au travers des données interceptées; l'autre partie des éléments cryptographies étant uniquement stockée sur les téléphones*" (ALL. n. 5)

11.14. Deve rilevarsi, d'altra parte, che, a ritenere illegittimo l'uso del *trojan* nelle forme adoperate nella specie, **la messaggistica criptata non sarebbe intercettabile**. Nonostante le previsioni di cui agli artt. 266 e ss. c.p.p., che non prevedono distinzioni, i telefoni sarebbero intercettabili salvo siano criptati, introducendo **una sorta di immunità** dal mezzo di ricerca della prova per coloro che possono dotarsi di simili apparecchi. Ciò sarebbe affermato proprio in un momento storico in cui, come è stato acutamente e significativamente riconosciuto dalla migliore dottrina, "*non esiste più alcuna organizzazione criminale dedita al narcotraffico minimamente strutturata, che non comunichi su piattaforme di messaggistica crittografata, accessibili attraverso i criptofonini*"[19].

Se, dunque, non pare seriamente discutibile la possibilità che i criptofonini siano tra gli apparecchi oggetto di intercettazione, allora non possono che postularsi come legittime, nella cornice normativa data, le operazioni informatiche **indispensabili e prive di alternativa tecnica** – nella specie, la captazione del flusso dati tra due *server* - che permettano l'acquisizione delle chiavi di cifratura.

L'intercettazione dei telefoni criptati nel nostro ordinamento, in altri termini, può avvenire anche quando, come nel caso di specie, il meccanismo tecnologico adoperato implica *necessariamente* l'inoculazione di un captatore informatico nel *server* utilizzato per le comunicazioni al fine di cogliere le chiavi di cifratura che sono tanto negli apparecchi, quanto nel *server*.

La qualificazione giuridica dell'attività investigativa, in breve, non può prescindere da uno sforzo di comprensione del sistema tecnologico sul quale essa si è innestata e, per un ovvio quanto doveroso rispetto del "principio di realtà", non può che considerare tale sistema quale variabile indipendente, così evitando di ragionare per archetipi astratti.

Bisognerebbe ritenere, altrimenti, che il diritto alla riservatezza delle conversazioni criptate – una sorta di diritto "tiranno" - sia onnivoro e prevalga sempre e comunque rispetto alla azione dello Stato (*recte:* degli Stati) per l'accertamento dei reati, senza alcuna possibilità di bilanciamento, anche in un caso in cui, in forza di specifici OEI, siano state acquisite soltanto determinate conversazioni relative a specifici soggetti, i quali, in sostanza, da indagati per un massivo narcotraffico intercontinentale di stupefacenti, si trasformano in paladini della minacciata legalità per i terzi estranei, co-fruitori della medesima piattaforma criptata,

[19] Così, M.T. Morcella, *Sky ECC: la partita vera si giocherà intorno all'art. 270 cod. proc. pen*., in *IUS penale*,13 novembre 2023

dolendosi della lesione della riservatezza di detti terzi, non indagati, anzi, persino non identificati, e le cui conversazioni non sono emerse nel corso delle indagini, né prese in considerazione in esse, né lo saranno mai.

Il diritto di comunicare in modo riservato, ai sensi dell'art. 15 Cost., invece, è soggetto a limitazione "*per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*".

11.15. Il vizio di inutilizzabilità, infine, non potrebbe derivare dalla prospettata violazione dell'art. 31 della direttiva OEI.

Questa disposizione infatti - disciplinando lo svolgimento di attività di intercettazioni per le quali non è necessaria l'assistenza tecnica dello Stato nel quale si trova la persona le cui conversazioni sono captate - subordina l'adempimento della notifica all'autorità competente dello Stato membro alla consapevolezza, al momento in cui è stata ordinata l'intercettazione, che la persona soggetta al mezzo di ricerca della prova si trova o si troverà nel territorio dello Stato notificato (art. 31, par. 1, lett. a), della direttiva). Non vi è prova, nel caso di specie, che l'autorità francese avesse questa conoscenza con riguardo ai ricorrenti.

La notifica, d'altra parte, può essere anche successiva alla esecuzione del mezzo di ricerca della prova. In questo caso, essa va compiuta "*non appena* [lo Stato che ha disposto l'intercettazione] *venga a conoscenza del fatto che la persona soggetta ad intercettazione si trova o si trovava durante l'intercettazione sul territorio dello Stato membro notificato*" (art. 31, par. 1, lett. b). La disposizione unionale, in tal modo, stabilisce un termine iniziale ("*non appena*"), ma non fissa un termine oltre il quale l'adempimento non possa essere più compiuto, né esclude che l'atto – l'informazione al pubblico ministero di altro Stato membro - sia insito nello svolgimento di attività di cooperazione giudiziaria (come nella specie, sarebbe la trasmissione delle captazioni in esecuzione di OEI trasmesso proprio dal pubblico ministero). La notifica, infatti, servirebbe a tutelare le prerogative dello Stato membro in cui si trova la persona intercettata, il quale non solo non ha ritenuto che la sua sovranità sia stata lesa, ma anzi ha sollecitato la trasmissione della prova raccolta.

La norma unionale, comunque, limita l'utilizzo dei risultati della captazione non preceduta dalla notifica soltanto alle ipotesi in cui l'intercettazione "*non sia ammessa in un caso interno analogo*", circostanza che, nel caso in esame, non sussiste per le ragioni dapprima illustrate. La causa di esclusione della prova, inoltre, ha una portata non assoluta, in quanto "*se necessario, gli eventuali risultati delle intercettazioni già ottenute … possono essere utilizzati solo alle condizioni da essa* [dall'autorità dello Stato membro in cui si trova la persona intercettata] *specificate*". Essa, infine, sembra colpire l'uso degli esiti delle intercettazioni nello Stato che le

ha eseguite e non l'impiego degli stessi nello Stato membro in cui si trovata la persona oggetto del mezzo di ricerca della prova e che non ha ricevuto la notificazione in esame (art. 31, par. 3, della direttiva).

Queste regole risultano conformi alla disciplina di cui all'art. 44 d.lgs. n. 108 del 2017 che, infatti, non regola una causa di inutilizzabilità, ma precisa che "*i risultati dell'intercettazione [non preceduti dalla notifica] possono comunque essere utilizzati alle condizioni stabilite dall'autorità giudiziaria dello Stato membro*", in una chiara prospettiva di salvezza del mezzo di prova raccolto.

12. - Il rispetto del principio di proporzionalità dell'ingerenza nei diritti della persona sottoposta a indagini o imputata (art. 6, § 1, della direttiva OEI).

12.1. Le condizioni che l'autorità di emissione deve valutare ai fini dell'emissione di un OEI, come già segnalato più volte, sono stabilite all'art. 6, § 1, della direttiva OEI.

