47798-23

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

TERZA SEZIONE PENALE

SU

Composta da

Ord. n. 1123 sez.

CC- 03/11/2023

R.G.N.33544/2023

ha pronunciato la seguente

ORDINANZA

DEPOSITATA IN CANCELLERIA

IN 30 NOV 2023

IL FUNZIONARIO GIUDIZIARIO

Luana Mariani

RITENUTO IN FATTO

1. Con ordinanza del 29 giugno 2023, il Tribunale di Potenza Sezione del riesame rigettava l'istanza proposta nell'interesse di Gjuzi Ermal avverso la ordinanza applicativa della misura della custodia in carcere emessa dal Gip del tribunale di Potenza in data 12.6.2023, in relazione ad ipotesi di reato riguardanti le fattispecie di cui agli artt. 73 e 74 del dPR n. 309/90 del 1990.

2. Avverso la suindicata ordinanza Gjuzi Ermal, tramite i difensori di fiducia, ha proposto ricorso per cassazione, sollevando tre motivi di impugnazione.

3. Deduce, con il primo, il vizio *ex* art. 606, lett. c) cod. proc. pen. in relazione agli artt. 234-*bis* e 191 cod. proc. pen.; premesso, infatti, che i dati informatici presenti sul *server* della *Sky Global* e relativi a conversazioni già intercorse mediante lo strumento di *Sky-Ecc* integrerebbero documenti informatici, si osserva che, tuttavia, la relativa acquisizione non sarebbe riconducibile nell'ambito della fattispecie di cui all'art. 234-*bis* cod. proc. pen. Ciò in quanto i dati informatici in questione, ottenuti dalla Autorità giudiziaria quali dati conservati all'estero presso l'Autorità giudiziaria francese, non sarebbero stati acquisiti, così come consentito dalla suindicata disposizione (che contempla anche l'ulteriore caso di acquisizione di dati "disponibili al pubblico"), direttamente presso un privato avente sede in altro Stato e con il suo consenso, senza attivazione di alcuna rogatoria, bensì sarebbero stati acquisiti 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. Inoltre, si deduce comunque la violazione dell'art. 234-*bis* cod. pen., ove ritenuto applicabile, perché il giudice, con riguardo a dati informatici presenti sui server della *Sky-Global* e relativi a conversazioni intercorse mediante lo strumento di *Sky-Ecc*, non avrebbe verificato la modalità di acquisizione dei predetti dati conservati all'estero e, in particolare, non avrebbe accertato la manifestazione del "consenso del legittimo titolare" degli stessi, come previsto dal predetto articolo. Manifestazione insussistente, posto che non sarebbe riconducibile al Pubblico ministero francese la figura del legittimo titolare dei dati di cui alla citata norma, con conseguente inutilizzabilità del dato probatorio.

4. Con il secondo motivo deduce la violazione di norme processuali ex art. 606, comma 1, lett. c), cod. proc. pen., in relazione all'art. 191 cod. proc. pen. e in relazione agli artt. 27 Cost. e 6 della CEDU, con inutilizzabilità dei dati acquisiti mediante *Sky-Ecc*. Si evidenzia che con motivo aggiunto si era rappresentato al Tribunale la circostanza per cui, qualificando le chat come prova documentale, si determinava l'effetto di mettere a disposizione delle parti e di sottoporre alla valutazione eventuale del Tribunale del riesame, solo la fase terminale del processo di acquisizione della prova, articolato nella acquisizione prima e nella decifratura poi, del contenuto dei messaggi ottenuti inizialmente dall'autorità estera in forma criptata, in assenza di elementi per poter verificare il profilo afferente alla formazione dei dati prelevati,. Il tutto in funzione della verifica della legittimità delle risultanze finali. Pertanto, per la legittima utilizzazione di una prova assunta da un'Autorità straniera, quale quella in esame, sarebbe stata

necessaria la messa a disposizione dell'intero compendio investigativo, in particolare dei *files* delle *chat* criptate. In tale prospettiva, sarebbe illegittima l'intervenuta valutazione, da parte del tribunale del riesame, di superfluità della conoscenza di tali circostanze, prodromiche alla acquisizione finale della prova (con particolare riferimento alla conoscenza anche dei *files* originari e della chiave di decifratura ovvero dell'algoritmo di riferimento); valutazione di superfluità assunta in base al rilievo per cui l'utilizzo di un algoritmo non conforme avrebbe condotto alla elaborazione di espressioni prive di senso, la quale, come tale, avrebbe impedito, di fatto, la verifica delle modalità di acquisizione del dato, con violazione del diritto di difesa.

