23755-24

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

SEZIONI UNITE PENALI

Composta da

Margherita Cassano	- Presidente -	Sent. n. sez. 3
Maria Vessichelli		CC - 29/02/2024
Francesco Maria Ciampi		R.G.N. 33544/2023
Gastone Andreazza		
Giovanna Verga		
Filippo Casa		
Ercole Aprile		
Angelo Caputo		
Antonio Corbo	- Relatore -	

ha pronunciato la seguente

SENTENZA

sul ricorso proposto da
Gjuzi Ermal, nato in Albania il 28/05/1991

avverso l'ordinanza del 29/06/2023 del Tribunale di Potenza

visti gli atti, il provvedimento impugnato e il ricorso;
udita la relazione svolta dal componente Antonio Corbo;
udito il Pubblico Ministero, in persona del Sostituto procuratore generale Luigi Giordano, che ha concluso chiedendo il rigetto del ricorso;
uditi, per il ricorrente, gli Avvocati Donatello Cimadomo e Vincenzo Antonio Rago, che hanno concluso chiedendo l'accoglimento del ricorso.

RITENUTO IN FATTO

Con ordinanza emessa in data 29 giugno 2023, il Tribunale di Potenza ha rigettato l'istanza di riesame proposta nell'interesse di Ermal Gjuzi avverso l'ordinanza del G.i.p. del Tribunale di Potenza che aveva applicato allo stesso la misura cautelare della custodia in carcere per il reato di cui all'art. 74 d.P.R. n. 309 del 1990.

Secondo l'ordinanza impugnata, sussisterebbero gravi indizi di colpevolezza a carico di Ermal Gjuzi in ordine alla sua partecipazione, dal dicembre 2019, e con condotta tuttora perdurante, ad un'associazione per delinquere finalizzata al traffico di eroina, cocaina, marijuana e hashish diretta da Marsel Hajri e da Gerti Hajri. Ai fini dell'individuazione dei gravi indizi di colpevolezza, l'ordinanza impugnata ha richiamato anche elementi costituiti da comunicazioni intercorse sulla rete criptata Sky-Ecc, acquisiti mediante Ordine Europeo di Indagine (c.d. o.e.i.) eseguito dall'autorità giudiziaria della Repubblica di Francia.

2. Ha presentato ricorso per cassazione avverso l'ordinanza indicata in epigrafe Ermal Gjuzi, con un atto sottoscritto dagli avvocati Vincenzo Antonio Rago e Donatello Cimadomo, articolando quattro motivi.

2.1. Con il primo motivo, si denuncia violazione di legge, con riferimento agli artt. 234-*bis* e 191 cod. proc. pen., a norma dell'art. 606, comma 1, lett. *c)*, cod. proc. pen., avendo riguardo alla ritenuta applicabilità della disciplina di cui all'art. 234-*bis* cod. proc. pen. ai dati informatici relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, gestito dalla società Sky Global.

Si premette che l'acquisizione dei dati informatici relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc non è qualificabile come attività di intercettazione, in quanto attiene a dati già in possesso dell'autorità di esecuzione dell'ordine europeo di indagine (d'ora in avanti o.e.i.), l'autorità giudiziaria francese.

Si osserva che, però, questa circostanza non implica l'applicabilità della disciplina di cui all'art. 234-*bis* cod. proc. pen.

Si rileva, a tal proposito, che la disposizione appena citata si riferisce a dati disponibili al pubblico o comunque acquisiti previo consenso del legittimo titolare, conformemente a quanto prevede l'art. 32, lett. *b)*, della Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001, e, quindi, ad acquisizioni compiute al di fuori di forme di collaborazione tra autorità giudiziarie di Stati diversi. Si precisa che legittimo titolare dei dati non è anche l'autorità giudiziaria la quale li abbia pur regolarmente acquisiti, in quanto gli Stati aderenti alla Convenzione del 23 novembre 2001 hanno convenuto, con una nota di

orientamento, che la disciplina di cui all'art. 32, lett. *b)*, è da limitare ai soli casi in cui il proprietario dell'*account* dia un consenso libero e volontario.