Tale disposizione stabilisce non solo il rispetto del principio di equivalenza rispetto ad un "*caso interno analogo*", ma anche che l'emissione dell'ordine debba essere necessaria e **proporzionata**, nel procedimento interno, quanto all'ingerenza nei diritti della persona sottoposta a indagini o imputata.

Anche in questo caso si tratta di una condizione per l'emissione dell'ordine, che rileva nel momento dell'ammissione dell'atto istruttorio. Ai sensi dell'art. 14, § 2, della direttiva OEI, anche il mancato rispetto di tale condizione può essere contestato nello Stato di emissione ("*Le ragioni di merito dell'emissione dell'OEI possono essere impugnate soltanto mediante un'azione introdotta nello Stato di emissione, fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione*").

L'inosservanza della proporzionalità dell'ingerenza sulle prerogative individuali, risolvendosi in una violazione dei diritti fondamentali, però, può essere dedotta come motivo di inutilizzabilità della prova.

Si tratta di applicare un principio generale di diritto che postula l'impossibilità di procedere ad investigazioni transfrontaliere per l'acquisizione di elementi probatori utili alle indagini disattendendo le regole di ammissibilità delle prove operanti a livello nazionale, pena l'inutilizzabilità delle informazioni raccolte.

Il principio di proporzionalità impone che l'attività da compiere debba essere adeguata e funzionale sia rispetto al suo presupposto (il reato), sia rispetto all'obiettivo che si intende perseguire (le esigenze investigative o probatorie), in modo che la sua esecuzione comporti il minor sacrificio possibile per i diritti e le libertà dell'imputato o dell'indagato (Sez.

6, n. 8320 del 31/01/2019, Creo). La sua applicazione impone di valutare il grado di interferenza e compressione nell'esercizio dei diritti fondamentali coinvolti e le specifiche modalità processuali con le quali sarebbe stato possibile acquisire in Italia i contenuti delle conversazioni.

12.2. Il principio illustrato risulta pienamente salvaguardato nel caso in cui si ritenesse che il provvedimento di acquisizione della prova sia riconducibile al sequestro di corrispondenza.

È stato già evidenziato come anche **questo istituto sia presidiato, in concreto, da garanzie, frutto anche dell'elaborazione della giurisprudenza di legittimità**, specificamente ispirate all'attuazione del principio di proporzionalità e di adeguatezza della misura (testualmente previste solo in tema di disciplina delle misure cautelari personali). I dati sequestrati, in quanto contenuti in un sistema informatico (il "*contenitore*", secondo la terminologia adoperata anche dal Corte Cost., sentenza n. 170 del 2023), vanno selezionati e fatti possibilmente oggetto di una copia clone, con restituzione del dispositivo.

Sul punto, codesta Corte di cassazione, oltre ad affermare che il decreto di sequestro probatorio debba contenere **una specifica motivazione della finalità perseguita per l'accertamento dei fatti** (Sez. U, n. 36072 del 19/04/2018, Botticelli, Rv. 273548), ha ritenuto conforme al principio di proporzionalità e adeguatezza il sequestro a fini probatori di un dispositivo elettronico che conduca, in difetto di specifiche ragioni, alla apprensione di informatici a seguito di una **selezione di essi** e comunque con l'indicazione degli eventuali criteri di selezione (Sez. 6, n. 6623 del 09/12/2020, dep. 2021, Rv. 280838 - 01).

Nel caso di specie, le Procure della Repubblica che hanno condotte le indagini non hanno compiuto una acquisizione all'estero di una prova con modalità "esplorativa" o "indifferenziata".

In entrambi procedimenti oggetto delle ordinanze di rimessione, difatti, sono state acquisite solo **determinate *conversation***, che ruotavano intorno a specifiche utenze, in presenza di sospetti relativi a specifici soggetti (gli odierni indagati nei due procedimenti) che, come si è visto, erano già gravemente indiziati della partecipazione a gravi reati proprio per l'uso di una specifica modalità di comunicazione anti-intercettazione.

L'autorità francese, in data 9 marzo 2021, invero, ha eseguito il sequestro dei server della società *OVH*, su cui il *provider* del servizio *Sky ECC* conservava copia della cronologia delle conversazioni intrattenute, sequestrando il "contenitore" (ALL. 2).

Ai sensi dell'art. 6, § 1, lett. a) della direttiva l'emissione dell'OEI, il giudizio di proporzionalità dell'ingerenza nei diritti della persona sottoposta alle indagini, tuttavia, deve essere condotta "*ai fini del procedimento di cui all'art. 4*" della direttiva, avendo cioè riguardo al procedimento in corso nello Stato di emissione.

Nel caso di specie, come è stato più volte sottolineato, **sono state richieste ed acquisite singole e specifiche comunicazioni e non una massa indifferenziata di dati.**

Il sequestro dei *server*, d'altra parte, compiuto dall'autorità francese, è stato solo **strumentale e, soprattutto, indispensabile in ragione della stessa modalità di comunicazione utilizzata rispetto alla successiva puntuale acquisizione di determinate conversazioni.**

La proporzionalità impone di considerare le specifiche modalità processuali alternative con le quali sarebbe stato possibile acquisire in Italia i contenuti delle conversazioni. Evitando il sequestro dei server, non sarebbe stato possibile acquisire le singole conversazioni più volte indicate.

Nel diritto interno, d'altra parte, come è stato già segnalato, sembra ormai acquisita la consapevolezza che il sequestro probatorio di un dispositivo elettronico comporta una **scansione operativa in più fasi**, rappresentate dal sequestro del dispositivo, dall'estrazione della copia forense e dalla estrapolazione dei dati in concreto rilevanti, che è volta, per gradi, a consentire l'acquisizione dei dati contenuti nel sistema informatico ed, al contempo, ad assicurare la minor invasività dell'operazione a vantaggio della parte interessata (cfr. tra le altre, Sez. 5, n. 21488 del 18/01/2022).

Nella specie, l'Autorità francese ha sequestrato il sistema e ne ha fatto la copia forense; a seguito di puntuale richiesta, ha trasmesso le sole conversazioni utili per le indagini.

12.3. Ritiene questo Ufficio che, eventualmente, anche il riferimento alternativo all'istituto regolato dall'art. 270 cod. proc. pen. assicuri pieno rispetto del principio di proporzionalità.

Nel caso in cui il trasferimento delle conversazioni intercettate nel procedimento penale francese (Stato di esecuzione dell'ordine europeo italiano) fosse ricondotto alla disciplina dell'utilizzazione dei risultati delle intercettazioni in un altro procedimento e, dunque, alla previsione dell'art. 270 cod. proc. pen., opererebbero le specifiche condizioni previste dalla norma: vale a dire, la rilevanza e l'indispensabilità delle captazioni per l'accertamento di delitti per i quali è obbligatorio l'arresto in fragranza di reato.