5. Con il terzo motivo, il ricorrente deduce vizi ex art. 606, comma 1, lett. b) ed e), cod. proc. pen., per erronea applicazione dell'art. 273, comma 1, cod. proc. pen., e per manifesta illogicità della motivazione in punto di ritenuta sussistenza dei reati contestati all'indagato. Si contesta l'intervenuta valutazione del ricorrente quale partecipe all'associazione di cui all'art. 74 del dPR n. 309 del 1990. Nel valorizzare gli elementi indiziari che suffragherebbero tale ricostruzione, il Tribunale non avrebbe illustrato i dati investigativi da cui dovrebbe desumersi la presenza del ricorrente al momento della consegna di danaro all'agente sotto copertura, in data 19 giugno 2019, né avrebbe indicato le ragioni per cui ha desunto la ritenuta provenienza illecita della somma e la consapevolezza, in capo al ricorrente, delle circostanze afferenti alla predetta transazione e riportate a pagina 125 della ordinanza impugnata. Al riguardo, da una parte, si osserva che il contenuto della conversazione 14, pur citato dal Tribunale per spiegare le suddette sue considerazioni, sarebbe equivoco, e dall'altra, si aggiunge che sarebbe illogico il ragionamento del Tribunale laddove desume la consapevolezza, da parte dell'indagato, delle circostanze inerenti la citata transazione, dalla fotografia riproducente il numero seriale di una banconota ottenuta dal ricorrente quale prova della ricezione del danaro poi da lui consegnato. Ciò in quanto quest'ultima circostanza, la ricezione della banconota, integrerebbe un fatto solo asserito ma mai provato.

Quanto alla valorizzazione, sempre ai fini di qualificare il ricorrente quale partecipe, della presenza dell'indagato al sopralluogo notturno del 30 marzo 2023, il Tribunale avrebbe fatto ricorso ad argomentazioni congetturali.

Si aggiunge, poi, che le conversazioni intercorse tra altri non potrebbero essere valorizzate per sostenere la consapevolezza, da parte del ricorrente, della presenza di sostanza stupefacente nella sua azienda. Sarebbe inoltre manifestamente illogica la tesi del Tribunale, per cui lo stupefacente non rinvenuto presso l'azienda del ricorrente sarebbe stato spostato, atteso che non si rinvengono plausibili elementi a supporto di tale ultima considerazione.

6. Con il quarto motivo, propone, ai sensi dell'art. 267 del Trattato sul funzionamento dell'Unione Europea (TFUE), una questione pregiudiziale da sollevare innanzi alla Corte di Giustizia Europea.

Si premette che, attenendo la vicenda in esame ad attività delle *Law enforcement Agencies* dirette "alla violazione della piattaforma criptata al fine di ottenere dati elettronici conservati nei *server* della società *Sky Global*", non verrebbe in rilievo, in questa sede, un'attività di intercettazione bensì di acquisizione di informazioni o di prove, già in possesso dell'autorità di esecuzione dell'O.E.I. emesso dall'Autorità giudiziaria italiana, per ottenere tali dati dalle autorità francesi. Le quali li avevano acquisiti non come flussi di comunicazioni in atto.

Si osserva, quindi, che il tema proposto non riguarderebbe l'inquadramento giuridico dell'attività richiesta con l'O.E.I., ma quello del rispetto delle garanzie previste a tutela della persona sottoposta ad indagini o imputata, nel quadro della procedura di cui all'O.E.I.

In tale quadro, dopo avere evidenziato, tra l'altro, che l'autorità di emissione dell'O.E.I. deve garantire il rispetto dei diritti della persona indagata o imputata (art. 6 par. 1 e 2 TUE) e certificare che l'O.E.I. è proporzionato e necessario e che nell'emetterlo si è tenuto conto dei diritti della persona, il ricorrente rileva che con l'O.E.I. ora in questione si sarebbe richiesta l'acquisizione di dati elettronici relativi al traffico, alla ubicazione e al contenuto di comunicazioni, per cui rappresenta che occorre distinguere tra dati elettronici non di contenuto (inerenti al traffico e all'ubicazione della comunicazione) e dati relativi al contenuto della stessa.

In proposito, si richiama la disciplina europea dei dati elettronici e in particolare la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, con specifico riguardo all'art. 15, paragrafo 1, della stessa, quanto ai limiti normativi sull'accesso a tali dati elettronici. Si rappresenta, inoltre, che ai sensi degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea, l'ingerenza nei diritti fondamentali riportati in tali norme, derivante dall'accesso, da parte della pubblica autorità, ad un insieme di dati inerenti il traffico e l'ubicazione e suscettibili di fornire notizie sulle comunicazione di un utente di un mezzo di comunicazione elettronica, presenta un carattere grave, ove l'insieme di essi consenta di trarre precise conclusioni sulla vita privata della persona o delle persone interessate, come evincibile da decisioni della Corte di Giustizia (Corte di Giustizia, Grande Camera, sentenza del 2 marzo 2021, *H.K. – Prokuratuur Conditions d'accèss aux données relatives aux communications èlectroniques*, C-746/18, ECLI:EU:C:2021:152, punto 39).