Si conclude che, non essendo l'autorità giudiziaria francese legittimo titolare dei dati trasmessi, il dato probatorio sarebbe inutilizzabile.

2.2. Con il secondo motivo, si denuncia violazione di legge, con riferimento agli artt. 191 cod. proc. pen., 27 Cost. e 6 CEDU, a norma dell'art. 606, comma 1, lett. *c)*, cod. proc. pen., avendo riguardo alla ritenuta utilizzabilità dei dati informatici relativi alle comunicazioni intercorse attraverso il sistema Sky-Ecc.

Si deduce che la qualificazione dei dati informatici rappresentativi delle comunicazioni in questione come prova documentale impedisce qualunque controllo sulla legittimità del processo di formazione della prova. Si evidenzia che, nella specie, la qualificazione giuridica criticata ha consentito l'acquisizione del contenuto delle conversazioni criptate intercorse attraverso il sistema Sky-Ecc non mediante i relativi *files*, ma a mezzo di una consulenza tecnica avente ad oggetto la decifratura delle stesse. Si aggiunge che la mancata conoscibilità dei *file* rappresentativi delle comunicazioni, nonché delle relative chiavi di decifrazione impedisce qualunque valutazione in ordine alla modalità di acquisizione del dato utilizzato e, quindi, l'esercizio del diritto di difesa (si cita Sez. 4, n. 32915 del 15/07/2022, Lori, non mass.).

2.3. Con il terzo motivo, si denuncia violazione di legge, con riferimento all'art. 273, comma 1, cod. proc. pen., nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *b)* ed *e)*, cod. proc. pen., avendo riguardo alla ritenuta sussistenza dei gravi indizi di colpevolezza.

Si deduce che illegittimamente l'ordinanza impugnata ha ritenuto la sussistenza dei gravi indizi di colpevolezza in ordine alla partecipazione del ricorrente all'associazione finalizzata al narcotraffico diretta da Marsel Hajri e da Gerti Hajri. Si premette che gli elementi valorizzati dal Tribunale sono costituiti: a) dalla presenza del ricorrente al momento della consegna del denaro contante, per la somma di 150.000,00 euro, all'agente sotto copertura il 19 giugno 2020; b) dalla presenza del ricorrente al "sopralluogo" notturno nella sua azienda agricola il 30 marzo 2023; c) dalle conversazioni scambiate da altri mediante il sistema Sky-Ecc tra il 3 ed il 13 aprile 2020 e tra il 6 e l'8 agosto 2020. Si osserva, in primo luogo, che la presenza del ricorrente al momento della consegna del denaro all'agente sotto copertura è un dato equivoco, in quanto non vi sono elementi evidenzianti la sua consapevolezza in ordine alla illiceità della provenienza del denaro o della sua destinazione: le conversazioni utilizzate dal Tribunale a tal fine sono intercorse fra terzi, e non è provata nemmeno l'attribuibilità al ricorrente della materiale consegna all'agente sotto copertura della banconota usata come ricevuta. Si rileva, inoltre, che la presenza del ricorrente al "sopralluogo" notturno nella sua azienda agricola non può ritenersi indicativa della partecipazione ad

un'attività diretta ad organizzarsi per reagire all'arresto di un preteso sodale, in quanto manca qualunque elemento utile per supportare tale conclusione. Si osserva, in terzo luogo, che le conversazioni intercorse tra altri non sono indicative né della presenza di droga nell'azienda agricola del ricorrente – anche perché in tale luogo non è stata mai trovata sostanza stupefacente –, né, a maggior ragione, dell'eventuale consapevolezza del medesimo in ordine a tale circostanza.

2.4. Con il quarto motivo, si solleva questione pregiudiziale *ex* art. 267 T.F.U.E. ai fini dell'interpretazione della Direttiva 2014/41/UE relativa all'o.e.i.