Si tratta di presupposti che assicurano il bilanciamento tra i diritti individuali e l'interesse all'accertamento dei reati secondo una logica di proporzionalità fondata sulla necessità probatoria e sulla previsione di un catalogo di reati che, per la loro assoluta gravità, giustificano addirittura l'applicazione di una misura cd. "precautelare" come l'arresto in flagranza.

Nel caso di specie, poi, la proporzionalità della misura è stata assicurata in concreto: il trasferimento della prova formata all'estero è stato richiesto in un procedimento relativo a reati che rientrano nel catalogo di cui all'art. 380 cod. proc. pen., la cui dimostrazione discende, per una parte considerevole, proprio dal tenore della corrispondenza intercettata.

Va ribadito, in tale ultima prospettiva, come il pubblico ministero abbia adottato l'ordine di indagine più volte indicato relativamente a prove esistenti in Francia concernenti persone già indagate e già raggiunte da consistenti indizi di traffico illecito di sostanze stupefacenti in grandi quantità, nonché di appartenenza a un gruppo criminale organizzato. Nell'ordinanza del Tribunale di Potenza, in particolare, è illustrata la gravità indiziaria in ordine alla costituzione di una organizzazione già dal 12 aprile 2019, che importava stupefacenti (cfr. pag. 20 dell'ordinanza). Già da questa data "*risultava documentata la presenza di un dispositivo smartphone dotato dell'applicativo criptato Sky-ECC associato al pin E10F7C*" (così pag. 27 dell'ordinanza), dovendo dunque concludersi che una grave ingerenza nei diritti fondamentali di persone sospettate è stata adeguatamente giustificata da un interesse pubblico egualmente importante e pienamente 'bilanciabile'.

12.4. Il principio di proporzionalità previsto per l'OEI stabilisce che i diritti fondamentali (nella specie principalmente quello alla riservatezza) possono essere compressi per ragioni investigative **solo nella misura strettamente necessaria** e lasciandone intatto il nucleo essenziale. Sulla base di quanto illustrato, deve concludersi che l'acquisizione di corrispondenza (nelle condizioni in cui è avvenuta in concreto) abbia rispettato il nucleo essenziale dei diritti fondamentali, essendosi proceduto ad acquisizioni solo nella misura strettamente necessaria.

13. - L'osservanza dei principi fondamentali dell'ordinamento italiano: il rispetto del diritto di difesa e delle regole del "giusto processo".

13.1. Uno dei temi di fondo sotteso all'acquisizione delle *chat* in esame, ed oggetto del secondo motivo di ricorso nel procedimento n. 33544/2023 RG, è rappresentato dalla

verifica del rispetto dei principi fondamentali dello Stato di emissione, dunque, dell'ordinamento italiano, in modo particolare del **diritto di difesa**.

Secondo l'art. 1, § 4, della direttiva 2014/41/UE, infatti, la disciplina introdotta dalla normativa europea "*non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità giudiziarie*".

L'art. 14, § 7, della direttiva, inoltre, sancisce che "[f]*atte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'ordine europeo di indagine*".

Al riguardo, è stato già osservato che, consentendo l'impugnazione dei provvedimenti che si fondano sulle prove ottenute mediante OEI e di dedurre le questioni sulla necessità e regolarità di queste prove, **l'ordinamento garantisce adeguatamente,** ancorché non necessariamente in via preventiva, **il diritto a un ricorso effettivo** sancito dall'art. 47, primo comma, della Carta dei diritti fondamentali dell'Unione europea.

Va poi aggiunto che la violazione dei diritti fondamentali è di difficile verificazione in relazione all'attività giudiziaria di uno Stato membro dell'Unione Europea, tenuto a condividere i principi fondamentali dell'ordinamento europeo, (Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, Rv. 283998; Sez. 1, n. 19082 del 13/01/2023; Costacurta, Rv. 284440, non massimate sul punto).

La presunzione del rispetto di tali principi, nondimeno, potrebbe essere confutata in un caso specifico mediante l'allegazione di specifici e concreti elementi di segno contrario dinanzi al giudice nazionale competente.

Con riferimento alla disciplina dettata dalla direttiva 2014/41/UE, difatti, la giurisprudenza di legittimità ha statuito che l'ordine europeo di indagine c.d. attivo deve avere ad oggetto una prova acquisibile nello Stato di emissione (il cd. principio di equivalenza su cui ci si è soffermati ampiamente), mentre è rimessa allo Stato di esecuzione la concreta assunzione della prova medesima, con le modalità e le garanzie previste in quell'ordinamento, potendosi presumere il rispetto da parte dell'Autorità delegata, nel sistema unionale, della relativa disciplina e dei diritti fondamentali stabiliti dalla CDFUE, nonché del principio di proporzione, **salvo concreta verifica di elementi di segno contrario** (Sez. 6, n. 48330 del 25/10/2022, Borrelli, Rv. 284027 - 01, Sez. 1, n. 19082 del 13/01/2023; Costacurta, Rv. 284440, fattispecie relative all'acquisizione dei codici di decriptazione delle chat di rete *Sky ECC*).

L'utilizzabilità delle prove acquisite o, come nella specie, delle prove già raccolte in uno Stato membro e trasferite in altro Stato in forza di un ordine europeo di indagine, pertanto, è questione rimessa alle scelte legislative dello Stato di emissione.

La questione concernente la violazione dei principi fondamentali, pertanto, può essere proposta dinanzi al giudice nazionale.

13.2. Tanto premesso, ad avviso di questo Ufficio, **le modalità con le quali l'autorità giudiziaria francese ha acquisito i messaggi presenti sulla piattaforma *Sky ECC***, nel caso di specie, **non hanno comportato alcuna violazione dei principi fondamentali e inderogabili dell'ordinamento giuridico italiano**.

13.3. L'acquisizione delle chat, in particolare, non ha determinato alcuna violazione dei diritti della difesa o del giusto processo nella valutazione delle prove acquisite tramite l'ordine europeo di indagine.

L'impossibilità di partecipare alla selezione delle prove trasmesse dall'autorità giudiziaria francese all'autorità italiana è prospettiva infondata, in quanto, come è già stato rilevato, l'acquisizione delle *chat* è avvenuta in conformità alla disciplina processuale francese. Le questioni relative alla raccolta delle prove avrebbero dovuto essere dedotte (solo) innanzi a tale autorità giudiziaria.

13.4. Il diritto di difesa, inoltre, non può essere ritenuto leso per effetto della mancata conoscenza (e, dunque, dell'indisponibilità per la difesa) dell'algoritmo utilizzato per la decriptazione della messaggistica acquisita.

Il difensore dell'indagato, nell'ordinamento italiano, può, infatti, avere conoscenza solo del verbale delle operazioni di cui all'art. 268 cod. proc. pen. e delle registrazioni, ma non anche dei mezzi tecnici, *hardware* e *software*, utilizzati per l'intrusione nelle conversazioni intercettate o per decodificare il contenuto.