Quindi, dopo avere sottolineato che solo gli obiettivi della lotta contro forme gravi di criminalità e di prevenzione di gravi minacce per la sicurezza pubblica

possono giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o alla ubicazione di un utente di un mezzo di comunicazione elettronica o riguardanti l'ubicazione di apparecchiature terminali utilizzate dallo stesso, tali da permettere di trarre precise conclusioni sulla vita privata delle persone interessate (Corte di Giustizia, Grande Camera, sentenza del 2 marzo 2021, *H.K. – Prokuratuur Conditions d'accèss aux donnèes relatives aux communications èlectroniques*, C-746/18, ECLI:EU:C:2021:152, punto 35), si rappresenta che, nel caso in esame, l'attività di acquisizione di dati avviata dal Pubblico ministero italiano, basatasi sulla disciplina interna, sarebbe lesiva dei diritti fondamentali e della proporzionalità. Laddove, ove invece fosse considerata proporzionata e legittima, si darebbe luogo ad un'incorenza interna del sistema: in un caso "interno", l'acquisizione dei dati di traffico e di ubicazione sarebbe possibile solo in caso di sussistenza del presupposto del grave reato (ai sensi dell'art. 132 del dlgs. n. 196 del 2003) mentre, nel caso di acquisizione dei medesimi mediante O.E.I., essa sarebbe sempre possibile, non ostando la stessa intrinseca natura del dato elettronico richiesto.

Consegue alfine, la rappresentazione del seguente quesito 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".*

Analoghe osservazioni e analogo quesito sono formulati con riguardo alla acquisizione di dati relativi al contenuto di comunicazioni informatiche.

Si rappresenta, poi, un ulteriore punto critico: quale la verifica della legittimazione del Pubblico ministero a richiedere, mediante O.E.I., l'accesso ai dati relativi al traffico e ai dati relativi alla ubicazione come anche ai dati di contenuto, ai fini di una istruttoria penale, senza una previa autorizzazione del

giudice, posto che si tratterebbe di parte nel processo, priva del requisito di indipendenza e imparzialità, da richiedersi alla autorità incaricata di un controllo preventivo in ordine all'accesso ai dati in questione.

Si osserva, infine, come si tratti di questioni pertinenti e rilevanti.

E si evidenzia, altresì, che il diritto nazionale deve assicurare che elementi di prova ottenuti in modo illegittimo non arrechino pregiudizio all'imputato, con conseguente rappresentazione del seguente ulteriore quesito da sottoporre alla Corte di Giustizia: *"se il divieto di utilizzo degli elementi investigativi o di prova possa derivare direttamente dal principio di effettività sancito dal diritto dell'Unione nel caso di elementi investigativi o prove ottenute tramite un OEI contrario a detto diritto.*

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".

CONSIDERATO IN DIRITTO

1. Il collegio osserva che il ricorso deve essere rimesso alle Sezioni Unite, in quanto - ai sensi dell'art. 618 comma 1 cod. proc. pen. - può emergere un contrasto giurisprudenziale in ordine alle seguenti questioni:

a) Se in tema di mezzi di prova l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante O.E.I., presso A.G. straniera che ne ha eseguito la decrittazione, costituisca acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-*bis* cod. proc. pen. a mente del quale "è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare" o di documenti ex art. 234 cod. proc. pen. o sia riconducibile in 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.

2. Va premesso che l'ordinanza impugnata, del Tribunale di Potenza Sezione del riesame, è stata emessa nel contesto dello svolgimento di indagini preliminari volte a disarticolare un'organizzazione criminale adusa all'utilizzo della criptofonia, nell'ambito di attività relative al traffico internazionale di sostanze stupefacenti provenienti dall'Albania. Le indagini scaturivano dal coinvolgimento di alcuni dei

soggetti indagati in attività investigative avviate dalla Procura Distrettuale della Repubblica di Trento nell'ambito di un contesto di riciclaggio internazionale, divenute successivamente oggetto di apposito coordinamento della Procura Nazionale Antimafia e Antiterrorismo.

Con particolare riferimento all'utilizzo di criptofonia, risulta, dalla ordinanza cautelare genetica del Gip del Tribunale di Potenza e dalla stessa ordinanza impugnata, che taluni indagati facevano uso di "criptofonini anti-intercettazione", da intendersi quali dispositivi *smartphone* che usano metodi di crittografia capace di proteggere i sistemi di comunicazione, solitamente basati, secondo l'ordinanza, sullo stesso *hardware* del telefonini normali, ma con l'aggiunta di sistemi di cifratura superiori al normali dispositivi *Android* o *Apple*. I criptofonini utilizzano un *hardware standard*, in genere *Android, Black Berry* o *IPhone*, ma rispetto ai normali telefonini ospitano un *software* capace di contenere un sistema operativo dedicato, avente particolari requisiti di sicurezza, in quanto disabilita servizi di localizzazione (GPS, *Bluetooth,* fotocamera, scheda SD e porta USB). Le chiamate rimangono attive ma solo in modalità *Voice over* IP (VoiP), non appoggiandosi alla rete GSM ed impiegano applicazioni *proprietarie e criptate* (*Encrochat, Sky ECC, Anom, no1bc*, etc.) che utilizzano reti diverse dalla normale rete telefonica, e che sono crittografate ad una cifratura a più livelli.