2.4.1. Si premette che la questione è rilevante, perché attiene alla disciplina applicabile all'acquisizione ed utilizzabilità di elementi costituenti la base probatoria dell'ordinanza impugnata, ed è seria, anche perché la Direttiva 2014/41/UE non è mai stata oggetto di interpretazione della Corte di giustizia UE.

2.4.2. Si evidenziano, poi, alcuni dati normativi e giurisprudenziali la cui considerazione è necessaria ai fini dell'esame della questione sollevata.

In particolare, si rappresenta che: a) l'autorità di emissione di un ordine europeo di indagine deve garantire il rispetto dei diritti della persona indagata o imputata e dei principi di necessità e di proporzionalità delle misure richieste, a norma dell'art. 6, paragrafi 1 e 2, Direttiva 2014/41/UE; b) il termine di riferimento per verificare il rispetto dei diritti e dei principi appena indicati, nella specie, è costituito dalla natura dei dati richiesti, attinenti al traffico, all'ubicazione ed al contenuto di comunicazioni elettroniche; c) i dati relativi al traffico di comunicazioni e all'ubicazione degli interlocutori, siccome utili a permettere precise conclusioni sulla vita privata delle persone interessate, sono ritenuti dalla consolidata giurisprudenza della Corte di giustizia UE accessibili solo per fronteggiare gravi forme di criminalità o per prevenire gravi minacce per la sicurezza pubblica (si citano: Corte giustizia, 02/10/2018, Ministerio Fiscal, C-207/16; Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-746/18; Corte giustizia, Grande Sezione, 06/10/2020, La Quadrature du Net, C-511/18, C-512/19 e 520/18); d) anche nell'ordinamento italiano, a norma dell'art. 132 d.lgs. 30 giugno 2003, n. 196, l'acquisizione di dati di traffico e di ubicazione è possibile solo in presenza del presupposto di un grave reato; e) l'o.e.i. è ammesso solo in reazione ad atti di indagine che avrebbero potuto essere disposti alle stesse condizioni in un caso interno analogo, e non può certo prevedere uno *standard* di tutela meno elevato; f) l'accesso ai dati relativi al traffico ed al contenuto di comunicazioni elettroniche, secondo la giurisprudenza della Corte di giustizia UE, è consentito solo in caso di un preventivo controllo del giudice o di un'autorità amministrativa indipendente, mentre non è sufficiente il solo provvedimento del pubblico ministero (si cita, specificamente, Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-746/18); g) i dati relativi al contenuto di comunicazioni elettroniche, come testo, voce, video, immagini o

suono, non possono avere minore tutela di quella assicurata ai dati di traffico e di ubicazione, perché aventi natura ancora più sensibile; h) il giudice dello Stato di esecuzione può procedere ad un mero controllo formale sugli elementi posti a base della emissione dell'o.e.i.; i) il principio di effettività del diritto euro-unitario, secondo la giurisprudenza della Corte di giustizia UE, impone di evitare indebiti pregiudizi ad un indagato o imputati in conseguenza dell'utilizzo di informazioni ed elementi di prova ottenuti in modo illegittimo (si citano: Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-746/18; Corte giustizia, Grande Sezione, 20/09/2022, VD e SR, C-339/20 e C-397/20).

2.4.3. Si conclude chiedendo alla Corte di cassazione, per il caso di mancato annullamento dell'ordinanza impugnata, di formulare alla Corte di giustizia UE i quesiti così sintetizzati:

a) 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, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'acquisizione di dati elettronici relativi al traffico, all'ubicazione o al contenuto di comunicazioni già in possesso della autorità di esecuzione, o comunque contenuti in basi di dati della polizia o delle autorità giudiziarie, 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;

b) 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, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'acquisizione di dati elettronici relativi al traffico, all'ubicazione o al contenuto di comunicazioni già in possesso della autorità di esecuzione, o comunque contenuti in basi di dati della polizia o delle autorità giudiziarie, senza che tale accesso sia previamente autorizzato da un giudice o da un'altra entità incaricata;

c) se, nel caso di elementi investigativi o di prova ottenuti tramite un o.e.i. contrario al diritto dell'Unione Europea, il principio di effettività sancito da tale ordinamento giuridico determini il divieto di utilizzo di tali elementi investigativi o di prova o comunque conseguenze a favore dell'imputato quantomeno sul piano della valutazione delle prove e della determinazione della pena.