Costituisce principio consolidato quello per cui, in tema di intercettazioni di flussi comunicativi, l'indisponibilità dell'algoritmo utilizzabile per la decriptazione dei dati informatici non determina alcuna lesione del diritto di difesa, perché l'interessato può avvalersi della procedura prevista dall'art. 268, commi 6 e 7, cod. proc. pen. per verificare il contenuto delle captazioni, ma non può anche pretendere un controllo diretto mediante l'utilizzo esclusivo e non mediato del programma di decriptazione (Sez. 6, n. 14395 del 27/11/2018 dep. 2019, Testa, Rv. 275534).

L'art. 89 disp. att. cod. proc. pen., come modificato con riferimento all'introduzione dei captatori informatici, d'altra parte, prevede che debba essere indicato nel verbale delle operazioni solo il tipo di programma di intrusione utilizzato, dovendo adoperarsi solo quelli conformi ai requisiti tecnici stabiliti al Ministero della giustizia; non è, invece, previsto che sia reso disponibile il contenuto del programma utilizzato, di norma di proprietà di soggetti privati.

Nell'ordinamento interno la conoscibilità delle eventuali tecniche di hackeraggio, del resto, sarebbe preclusa dal "segreto industriale" del proprietario del *software* utilizzato per l'operazione di intrusione.

In ogni caso, **la violazione dell'art. 268, commi 6 e 7, cod. proc. pen. non rientra tra le cause di inutilizzabilità dell'intercettazione contemplate dall'art. 271 cod. proc. pen.**

Resta ferma la possibilità per la difesa di dedurre, sulla base di ragioni specifiche, **anomalie tecniche in grado di fare dubitare della correttezza delle acquisizioni e dell'inquinamento del risultato probatorio** e, in tal caso, il correlativo obbligo, per l'autorità giudiziaria, di promuovere accertamenti sul punto.

Su questo punto, deve rilevarsi che i singoli utilizzatori dei criptofonini posseggono i messaggi "in chiaro", potendo, pertanto, per esempio producendo le schermate, produrre almeno un *principio* di prova che possa lasciare dubitare della correttezza delle decodificazioni.

Nel caso di specie, come è stato opportunamente rilevato in una delle ordinanze impugnate, le difese si dolgono della mancata acquisizione della documentazione relativa all'estrapolazione dei dati o informatici originali dal server "*senza tuttavia addurre elementi di una qualche consistenza (es. messaggi troncati, incompleti o dissonanti) tali da far dubitare della compromissione del dato, assumendo la censura carattere di genericità*", rivelandosi, pertanto, inidonea a "*superare la presunzione di legittimità della prova trasmessa tramite l'ordine di indagine europeo*" (cfr. pag. 7 dell'ordinanza del Tribunale di Reggio Calabria).

13.5. I dubbi sulla violazione di diritti fondamentali della difesa sono inconsistenti anche se fondati sulla "*suggestione*" di una presunta non ostensibilità di informazioni in ragione di un "*segreto di sicurezza nazionale*" abdotto dallo Stato francese di esecuzione come risulta nella sentenza *Conseil constitutionnel* francese, con la decisione n. 2022-987 QPC dell'8 aprile 2022.

Il suddetto segreto previsto specificamente dalla *lex loci* (art. 230 del codice di procedura penale, nella sua formulazione risultante dalla legge del 13 novembre 2014), non

esclude che la legge francese "*applica per l'acquisizione della messaggistica già trasmessa e conservata nei dispositivi personali regole sostanzialmente corrispondenti a quelle italiane sulle intercettazioni*" sicché, con gli OEI, *"le autorità inquirenti italiane hanno chiesto e ottenuto copie di prove raccolte in un procedimento francese con provvedimento del giudice sotto il suo diretto controllo*" (cfr. Sez. 6 n. 46832 del 26/10/2023, cit.).

La Corte costituzionale francese, del resto, ha affermato che "*se le disposizioni impugnate sono idonee a esonerare dal contraddittorio talune informazioni tecniche soggette al segreto della difesa nazionale, deve restare nel fascicolo processuale l'ordinanza scritta e motivata del giudice che autorizza l'attuazione del procedimento, un dispositivo di cattura e menziona, a pena di nullità, il reato che motiva l'uso di tale dispositivo, l'ubicazione esatta o la descrizione dettagliata dei sistemi automatizzati di trattamento dei dati interessati, nonché la durata durante la quale tale operazione è autorizzata. Nel fascicolo è inserita anche la relazione sull'attuazione del sistema, nella quale sono menzionate in particolare la data e l'ora in cui l'operazione è iniziata e terminata, e quella che descrive o trascrive i dati registrati ritenuti utili per l'evento della verità. Tutti gli elementi ottenuti al termine delle operazioni di chiarimento, infine, formano oggetto di un verbale di ricezione inserito nel fascicolo del procedimento e sono accompagnati da un certificato firmato dal responsabile dell'organismo tecnico attestante la sincerità dei risultati trasmessi*" (così, *Conseil constitutionnel*, n. 2022-987 QPC dell'8 aprile 2022).

La disciplina applicabile, pertanto, sembra sovrapponibile a quella di cui all'art. 89 disp. att. cod. proc. pen. che, nel caso di intercettazioni compiute a mezzo del captatore informatico, impone di indicare nel verbale il tipo di programma impiegato, consentendo l'uso solo di programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia.

13.6. La correttezza dell'algoritmo utilizzato nel caso di specie nell'operazione di decodificazione, del resto, è attestata dalla stessa intellegibilità delle *chat* acquisite.

Secondo l'orientamento giurisprudenziale consolidato, qualora il messaggio telematico sia criptato mediante un impiego di un algoritmo o di una chiave di cifratura e trasformato in un mero dato informatico, l'intelligibilità del messaggio è subordinata all'attività di decriptazione che presuppone la disponibilità dell'algoritmo che consente di trasformare il codice binario in un contenuto dimostrativo.

Ogni messaggio cifrato è inscindibilmente accoppiato alla sua chiave di cifratura.

Pertanto, solo la chiave esatta produrrà una decifratura, necessariamente l'unica possibile e, per ciò stesso, necessariamente quella corretta e necessariamente quella 'integrale'.

È, insomma, una regola informatica su base matematica, abbastanza elementare; o, se si vuole, nel versante della logica classica, è il principio del terzo escluso: o è vera A oppure è vera la sua negazione (non A); non esiste altra possibilità, *tertium non datur*. O il messaggio è decrittato attraverso l'unico codice possibile o rimane una stringa alfanumerica priva di significato, cioè criptata: si deve escludere che si possa decifrarne una parte corretta e una non corretta; né vi sono possibilità che una chiave errata possa decrittare il contenuto, anche parziale, del codice umano contenuto (Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, Rv. 283998, in motivazione, ma anche Sez. 1, n. 6363, Minichino, 13/10/2022, dep. 2023, non massimata).