Vengono in rilievo in questo contesto ed in sintesi, per quanto qui di interesse, quali strumenti di comunicazione, *chat* del tipo *peer-to-peer* che non sono salvate su un *server* pubblico. I *backup* delle comunicazioni vengono invece salvati sul dispositivo criptato e su di un *server* dedicato messo a disposizione degli utenti dall'azienda che fornisce il servizio.

Anche la SIM utilizzata è particolare e dedicata, connettendosi esclusivamente alla rete di *server* predisposta dal fornitore del servizio.

In tal modo i criptofonini sarebbero al sicuro da intercettazioni.

Come prima accennato, telefoni di questo tipo necessitano di una infrastruttura di *server* messi a disposizione dalla compagnia che li produce, con relativo abbonamento.

Quanto alla piattaforma *Sky-ECC*, pure qui di interesse, lo sforzo congiunto della polizia francese, belga ed olandese, coordinati da EUROPOL, ha permesso a quegli organismi di introdursi nella rete criptata *Sky-ECC* avendo accesso alle comunicazioni di soggetti dediti ad attività illecite.

In particolare, il 9 marzo 2021 la polizia belga dava esecuzione ad una maxi operazione su base internazionale, così rendendo pubblica l'avvenuta violazione del sistema criptato *Sky-ECC*.

Di fatto, l'operazione ha permesso di decrittare i contenuti delle *chat* scambiate dai criminali, avendo accesso ai flussi di informazioni di oltre 70.000 utenti, che la Cooperazione internazionale guidata da EUROPOL ha permesso di

rendere disponibili in favore di autorità giudiziarie comunitarie, tramite Eurojust e l'emissione di appositi O.E.I.

Nel procedimento in esame, il materiale indiziario è costituito anche da messaggi scambiati con il sistema cifrato *Sky-Ecc* utilizzato dagli indagati.

3. Quanto alla acquisizione dei suddetti dati, emerge dalle citate ordinanze che i predetti messaggi, per quanto ora interessa, sono stati richiesti all'Autorità Giudiziaria francese con O.E.I. emessi dalla Procura della Repubblica italiana e l'operazione di decriptazione è stata eseguita mediante l'individuazione del necessario algoritmo utilizzato dalla società proprietaria del sistema di cifratura *Sky-Ecc* come sopra anticipato.

L'ordinanza impugnata, nel respingere la tesi difensiva della assenza di autorizzazione del Gip alla effettuazione di intercettazioni con violazione dell'art. 266 e ss. cod. proc. pen., ha sottolineato la natura documentale e non captativa delle chat in questione richiamando in tal senso conforme giurisprudenza di legittimità, nè è contestato dal ricorrente, come evidenziato nei precedenti paragrafi (il quale peraltro, sia pure confermando le proprie critiche, a pagina 35 del ricorso rileva come "il dato sia stato fornito dal Tribunale di Parigi e nell'acquisizione sia intervenuta una autorità giurisdizionale"), che si tratti di acquisizione di messaggi costituenti dati "freddi" ovvero estranei, nella loro acquisizione, ad un flusso di comunicazioni in corso.

Viene, a questo punto, in rilievo la necessità di stabilire se l'acquisizione, mediante O.E.I., di messaggi su *chat* di gruppo presso Autorità Giudiziaria straniera che ne abbia già eseguito la decrittazione costituisca acquisizione o meno di "documenti e di dati informatici" ai sensi innanzitutto dell'art. 234-*bis* cod. proc. pen.

In senso positivo risultano numerose sentenze di questa suprema Corte (tra le tante, sez. 4, n. 37503 del 30/05/2023 n.m.; sez. IV del 16/05/2023 n. 38002/23 n.m; 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. 15/02/2023) Rv. 283998 - 01;) formulate nel quadro dei seguenti principi.

In particolare, la tesi della acquisibilità delle *chat* in parola ai sensi dell'art. 234-*bis* cod. pen. muove dalla distinzione, con particolare riferimento per quanto qui di interesse a comunicazioni criptate, tra intercettazioni da una parte e acquisizione e decifrazione di dati comunicativi dall'altra.

In proposito, si distingue tra operazioni di captazione e di registrazione del messaggio cifrato nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario, e le operazioni di acquisizione del contenuto del messaggio già inoltrato oltre che di decriptazione dello stesso, necessarie per trasformare mere stringhe informatiche in dati comunicativi intellegibili.