3. Con ordinanza del 3 novembre 2023, la Terza Sezione penale della Corte di cassazione, cui era stato assegnato il ricorso, ha rimesso lo stesso alle Sezioni Unite ai sensi dell'art. 618, comma 1, cod. proc. pen., rilevando l'esistenza di due

questioni di diritto idonee a dare luogo ad un contrasto giurisprudenziale, anche per la pluralità degli orientamenti giurisprudenziali emersi in proposito.

Le questioni sono le seguenti:

a) se l'acquisizione di messaggi su *chat* di gruppo scambiati con sistema cifrato attraverso un ordine europeo di indagine rivolto ad un'autorità giudiziaria straniera che ne abbia 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.

3.1. L'ordinanza di rimessione premette alcune indicazioni generali sulle comunicazioni mediante "criptofonini".

Rappresenta, innanzitutto, che i criptofonini sono dispositivi *smartphone* che utilizzano un *hardware standard*, in genere *Android*, *BlackBerry* o *IPhone*, al quale è abbinato un *software* contenente un sistema operativo dedicato, il quale disabilita i servizi di localizzazione (GPS, *Bluetooth*, fotocamera, scheda SD e porta USB). Precisa, poi, che, per effetto dell'attivazione del *software* in questione, le chiamate rimangono attive solo in modalità *Voice over IP* (VoIP), perché non si appoggiano alla rete GSM ed impiegano applicazioni proprietarie e criptate (ad esempio: *Encrochat*, Sky-ECC, Anom, no1bc), le quali utilizzano reti diverse dalla normale rete telefonica e sono crittografate ad una cifratura a più livelli. Segnala, ancora, che le comunicazioni intercorse a mezzo dei criptofonini non sono salvate su un *server* pubblico: i *backup* delle stesse vengono salvati sul dispositivo criptato e su di un *server* dedicato messo a disposizione degli utenti dalla compagnia che fornisce il servizio. Evidenzia, quindi, che anche la S.I.M. da utilizzare per attivare il *software* in questione è particolare e dedicata, in quanto si connette esclusivamente alla rete di *server* predisposta dal fornitore del servizio.

3.2. L'ordinanza di rimessione, poi, espone che, secondo un orientamento, seguito da numerose decisioni (si citano: Sez. 4, n. 37503 del 30/05/2023, Iannaci, non mass.; Sez. 4, n. 38002 del 16/05/2023, Zambara, non mass.; Sez. 4, n. 16345 del 05/04/2023, Liguori, non mass.; Sez. 4, n. 16347 del 05/04/2023, Papalia, Rv. 284563 - 01; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, Rv. 283998 - 01), le conversazioni intercorse sui criptofonini ed ottenute dall'autorità giudiziaria francese mediante o.e.i. sarebbero acquisibili a norma dell'art. 234-*bis* cod. proc. pen.

Secondo questo orientamento, occorre distinguere tra le operazioni di intercettazione, le quali si riferiscono alla captazione del messaggio cifrato mentre è in transito dall'apparecchio del mittente a quello del destinatario, come tali

sussumibili nella disciplina di cui all'art. 266-*bis* cod. proc. pen., e le operazioni di acquisizione di un messaggio già inoltrato, le quali hanno ad oggetto una «rappresentazione comunicativa incorporata in una base materiale con un metodo digitale», come tali sussumibili nella disciplina di cui all'art. 234-*bis* cod. proc. pen.

Alcune delle decisioni dell'orientamento in esame precisano che, nella prospettiva dell'ordinamento italiano che riceve tali rappresentazioni comunicative, sono da considerare "dati freddi" e non "flussi di comunicazioni" anche i dati acquisiti dall'autorità giudiziaria straniera in tempo reale, se i flussi di comunicazione non erano più in corso nel momento in cui i relativi dati sono stati chiesti o sono stati trasmessi di iniziativa da parte dell'autorità giudiziaria straniera (così Sez. 4, n. 38002 del 16/05/2023, Zambara, non mass.).