13.7. L'inutilizzabilità del dato probatorio, inoltre, non può essere desunta dal fatto che non siano stati versati in atti i verbali delle operazioni d'intercettazione ovvero, seguendo la formulazione del secondo motivo di ricorso nel procedimento n. 33544/2023, dal fatto che sono presenti in atti "*i soli esiti dell'attività svolta all'estero e non anche il percorso di acquisizione di quei dati*".

Secondo un consolidato orientamento giurisprudenziale, infatti, l'omesso deposito degli atti concernenti le intercettazioni disposte nel procedimento *a quo* presso l'autorità competente per il procedimento *ad quem* non determina l'inutilizzabilità dei risultati intercettativi, in quanto detta sanzione non è prevista dal citato art. 270 cod. proc. pen. e non rientra tra quelle tassativamente indicate dall'art. 271 cod. proc. pen. (cfr. Sez. 5, n. 4758/16 del 10/07/2015, Bagnato, Rv. 265993; Sez. 5, n. 14783 del 13/03/2009, Badescu, Rv. 243609; Sez. 6, n. 48968 del 24/11/2009, Scafidi, Rv. 245542).

14. - segue: Il rispetto della segretezza delle comunicazioni e della riservatezza della vita privata e le attribuzioni del pubblico ministero italiano.

14.1. L'acquisizione delle chat per mezzo di ordine europeo di indagine, ad avviso di questo Ufficio, non ha determinato alcuna violazione della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione di cui all'art. 15 Cost., né, più in generale, del diritto alla riservatezza ed alla vita privata dei cittadini, né, ancora, della direttiva 58/20027CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Sotto questo aspetto vengono in rilevo diversi temi.

14.2. Va esclusa, in primo luogo, la violazione della riserva di giurisdizione prevista dall'art. 15 Cost. perché l'acquisizione delle chat di cui si controverte è avvenuta, in conformità alla *lex loci*, in forza di una autorizzazione del giudice e sotto il controllo dell'autorità giudiziaria francese.

È stata, dunque, tale autorità giudiziaria a contemperare il diritto alla riservatezza ed alla segretezza di ogni forma di comunicazione privata con la necessità di perseguire reati di particolare allarme sociale, quali il traffico di sostanze stupefacenti internazionale.

L'OEI, in ogni caso, è un provvedimento motivato emesso in base alla legge da una autorità giudiziaria, che ha provveduto alla sola estrapolazione di specifiche conversazioni dalla copia clone dei server sequestrati dall'autorità giudiziaria francese.

14.3. L'inutilizzabilità delle chat acquisite dall'autorità francese, inoltre, non può farsi discendere dall'art. 15, § 1, della direttiva 2002/58, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), così come interpretato dalla Corte di giustizia dell'Unione europea, in particolare, nella sentenza 2 marzo 2021, H.K. c. Prokuratuur. In questa pronuncia la Corte di Giustizia ha statuito che tale disposizione osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.

Sul punto, in una delle decisioni che si sono occupate del tema, è stato affermato che "*l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione debba essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero*" (Sez. 6, n. 44154 del 26/10/2023, Iaria, cit.).

14.4. Nel caso in cui si individuasse nel sequestro di corrispondenza la disciplina che, in un "*caso interno analogo*", avrebbe giustificato l'importazione della prova, **le prescrizioni della direttiva 2002/58/CE**, relativa alla vita privata e alle comunicazioni elettroniche, **sarebbero state rispettate già per effetto dell'intervento del giudice istruttore francese**.

Il sequestro disposto in Francia, in verità, ha riguardato dati personali trattati - nel senso precisato dall'art. 4, par. 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche - dalla società che gestisce il servizio di comunicazione informatica. Questo provvedimento, nondimeno, è stato disposto da un giudice nel pieno rispetto della direttiva relativa alla vita privata.

La direttiva OEI, invece, non prevede che un ordine volto all'acquisizione di prove già in possesso dello Stato di esecuzione, nel quale le ha acquisite un giudice, debba essere emesso necessariamente da un giudice, se, in base alla normativa dello Stato di emissione (nel caso di specie, l'Italia), il mezzo di ricerca della prova che ne costituisce la base (acquisizione di dati personali trattati dalla società che dispone il servizio), avrebbe dovuto essere ordinata dal giudice in un "*caso interno analogo*" (il riferimento sarebbe all'art. 132, comma 3, del d.lgs. 30 giugno 2003, n. 196, Codice della privacy).

La stessa disciplina, inoltre, non stabilisce che il predetto ordine europeo di indagine mirante all'acquisizione di prove raccolte da un giudice debba sempre essere emesso da un giudice dello Stato di emissione (o da un organismo indipendente non coinvolto nelle indagini penali), senza tener conto delle norme nazionali in materia di competenza dello Stato di emissione, qualora la misura riguardi gravi ingerenze in diritti fondamentali di rango elevato, come la riservatezza.

L'art. 27 d.lgs. n. 108 del 2017, che ha recepito la direttiva OEI, non prevede che, nei casi appena indicati, sia necessario l'intervento del giudice.

Le norme del codice di procedura penale che disciplinano il sequestro della corrispondenza non prevedono l'intervento del giudice.

Queste disposizioni non sono suscettibili di interpretazioni adeguatrici, se non altro perché la direttiva OEI non prevede l'intervento del giudice nel caso in cui l'ordine abbia ad oggetto corrispondenza.

Questo Ufficio, peraltro, è consapevole che pende sull'interpretazione dell'espressione "*autorità di emissione*" di cui all'art. 6, par. 1, in combinato disposto con l'art. 2, lett. c), della direttiva OEI un procedimento dinnanzi alla CGUE, ancorché proposto nella prospettiva secondo cui con l'OEI sono state acquisiti i risultati di intercettazioni. La questione, in sostanza, mira a chiarire i rapporti tra l'art. 15 della direttiva 2002/58/UE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche) e le previsioni della direttiva 2014/41/UE sull'OEI, per verificare se sussistano effettivi momenti di sovrapponibilità delle due discipline, **finora mai affermati dalla giurisprudenza europea.**

Fermo restando il diritto a contestare nello Stato membro di emissione la necessità e la regolarità di un OEI sulla base delle regole illustrate, ad avviso di quest'Ufficio, **il ruolo fondamentale del principio del riconoscimento reciproco** nell'ambito della cooperazione giudiziaria europea **esclude che**, **quando l'atto di indagine nello Stato di esecuzione sia stato autorizzato da un giudice**, come è avvenuto nella specie, **non è necessario che l'OEI diretto al trasferimento della prova sia parimenti emesso da un giudice**, anche se, ai sensi del diritto dello Stato di emissione, la raccolta delle prove alla base dell'OEI avrebbe dovuto essere disposta da un giudice.