Solo alla prima delle due suindicate tipologie di operazioni fa riferimento l'art. 266-*bis* cod. proc. pen., che estende l'applicabilità delle norme del codice di rito relative alle 'normali' intercettazioni di conversazioni o comunicazioni tra soggetti a distanza, alle intercettazioni di flussi di comunicazioni relativi a sistemi telematici ovvero intercorrenti tra più sistemi telematici: flussi che non avvengono in via diretta tra apparecchi informatici, ma che sfruttano la trasmissione dei dati in via telematica, dunque via cavo o ponti radio, ovvero per mezzo di altra analoga strumentazione tecnica (cfr. in motivazione, Sez. 6 - n. 18907 del 20/04/2021 Rv. 281819 - 01; nel medesimo senso quanto all'acquisizione dei contenuti di messaggistica in atto, effettuata con sistema *Blackberry*, cfr. Sez. 4, n. 49896 del 15/10/2019, Rv. 277949-01; Sez. 3, n. 47557 del 26/09/2019, Rv. 277990-01, 02; Sez. 3, n. 50452 del 10/11/2015, Rv. 265615-01).

Quando, invece, il messaggio telematico sia acquisito allorquando non sia più all'interno di un flusso in corso di comunicazioni, e sia stato criptato - come è appunto accaduto nel caso di specie –, va esclusa la disciplina delle intercettazioni, destinata ad operare solo con riferimento a flussi di comunicazioni in atto (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) e gli inquirenti ne possono valorizzare il contenuto a fini dimostrativi, laddove abbiano la disponibilità dell'algoritmo che consente di decriptarne il tenore ovvero se tale 'chiave' venga altrimenti messa a disposizione degli investigatori dalla società che ne è proprietaria. Si è anche precisato (con riguardo al caso analogo di messaggi "*whatsapp*" e *sms* conservati nella memoria di un telefono cellulare) che i messaggi in parola integrano mera documentazione di detti flussi (in tale ultimo senso, tra le altre, cfr. Sez. 6 - n. 1822 del 12/11/2019 (dep. 17/01/2020) Rv. 278124 – 01; Sez. 5, n. 1822 del 21/11/2017 (dep. 16/01/2018) Rv. 272319 - 01) 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, Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Rv. 283998, in motivazione, e anche Sez. 1, n. 6363, n.m., in pari data).

Si tratta quindi, in altri termini, di attività non rientrante propriamente nella nozione di operazioni di intercettazioni, perché non riguardante la captazione e la registrazione di dati comunicativi *in itinere* dal mittente al destinatario.

In questa prospettiva, si è anche osservato che 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 "flussi di comunicazioni"). Osservandosi, in sostanza, che ciò che rileva è che i flussi di comunicazione non fossero più in corso al momento in cui sono stati chiesti i dati e (a maggior ragione) quando quei dati furono trasmessi dalla Autorità che li aveva acquisiti. Per cui, in tal caso, la situazione non sarebbe dissimile da quella che si verifica quando viene acquisito *ex post* un flusso di comunicazioni, scritte o per immagini, memorizzato sulla memoria di un apparecchio telefonico (Sez. IV del 16/05/2023 n. 38002/23 n.m. cit.).

In conclusione, quindi, la suddetta natura delle *chat* in esame, quali dati o documenti informatici di tipo comunicativo, distinti dal flusso di comunicazioni informatiche o telematiche in atto, cui soltanto è riconducibile la disciplina delle intercettazioni ai sensi dell'art. 266-*bis* cod. proc. pen., consentirebbe, secondo gli indirizzi di legittimità sopra variamente citati, l'acquisizione delle medesime, ove già acquisite e conservate da Autorità Giudiziaria estera, mediante O.E.I. attivato dal Pubblico ministero.

Ciò nel presupposto della individuazione dell'art. 234-*bis* cod. proc. pen. (introdotto dall'art. 2, comma *1-bis*, del dl. n. 7 del 2015, convertito, con modificazioni, nella legge n. 43 del 2015) quale norma interna di riferimento, alla stregua della quale verificare l'esistenza del potere di procedere con l'Ordine Europeo di Indagine, posto che quest'ultimo può avere ad oggetto solo atti d'indagine richiesti che "avrebbero potuto essere emessi in un caso interno analogo", secondo la direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014.

Tale norma, è stato precisato, troverebbe applicazione in quanto 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» (tra le altre, in particolare, Sez. 1 - n. 6364 del 13/10/2022 (dep. 15/02/2023) Rv. 283998 – 01 cit.).

4. Il portato della suesposta impostazione, che assume immediata rilevanza per la seconda questione indicata in premessa, volta a verificare se l'acquisizione in esame 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 del giudice nazionale, consiste nella affermazione della piena legittimità dell'ottenimento dei documenti informatici in parola, attraverso un atto, l'O.E.I., attivato dal Pubblico ministero, senza necessità di ulteriori verifiche giurisdizionali interne anteriori e tantomeno posteriori, rispetto alla citata acquisizione.

In proposito, e nel quadro di una doverosa sintesi (cfr. per tutte, sul tema, Sez. 1 - n. 6364 del 13/10/2022 (dep. 15/02/2023) Rv. 283998 – 01) rispetto alle

numerose pronunce rinvenibili al riguardo, si deve premettere che l'Ordine europeo d'indagine è 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.