Ad avviso dell'orientamento in esame, poi, l'o.e.i. relativo all'acquisizione di comunicazioni già inoltrate, in quanto avente ad oggetto la richiesta non di procedere ad intercettazioni, bensì di ricevere esiti documentali di attività di indagine precedentemente svolta, può essere presentato dal pubblico ministero. Ancora, secondo questo indirizzo: a) spetta al giudice straniero la verifica della correttezza della procedura di acquisizione della prova e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate in tale fase; b) la necessità dell'autorizzazione del giudice non è imposta nemmeno dalla disciplina prevista per l'acquisizione di tabulati di conversazioni dall'art. 132 del codice *privacy*, come introdotto dal d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178, perché, nella specie, oggetto dell'acquisizione sono documenti informatici e non "dati esteriori" (per questo rilievo, v. Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, Rv. 283998-01); c) il legittimo titolare che può disporre dei documenti conservati all'estero, a norma dell'art. 234-*bis* cod. proc. pen., è anche l'autorità giudiziaria straniera, in quanto li abbia già acquisiti al momento della richiesta mediante o.e.i. e li detenga in forza di un titolo legittimo; d) non è necessario acquisire l'algoritmo per decrittare i messaggi, in quanto, secondo la scienza informatica, ove la chiave di decrittazione non fosse corretta, sarebbe impossibile ottenere un testo avente un significato intelligibile.

3.3. L'ordinanza di rimessione, a questo punto, rappresenta che, secondo altro orientamento, seguito in particolare da due decisioni (Sez. 6, n. 44154 del 26/10/2023, Iaria, Rv. 285284 – 01, 02, 03, e Sez. 6, n. 44155 del 26/10/2023, Kolgjokaj, Rv. 285362 – 01, 02), in relazione ai risultati di una attività acquisitiva che si sia concretizzata in una apprensione occulta o nel sequestro di dati archiviati in un *server* o presenti in altri supporti informatici, è applicabile non la disposizione di cui all'art. 234-*bis* cod. proc. pen., ma la disciplina in materia di perquisizione e sequestro, e, in particolare, quella di cui all'art. 254-*bis* cod. proc. pen.

Secondo questo diverso orientamento, la disciplina di cui all'art. 234-*bis* cod. proc. pen. è applicabile esclusivamente nell'ipotesi di documenti e dati informatici

preesistenti all'avvio delle indagini o comunque formati fuori delle investigazioni. Inoltre, l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza richiede sempre un provvedimento del giudice, sia perché nella disciplina italiana ed euro-unitaria per l'acquisizione dei tabulati telefonici è necessaria un'autorizzazione del giudice (si richiamano l'art. 132 del codice *privacy* e Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-746/18) sia perché le garanzie a tutela della libertà e segretezza della corrispondenza, come precisato dalla giurisprudenza costituzionale (si cita Corte cost., sent. n. 170 del 2023) e dalla giurisprudenza della Corte EDU, si estendono anche ai messaggi di posta elettronica, o comunque inviati via *internet*, e già ricevuti dal destinatario.

3.4. L'ordinanza di rimessione, quindi, osserva che un ulteriore orientamento, espresso da altre due pronunce (Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, Rv. 285543 - 01, 02, 03, e Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363 - 01, 02, 03, 04), con riguardo ai c.d. "dati freddi" richiesti ed ottenuti tramite o.e.i., ritiene applicabile la disciplina di cui all'art. 234 cod. proc. pen.