Qualora l'esito del giudizio pendente dinanzi alla CGUE conducesse all'affermazione secondo cui un OEI, in talune condizioni, debba sempre essere emesso da un giudice (o da un organismo indipendente non coinvolto nelle indagini penali), **senza tener conto delle norme nazionali in materia di competenza dello Stato di emissione e nonostante che la prova, nello Stato di esecuzione, sia stata ammessa da un giudice e assunta sotto il suo controllo**, però, si verificherebbe una situazione non diversa da quella che ha fatto seguito alla CGUE, 2 marzo 2021, H.K. c. Prokuratuur: l'art. 27 del d.lgs. 21 giugno 2017, n. 108, nella parte in cui individua nel pubblico ministero che procede, oltre che nel giudice, l'autorità di emissione "*nell'ambito delle sue attribuzioni*" risulterebbe in contrasto con l'art. 6 della direttiva come eventualmente sarebbe stato interpretato dalla CGUE alla luce della direttiva 2002/58/UE, imponendo al legislatore di intervenire, come è avvenuto per i dati di traffico telefonico con il d.l. 30 settembre 2021, n. 132, convertito nella legge 23 novembre 2021, n. 178 (che ha dettato una norma transitoria, volta specificamente a superare i contrasti interpretativi insorti in ordine all'utilizzabilità dei tabulati telefonici acquisiti dal pubblico ministero in forza della disciplina previgente).

Allo stato, però, trattasi di una ipotesi del tutto virtuale, che questo Ufficio ritiene infondata, in quanto manifestamente contraria al mutuo riconoscimento e basata sull'individuazione di spazi di sovrapposizione tra due distinte direttive, al momento non riconosciuti dalla CGUE: essa, pertanto, non pare possa condurre ad interpretazioni adeguatrici della norma interna o alla disapplicazione delle norme unionali e di quella interna che individuano anche nel pubblico ministero l'autorità di emissione.

Il pubblico ministero italiano, in forza della normativa vigente, è legittimato, ai sensi dell'art. 27, comma 1, del d.lgs. n. 108 del 2017 a emettere, nell'ambito delle proprie attribuzioni nella fase delle indagini preliminari, un OEI volto all'acquisizione di una prova «già disponibile» e a trasmetterlo direttamente all'autorità di esecuzione.

Il pubblico ministero, inoltre, ai sensi dell'art. 253 cod. proc. pen. dispone con decreto motivato il sequestro probatorio delle cose pertinenti al reato necessarie per l'accertamento dei fatti ovvero, ai sensi degli artt. 254 e 254-*bis* cod. proc. pen., il sequestro della corrispondenza anche telematica.

Secondo l'art. 78 disp. att. cod. proc. pen., infine, "*la documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera può essere acquisita a norma dell'art. 238 del codice*".

14.5. Nel caso in cui si individuasse nell'art. 270 cod. proc. pen. la disposizione che, in un caso interno analogo, avrebbe giustificato l'importazione degli esiti di intercettazioni svolte in un diverso procedimento, invece, **il riferimento alla direttiva 2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche non sarebbe pertinente.**

Essa riguarda solo il caso in cui le autorità pubbliche **chiedono l'accesso ai dati trattati dai fornitori di servizi di telecomunicazione**, dovendo ricomprendersi nel concetto di "*trattamento dei dati personali*", di cui all'art. 4, § 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche, in special modo la conservazione di detti dati.

Qualora, invece, **l'intercettazione sia effettuata direttamente dagli Stati membri, con accesso diretto alle utenze con provvedimento mirato, senza che sia imposto alcun obbligo di trattamento dei dati ai fornitori di servizi di telecomunicazione, la direttiva relativa alla vita privata e alle comunicazioni elettroniche non trova applicazione.**

La direttiva 2002/58/CE, infatti, è stata adottata sul presupposto che la disponibilità di una enorme mole di dati conservati dai fornitori di servizi di comunicazione elettronica consente alle autorità pubbliche di "andare indietro nel tempo" e di reperire informazioni utili a scopi di prevenzione, indagine e repressione di minacce alla sicurezza pubblica e nazionale, svolgendo indagini "retrospettive". Per tale ragione, la disciplina europea ha accolto un approccio fortemente attento al rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati, anche a discapito della efficacia degli strumenti posti a garanzia della sicurezza.

Detta direttiva, più in particolare, si è resa necessaria per garantire i diritti fondamentali individuali e per evitare la realizzazione di forme di sorveglianza di massa; in altri termini, la disciplina in esame mira a circoscrivere le informazioni che i privati fornitori

di servizi possono conservare ed il loro uso successivo a scopo di prevenzione, di indagine e di repressione di minacce alla sicurezza pubblica e nazionale. Si tratta di informazioni riguardanti soggetti previamente sconosciuti e non sospettati dalle forze dell'ordine e, dunque, non sottoposti a controlli specifici o intercettazioni dirette da parte dell'Autorità giudiziaria.

Nella specie, non essendo intervenuto alcun accesso ai dati conservati dai fornitori del servizio, la loro acquisizione da parte del pubblico ministero con ordine europeo d'indagine non ha rappresentato alcuna elusione del disposto dell'art. 132 del d.lgs. 30 giugno 2003, n. 196, come di recente riformato dal d.l. 30 settembre 2021, n. 132, convertito nella legge 23 novembre 2021, n. 178, proprio a seguito della sentenza della Corte di Giustizia dapprima citata perché non sussistevano i presupposti perché fosse necessario l'intervento di un giudice.

L'accesso alla corrispondenza nel procedimento penale svoltosi all'estero, d'altra parte, è avvenuto con l'autorizzazione e sotto il controllo di un giudice, nell'ambito di un'indagine penale.

14.6. L'individuazione dell'area operativa della Direttiva 2002/58/CE come appena delineata è conforme all'interpretazione della stessa offerta dalla CGUE.

Secondo un ordine cronologico, vengono in rilievo le seguenti sentenze:

a) CGUE 21 dicembre 2016, C-203/15 e C-698/15, *Tele2 Sverige e Watson*.

La pronuncia ha affermato che l'art. 15, § 1, della Direttiva osta ad una disciplina nazionale che preveda "*una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica», «senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione"*.

La sentenza, dunque, ha affrontato il tema della disciplina della *data retention* da parte delle società fornitrici del servizio e non quello dell'accesso diretto alle conversazioni o alla corrispondenza in forza di provvedimenti dell'autorità;

b) CGUE 2 ottobre 2018, C-207/16, *Ministerio Fiscal*, secondo cui l'art. 15, § 1, della Direttiva "*deve essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi,*

sanciti dai suddetti articoli della Carta dei diritti fondamentali, che non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave".

c) CGUE 6 ottobre 2020, C-511/18, C-512/18, C-520/18, *La Quadrature du Net ed altri*, concernente normative nazionali che impongono ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione generalizzata e indifferenziata dei dati dei loro abbonati e di consentire alle autorità di pubblica sicurezza e di intelligence di accedervi che, all'evidenza, in nessun modo e punto involge la disciplina delle intercettazioni. La Corte europea, infatti, ha espressamente osservato che " … *quando gli Stati membri attuano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di detti servizi di comunicazione, la protezione dei dati delle persone interessate non ricade nell'ambito della direttiva 2002/58, bensì unicamente in quello del diritto nazionale, fatta salva l'applicazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89), di modo che le misure in questione devono rispettare in particolare il diritto nazionale di rango costituzionale e i requisiti della CEDU*" (così § 103).