L'Ordine europeo d'indagine, per quanto qui di interesse, "può anche essere emesso per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione" (art. 1, punto 1 della direttiva suindicata). Inoltre, secondo gli artt. 6 e 9 della direttiva citata, l'O.E.I. può avere ad oggetto, come sopra già riportato, solo atti d'indagine richiesti che "avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo" e l'autorità di esecuzione riconosce l'O.E.I., "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".

Consegue, alla luce di tali principi, la ricostruzione giurisprudenziale per cui, da una parte, nel caso in esame si tratta non di una richiesta di procedere ad intercettazioni, ma di una richiesta di acquisizione degli esiti documentali di attività d'indagine precedentemente svolta, rispetto alla quale l'ordinamento interno rinviene la piena ed esclusiva competenza del P.M.; organo peraltro competente nella fase di indagine, salve specifiche eccezioni, quali la richiesta di effettuazione di intercettazioni all'estero (art. 43 del dlgs. n. 108 del 2017), all'emissione dello stesso O.E.I.

Per cui la competenza esclusiva del P.M. nell'effettuare, nell'ordinamento interno, l'acquisizione in parola, trova riflesso anche nella analoga richiesta rivolta all'estero mediante O.E.I.

Inoltre, l'utilizzazione degli atti trasmessi a seguito di attività di cooperazione internazionale non è condizionata da un accertamento svolto ad opera del giudice italiano concernente la regolarità delle modalità di acquisizione esperite dall'Autorità straniera, 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). In altri termini, l'O.E.I. oltre a dover avere ad oggetto una prova acquisibile nello Stato di emissione, 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, quindi, 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.

Secondo la tesi in esame, si tratta di una richiesta di acquisizione degli esiti documentali di attività d'indagine che l'Autorità straniera ha già svolto, nella sua piena autonomia, nel rispetto della sua legislazione in relazione ad altri reati; pertanto la tutela giurisdizionale relativa a tali atti non può che trovare spazio in tale altro ordinamento.

Né, si è osservato (cfr. Sez. 1 - n. 6364 del 13/10/2022 (dep. 15/02/2023) Rv. 283998 - 01 cit.), trova pregio l'argomento inerente un'asserita incompatibilità delle *chat* così acquisite con il diritto interno, nella misura in cui si faccia riferimento alla 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 dello Stato italiano in materia di acquisizione di tabulati introdotta con il d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178. Ciò in ragione innanzitutto (e ancor prima della eventuale verifica dell'intervento, in ogni caso, all'estero, dell'Autorità Giudiziaria ai fini della acquisizione dei dati in parola), del rilievo per cui ciò che viene acquisito, nel quadro in esame, sono documenti informatici e non "dati esteriori" (il riferimento è ai tabulati, dei quali le Sezioni Unite n. 21 del 13/07/1998, Gallieri, Rv. 211196 - 01, hanno offerto una utile definizione, precisando che "essi costituiscono la documentazione in forma intellegibile del flusso informatico relativo ai dati esterni al contenuto delle conversazioni").

E' su queste basi, così sintetizzate, che si esclude dunque, secondo un diffuso orientamento di legittimità, che l'acquisizione in esame debba essere oggetto, ai fini della utilizzabilità dei dati versati in atti, di preventiva o successiva verifica della sua legittimità da parte del giudice nazionale.

5. Per esigenze di completezza, occorre aggiungere che corollari della suesposta tesi della acquisibilità, nel quadro dell'art. 234-*bis* cod. proc. pen., di messaggi su *chat* di gruppo presso Autorità Giudiziaria straniera che ne abbia eseguito la decrittazione sono inoltre, in sintesi, anche i seguenti principi, variamente rinvenibili nelle decisioni di legittimità sopra citate e in parte già sopra accennati. Si tratta:

- della legittimità del ricorso, per chiedere la trasmissione di documentazione già acquisita dall'Autorità Giudiziaria estera, ad un O.E.I. emesso dal PM nazionale;

- della rinvenibilità del consenso all'acquisizione dei dati, da parte del "legittimo titolare" di quei documenti conservati all'estero, come previsto dall'art. 234 bis cod. proc. pen., nell'assenso che proviene dal soggetto che di quei documenti o di quei dati poteva disporre: da intendersi come persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del Paese estero, identificabile non soltanto nella persona fisica e\o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria, nell'autorità giudiziaria, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'*internet service provider* (in motivazione sez. 1 - n. 6364 del 13/10/2022 Rv. 283998 - 01 cit.);

- dell'esclusione, salvo allegazione di specifici e concreti elementi di segno contrario, della ricorrenza 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. 02/04/2019) Rv. 275534 - 01)

- dell'affidamento della garanzia del rispetto dei diritti fondamentali, nell'ambito del procedimento di cui all'O.E.I., in primo luogo allo Stato membro di emissione, che si deve presumere rispetti il diritto dell'Unione.

6. Rispetto alla complessiva tesi suesposta, sono intervenute di recente due sentenze della Sezione VI di questa Corte, che risultano aprire orientamenti dissenzienti rispetto alle suesposte soluzioni rivenute in ordine alle due questioni sottoposte all'esame di codeste Sezioni Unite.