Nella stessa sentenza è stato aggiunto che rientra nell'ambito di applicazione della direttiva 2002/58 "*una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di conservare dati relativi al traffico e dati relativi all'ubicazione a fini di salvaguardia della sicurezza nazionale e di lotta alla criminalità, quali le normative di cui trattasi nei procedimenti principali*" (§ 104);

d) CGUE 6 ottobre 2020, C-623/17, *Privacy international*, secondo cui "*l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, dev'essere interpretato nel senso che osta ad una normativa nazionale che consente a un'autorità statale di imporre ai fornitori di servizi di comunicazione elettronica, ai fini della salvaguardia della sicurezza nazionale, la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence".* Anche in questo caso, è sufficiente il rinvio alla sentenza per avere contezza del fatto che non coinvolge la disciplina delle intercettazioni;

e) CGUE 2 marzo 2021, C-746/18, *Procuratuur, cit.,* secondo cui l'art. 15, § 1, della direttiva 2002/58/CE "*deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi*

all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo». Inoltre, "*il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento*, [non è] *competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale*".

In definitiva, l'esame delle sentenze rende certo che, in nessun modo e punto, hanno avuto ad oggetto la disciplina delle intercettazioni disposte nel processo penale ad opera dell'autorità dello Stato preposta.

Per dovere di completezza, va osservato che questione posta in tre giudizi è stata altresì quella dell'applicabilità della direttiva alla "*domanda di accesso* [che] rientri *nell'esercizio, da parte delle autorità nazionali, dello ius puniendi*", sollevata sul rilievo che questa "*rientra nell'eccezione prevista* [..] *all'articolo 1, paragrafo 3, della direttiva 2002/58"* (sollevata dalla Spagna nel giudizio deciso dalla sentenza 2 ottobre 2018, C-207/16, *Ministerio Fiscal*), nonché della riferibilità della direttiva alle sole "*norme nazionali relative alla conservazione dei dati"* (secondo un'osservazione svolta dalla Commissione nel giudizio deciso dalla sentenza 21 dicembre 2016, C-203/15 e C-698/15, *Tele2 Sverige e Watson e altri).*

La Corte di giustizia ha ritenuto che "*il citato articolo 15, paragrafo 1, presuppone necessariamente che le misure nazionali da esso contemplate, come quelle relative alla conservazione di dati per finalità di lotta contro la criminalità, rientrino nell'ambito di applicazione di questa medesima direttiva*" (§ 73 della sentenza 21 dicembre 2016, C-203/15 e C-698/15, *Tele2 Sverige e Watson e altri*, con affermazione ripresa dalle due sentenze successive), significativamente facendo tuttavia cadere l'accento tonico sulla "***conservazione dei dati***".

Le sentenze hanno dunque chiaramente ed esclusivamente avuto ad oggetto le discipline interne sulla *data retention*, esaminate alla luce delle norme della direttiva, non quella sulle intercettazioni disposte nel corso di una indagine penale, né comunque quelle che concernono il sequestro dei dati disposto direttamente dall'autorità pubblica.

Le disposizioni del d.lgs. n. 196 del 2003 (codice della *privacy*), che hanno attuato detta direttiva, come modificate dal d.lgs. n. 101 del 2018 (che ha adeguato la nostra normativa alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27

aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali), a loro volta, non si occupano dell'attività di intercettazione disposta nel corso di un processo penale e, *a fortiori*, dei presupposti e dei limiti di applicabilità delle stesse a detta attività.

Le disposizioni di detto codice prevedono una particolare disciplina del trattamento di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado (art. 2-*duodecies*). L'art. 160-*bis* stabilisce che la "*validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali"*, sicché, per l'utilizzabilità della prova in sede giudiziaria, anche se in violazione delle norme in materia di protezione dei dati personali, occorre che la prova sia acquisita lecitamente, e cioè rispettando le regole che presiedono alla formazione della prova all'interno del processo.

Pochi mesi dopo la pronuncia della Corte di giustizia 2 marzo 2021, C-746/18, *Procuratuur*, inoltre, è stato adottato il d.l. 30 settembre 2021, n. 132 (Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP), entrato in vigore il 30 settembre 2021, che, in estrema sintesi, ha subordinato l'acquisizione dei tabulati telefonici e informatici, solo per reati tassativamente indicati e ritenuti gravi dal legislatore, a un previo controllo giurisdizionale sulla richiesta del pubblico ministero (o a una convalida successiva, in caso di acquisizione operate in via di urgenza dal pubblico ministero). La legge 23 novembre 2021, n. 178, in sede di conversione del decreto-legge di cui sopra, oltre ad apportare alcuni correttivi alla disciplina dell'acquisizione, ha dettato una norma transitoria, volta specifica mente a superare i contrasti interpretativi insorti in ordine all'utilizzabilità dei tabulati telefonici acquisiti dal pubblico ministero in forza della disciplina previgente.

Dalla normativa interna adottata a seguito dell'interpretazione della direttiva fornita dalla CGUE si trae una **conferma indiretta** alla considerazione che queste sentenze non concernono le intercettazioni, cioè la captazione di comunicazioni o conversazioni contestualmente al loro svolgersi, una attività compiuta da organi dello Stato, ma i presupposti ed i limiti per l'accesso ai dati personali relativi a comunicazioni elettroniche conservati dai fornitori di servizi di comunicazione elettronica.

14.7. Distinta considerazione merita un'ulteriore sentenza della Corte europea.

Invero, con la sentenza CGUE 16 febbraio 2023, C-349/21, *Spetsializirana prokuratura*, la Corte ha affermato che "*l'articolo 15, paragrafo 1, della direttiva 2002/58/CE* […] *deve essere interpretato nel senso che: esso non osta a una prassi nazionale in forza della quale le decisioni giudiziarie che autorizzano l'utilizzo di tecniche investigative speciali in seguito a una richiesta motivata e circostanziata delle autorità penali sono redatte mediante un testo prestabilito e privo di motivazione specifica, ma che si limita a indicare, oltre alla durata di validità dell'autorizzazione, che i requisiti previsti dalla normativa e menzionati da tali decisioni sono stati rispettati, a condizione che le ragioni precise per le quali il giudice competente ha ritenuto che i requisiti di legge fossero rispettati alla luce degli elementi di fatto e di diritto che caratterizzano il caso oggetto di esame possano essere inferiti agevolmente e senza ambiguità da una lettura incrociata della decisione e della richiesta di autorizzazione, che deve essere resa accessibile, posteriormente all'autorizzazione concessa, alla persona contro cui è stato autorizzato l'utilizzo delle tecniche investigative speciali*".