7. Con sentenza n. 44154 del 26/10/2023 (dep. 02/11/2023) Rv. 285284 - 01, si è innanzitutto evidenziata la peculiarità del caso esaminato dalla suprema Corte, caratterizzato dal fatto che, nel provvedimento gravato, non era stato chiarito se rispetto al momento della emissione e della trasmissione degli O.E.I., le investigazioni compiute dall'Autorità Giudiziaria francese fossero state tutte definitivamente concluse, oppure se fossero proseguite anche sulla base delle richieste formulate dall'Autorità Giurisdizionale italiana; cosicchè si è precisato - senza che tale prospettiva, a fronte di un caso di riferimento che pare peculiare e

diverso, appaia, per vero, in contrasto con l'orientamento in precedenza esposto riguardo alla prima questione deferita a codeste Sezioni Unite – che la disposizione dettata dall'art. 234-*bis* cod. proc. pen. è inapplicabile 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. Aggiungendosi, altresì, che una siffatta attività acquisitiva va piuttosto inquadrata nelle disposizioni dettate in materia di perquisizione e sequestri, in specie nella norma dettata dall'art. 254-*bis* del codice di rito, riguardante le ipotesi di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni.

E', tuttavia opportuno, in ogni caso evidenziare, costituendo essa un punto nodale di contrasto, la premessa delle suesposte conclusioni, secondo la quale 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 portato all'odierna attenzione di questa Corte, di contro, risulta in maniera sufficientemente chiara che quella acquisita è stata documentazione di attività di indagine della autorità straniera". Si tratta di un'affermazione che, nella misura in cui debba interpretarsi nel senso di delimitare la predetta fattispecie ex art. 234-*bis* cod. proc. pen. alla sola acquisizione di dati informatici in ogni caso estranei, nella loro formazione, a qualsivoglia coinvolgimento di autorità investigative, appare entrare in contrasto con il diffuso e diverso indirizzo sopra esposto, secondo cui ciò che invece importa, per la rilevanza della norma citata, è che i flussi di comunicazione non fossero più in corso al momento in cui sono stati chiesti i dati e (a maggior ragione) quando quei dati furono trasmessi.

Di interesse è anche l'ulteriore notazione, siccome rilevante in ordine alla seconda questione qui sollevata, con cui, evidenziandosi l'incidenza, sulla normativa nazionale per l'acquisizione presso il *server* dei dati esterni alle telecomunicazioni, di arresti della Corte di giustizia dell'Unione europea (in particolare Corte di Giustizia, Grande Camera, del 2 marzo 2021 H.K., C-746/18), questa Suprema Corte ha sottolineato l'intervenuta adozione in via d'urgenza (decreto-legge n. 132 del 2021) delle novelle disposizioni inserite nell'art. 132 Cod. *privacy* (così come risultanti dalla legge di conversione n. 178 del 2021), mediante le quali il legislatore ha "giurisdizionalizzato" nel procedimento penale la procedura di acquisizione dei dati esterni di traffico telefonico e telematico (che richiede ora un provvedimento autorizzatorio motivato del giudice). Così da concludere, 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". Tanto si sostiene anche alla luce della illustrata valenza della posizione assunta dalla Corte costituzionale in ordine all'estensione applicativa delle garanzie previste dall'art. 15 Cost., in materia di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (Corte cost., sent. n. 170 del 2023), 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, § 72; Corte EDU, sent. 3/04/2007, Copland c. Regno Unito, § 41), gli SMS (Corte EDU, sent. 17/12/2020, Saber c. Norvegia, § 48) e la messaggistica istantanea inviata e ricevuta tramite internet (Corte EDU, sent. Barbulescu, cit., § 74). Si tratta di affermazione, va precisato, che al di là del riferimento ad una attività investigativa che pare diversa (per quanto sopra già sottolineato) da quelle considerate dalla duplice tesi in precedenza illustrata, tanto da delineare, piuttosto, 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. Tanto più che disponendosi l'annullamento con rinvio della ordinanza impugnata si ribadisce tra l'altro, la necessità, per il giudice del rinvio, di "verificare, ai fini della utilizzabilità dei dati informativi acquisiti, concernenti comunicazioni nella fase "statica", se sussistevano le condizioni originarie per l'autorizzabilità in sede giurisdizionale delle relative attività investigative oggetto degli ordini europei".

Quanto alla seconda sentenza della sesta sezione di questa Corte, n. 44155 del 26/10/2023 (dep. 02/11/2023) Rv. 285284 - 01, essa sembra ripercorrere l'impostazione della precedente, pur in assenza di espliciti riferimenti, anche solo di natura dubitativa, come avvenuto con la precedente decisione, al contenuto della ordinanza allora impugnata quanto alla concreta attività svoltasi all'estero a seguito di O.E.I. del Pubblico ministero italiano.