Questa decisione, che non è immune da difficoltà interpretative, invero, potrebbe condurre alla diversa conclusione dell'applicabilità della direttiva 2002/58/CE anche alle intercettazioni, in virtù di un principio marcatamente innovativo e mai enunciato prima.

Da un canto, è infatti affermato che "*la nozione di trattamento* [stabilita dall'art. 4, paragrafo 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche] *include segnatamente il fatto che detti fornitori concedano l'accesso alle comunicazioni e ai dati o trasmettano questi ultimi alle autorità competenti*» (cfr. § 37 della sentenza).

Dall'altro, è altresì affermato che "*Nel caso di specie, spetta al giudice del rinvio verificare se le tecniche investigative speciali utilizzate nel procedimento principale e, segnatamente, l'intercettazione di cui all'articolo 6 dello ZSRS, hanno avuto l'effetto di imporre simili obblighi di trattamento ai fornitori interessati e, se, quindi, il procedimento principale rientri nell'ambito di applicazione della direttiva 2002/58. Occorre quindi precisare che la Corte risponderà alla prima questione soltanto nei limiti in cui il procedimento principale rientra nell'ambito di applicazione di tale direttiva, segnatamente del suo articolo 15, paragrafo 1"* (§ 38).

Emerge dunque un'evidente incertezza in ordine allo stesso presupposto di applicabilità della direttiva alla fattispecie concreta, che la CGUE non ha sciolto, ma ha rimesso al giudice del rinvio che, in tesi, potrebbe essere dipanato nel senso che l'intercettazione, in quanto non riconducibile ad un caso di *data rendition*, non configura un trattamento nei sensi della Direttiva 2002/58/CE.

In ogni caso, anche ad accedere all'interpretazione che sembra accolta dalla sentenza secondo cui "*la nozione di trattamento* [che rileva ai fini della applicazione della Direttiva

2002/58/CE] *include segnatamente il fatto che detti fornitori concedano l'accesso alle comunicazioni e ai dati o trasmettano questi ultimi alle autorità competenti*", deve rilevarsi che, nel caso di specie, **non vi è stata alcuna messa a disposizione dei dati conservati da parte della società che gestiva il servizio di comunicazione elettronica**, ma **un'attività investigativa "ostile", posta in essere dallo Stato, autonomamente, per mezzo di sofisticati programmi informatici che hanno compiuto una intercettazione**.

Fin dal primo provvedimento autorizzativo del giudice istruttore di Lille del 14 giugno 2029 risulta che "*Le autorità belghe hanno anche specificato che SKYECC non ha collaborato con le forze di sicurezza, dopo aver ottenuto un mandato dal giudice*".

14.8. Risulta pertanto legittimo che, con OEI emesso dal pubblico ministero, siano acquisiti gli esiti di intercettazioni svolte all'estero e che l'autorità di emissione di un simile ordine non sia il giudice, né che il giudice intervenga successivamente a 'convalidare' l'OEI emesso dal pubblico ministero, allorquando la prova sia stata raccolta, nello Stato di esecuzione, attraverso l'intervento di un giudice.

Quando gli Stati membri attuano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di detti servizi di comunicazione, la protezione dei dati delle persone interessate non ricade nell'ambito della direttiva 2002/58/CE.

L'intervento del giudice è imposto dalla direttiva 2002/58/CE nel caso di accesso ai dati conservati dai gestori dei servizi di comunicazione e non quando si tratta di ottenere risultati di intercettazioni già autorizzate nello Stato di esecuzione da un giudice.

15. - Gli orientamenti delle altre Autorità giudiziarie europee.

A conclusione della lunga illustrazione, infine, giova rilevare che, come è stato rilevato in una delle decisioni della Corte di cassazione che si è occupata dalle questioni (Sez. 6, n. 48838 del 11/10/2023, Brunello, pag. 4), anche altre Autorità giudiziarie dell'Unione Europea hanno esaminato il tema relativo alle modalità di acquisizione e ai limiti di utilizzabilità delle comunicazioni ottenute "violando" le piattaforme di comunicazioni criptate (come *Encrochat* e *Sky-Ecc*), successivamente trasferite in altri Stati membri mediante ordine europeo di indagine.

Le soluzioni accolte sono tutte favorevoli all'utilizzo processuale delle prove acquisite secondo le modalità illustrate. E' stato rilevato, in particolare, che "il *Conseil constitutionnel* francese, con la decisione n. 2022-987 QPC dell'8 aprile 2022, ha statuito che la disciplina

francese, sulla cui base è stata disposta l'acquisizione delle chat e l'intercettazione delle comunicazioni operate nel presente procedimento, è conforme alla Costituzione francese; il *Bundesgerictshof*, con la sentenza 5 StR 457/21 del 2 marzo 2022, ha ritenuto che l'intercettazione della piattaforma *Encrochat*, "violata" dall'autorità giudiziaria francese, fosse legittima ai sensi del diritto processuale penale tedesco; […] la Corte Suprema dei Paesi Bassi (*Floge Raad*), con la sentenza n. 913 del 13 giugno 2023, ha ritenuto conforme al diritto interno l'acquisizione dei dati informatici presenti sulle piattaforme criptate *Encrochat* e *Sky Ecc*, acquisite dall'autorità giudiziaria francese".

Risulterebbe davvero singolare che, mentre i più alti consessi giurisdizionali del Paesi dell'Unione riconoscono la piena legittimità dello strumento di collaborazione investigativo (e, con esso, la presunzione di legittimità degli atti acquisitivi posti in essere, in ragione di collaudate garanzie riconosciute ai reciproci ordinamenti), si prospettasse un'inspiegabile *enclave* di eccezione da parte dello Stato italiano, in nulla giustificata, secondo quanto ci si è sforzati di dimostrare. L'effetto, in punto di affidabilità del principio di collaborazione giudiziaria tra gli Stati, risulterebbe disastroso ed assai marginalizzante, in futuro, per il nostro Paese: soprattutto, se privo di qualsivoglia effettiva giustificazione e, dunque, incomprensibile a livello unionale.

Tutti gli ulteriori profili inerenti ai vari motivi di ricorso prospettati nei due procedimenti dalle impugnazioni proposte in questa sede dai signori Avvocati difensori saranno esaminati nel corso della discussione all'udienza del 29 febbraio 2024 ed in quella sede saranno naturalmente rassegnate le relative conclusioni.

Roma, 12 febbraio 2024.

IL SOSTITUTO PROCURATORE GENERALE

Luigi Giordano

L'AVVOCATO GENERALE

Pietro Gaeta