8. Pare anche opportuno aggiungere, per completezza informativa, che successivamente alla decisione di questa suprema Corte di rimettere il presente ricorso alle Sezioni Unite e nelle more della redazione della presente ordinanza sono state depositate due sentenze della VI Sezione penale (sez. 6 n. 46482 del 27.09.2023 dep. 17.11.2023 n.m.; sez. 6 n. 46833 del 26.10.2023 dep.

21.11.2023 n.m.). In particolare, con sentenza n. 46833 del 26.10.2023 la VI Sezione, nel condividere l'impostazione di fondo di cui all'indirizzo illustrato nei paragrafi 3 e 4 precedenti, secondo il quale va esclusa l'applicabilità della disciplina sulle intercettazioni *ex* art. 266 e ss. cod. proc. pen., a fronte di O.E.I. avente ad oggetto la richiesta, all'Autorità Giudiziaria straniera, di specifici «dati freddi», cioè documenti costituenti l'esito delle comunicazioni memorizzate su server, già acquisiti e decriptati dai giudici stranieri, in un loro procedimento autonomamente avviato e concluso (secondo una procedura peraltro garantita, nello specifico caso esaminato), ha elaborato una prospettazione ulteriore, rispetto a quelle sinora illustrate quanto alla individuazione dell'art. 234-*bis* cod. proc. pen., quale norma interna di riferimento per il caso in esame. Si è infatti sostenuto, pur sul rilievo per cui, alla luce della sentenza della Corte Costituzionale n. 170 del 2023 sopra già citata, anche la messaggistica informatica conservata dopo la ricezione, costituisce e mantiene il suo carattere di corrispondenza (dovendosi ritenere permanere, secondo la Consulta, come noto, 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"), che la corrispondenza, anche informatica, rientra nel fuoco dell'art. 234 cod. proc. pen. Con esclusione, quindi, del riferimento all'art. 234-*bis* cod. proc. pen., in quanto tale disposizione non sarebbe conferente perché, nella specie, si ha riguardo ai risultati di un'attività investigativa concretizzatasi nell' acquisizione di documenti di altro procedimento penale, svoltosi all'estero, attraverso una forma di collaborazione internazionale. Laddove, invece, l'art. 234-*bis* cod. proc. pen. è stato introdotto nel 2015 e specifica ulteriormente l'art. 32 della Convenzione di Budapest sul *cybercrime*, già vigente nell'ordinamento in forza della legge di ratifica n. 48 del 2008, consentendo in ogni caso 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.

In pratica, la Convenzione avrebbe introdotto la possibilità di acquisire la documentazione esistente in rete senza dover fare ricorso al sistema delle rogatorie internazionali o ad altri strumenti di cooperazione giudiziaria internazionale.

Tale disposizione, che mira a rendere agevole l'acquisizione della documentazione reperibile via *internet*, non sarebbe rilevante secondo la citata sentenza, allorquando le prove documentali digitali siano state formalmente consegnate dall'Autorità giudiziaria straniera, come nel caso in esame. Con l'ulteriore rilievo per cui, comunque, stabilire se l'acquisizione sia stata disposta ai

sensi dell'una o dell'altra disposizione, riguarda profili meramente definitori, in concreto irrilevanti.

Con l'altra citata sentenza (n. 46482 del 27.09.2023 dep. 17.11.2023) la Sezione VI ha condiviso il punto suesposto rilevando che, secondo quest'impostazione, l'art. 234-*bis* cod. proc. pen. nulla aggiunge ai fini dell'accesso alla documentazione con i comuni mezzi (come il sequestro o la consegna diretta) e certamente il riferimento al "legittimo titolare" non significa che le legittime modalità di acquisizione delle prove siano condizionate dall'autorizzazione del "proprietario" del documento.

Oltre a concludere, pur nello sviluppo di una più articolata analisi delle possibili norme interne di riferimento per la problematica qui in esame, nel senso per cui anche nella relazione tra Stati, cui si applica la disciplina O.E.I., quando la prova sia già stata acquisita con atto del giudice nel paese di esecuzione, il semplice trasferimento della prova preesistente nel procedimento in Italia, come da regole interne, può essere disposto sulla base della sola richiesta del Pubblico ministero.

9. Si ritiene, pertanto, tenuto conto delle diverse impostazioni giurisprudenziali riferite che sussista, dunque, una duplice questione di diritto che pare idonea a dare luogo ad un contrasto giurisprudenziale che, ai sensi dell'art. 618, comma 1, cod. proc. pen., considerata anche la particolare rilevanza della questione, come dimostrato dalla non esigua messe di pronunce, non sempre uniformemente orientate, che si sono succedute in breve tempo sulla materia, giustifica la rimessione del ricorso alle Sezioni Unite di questa Corte, invitate, pertanto, a decidere sulle seguenti questioni:

a) Se in tema di mezzi di prova la acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante O.E.I., presso A.G. 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. o sia riconducibile in 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.

P.Q.M.

Rimette il ricorso alle Sezioni Unite.

Così deciso, il 03/11/2023

Il Consigliere estensore
Giuseppe Noviello

Il Presidente
Andrea Gentili