Questo ulteriore indirizzo osserva, in via preliminare, che l'art. 234-*bis* cod. proc. pen. non è riferibile all'acquisizione di atti mediante o.e.i., perché la sua genesi si ravvisa nell'art. 32 della Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001 (ratificata con legge n. 48 del 2008), il quale ha riferimento a documentazione accessibile senza ricorso alle procedure di collaborazione con lo Stato in cui i documenti sono collocati. Le indicate decisioni, peraltro, non prospettano ricadute operative differenti da quelle indicate dall'orientamento che fa riferimento all'applicazione della disciplina di cui all'art. 234-*bis* cod. proc. pen., almeno con riguardo all'ammissibilità del trasferimento della prova in Italia sulla base della sola richiesta del pubblico ministero e senza preventiva autorizzazione del giudice.

4. Con decreto del 13 dicembre 2023, la Prima Presidente ha assegnato il ricorso alle Sezioni Unite, a norma degli artt. 610, comma 3, e 618, comma 1, cod. proc. pen., e ne ha disposto la trattazione all'odierna camera di consiglio.

Con istanza trasmessa il 19 dicembre 2023 l'Avvocato Donatello Cimadomo, quale difensore del ricorrente, ha chiesto di poter discutere oralmente la causa.

Con provvedimento adottato il 24 gennaio 2024 la Prima Presidente ha disposto in conformità.

5. In data 31 gennaio 2024, i difensori del ricorrente hanno presentato motivi nuovi, connessi al quarto ed al primo motivo del ricorso.

5.1. Il motivo nuovo connesso al quarto motivo del ricorso approfondisce i temi della necessità, in relazione all'istituto dell'o.e.i., della verifica della sussistenza dei presupposti per l'adozione della misura di acquisizione della prova

in un caso interno analogo, e della necessità, nel caso di specie, di una preventiva autorizzazione del giudice ai fini dell'emissione dell'o.e.i. da parte del pubblico ministero.

Si osserva, innanzitutto, che la necessità, in relazione all'istituto dell'o.e.i., della preventiva verifica della sussistenza, in concreto, dei presupposti per l'adozione della misura di acquisizione della prova in un caso interno analogo da parte dell'autorità giudiziaria dello Stato di emissione discende dalla disciplina della Direttiva 2014/41/UE, in particolare dall'art. 6, paragrafo 1, e dall'art. 10, paragrafo 2, ed ha trovato una recentissima e puntuale conferma nella giurisprudenza euro-unitaria (si citano Corte giustizia, Grande Sezione, 21/12/2023, G.K., C-281/22, e Corte giustizia, 16/12/2021, Spetsializirana prokuratura, C-724/19). Si aggiunge che questa conclusione vale ancor di più nel caso di o.e.i. relativo a prove già in possesso dell'autorità giudiziaria dello Stato di esecuzione, dato il limitatissimo potere di controllo alla stessa attribuito in tale ipotesi dall'art. 11, paragrafo 2, Direttiva 2014/41/UE.

Si evidenzia, quindi, che il tipo di controllo preventivo necessario e l'individuazione dell'autorità competente sono correlati al tipo di atto da compiere.

Si rappresenta che, nel caso di specie, deve escludersi che l'o.e.i. attenga ad una richiesta di intercettazione, perché lo stesso, come si evince dall'esame del suo contenuto (in particolare dalla sezione C dell'atto), ha ad oggetto informazioni o prove già in possesso dell'autorità di esecuzione, e, precisamente, dati elettronici relativi a comunicazioni, già acquisiti dall'autorità giudiziaria francese nell'ambito di indagini da essa autonomamente svolte, e custoditi in banche dati francesi.

Si espone che, anche in caso di acquisizione di documenti relativi al traffico, all'ubicazione e al contenuto delle comunicazioni, è sempre necessario un preventivo controllo in concreto del giudice in ordine alla legittimità dell'adozione della misura, e che questa esigenza si impone, a maggior ragione, nel caso di trasferimento di prove già acquisite, perché, in tale ipotesi, il controllo dell'autorità giudiziaria dello Stato di esecuzione sarebbe stato compiuto prima dell'o.e.i. a fini ben diversi, e non potrebbe essere compiuto in sede di delibazione dell'o.e.i., stanti i limitatissimi spazi operativi previsti dall'art. 11, paragrafo 2, Direttiva 2014/41/UE. Si precisa che, con riferimento alle misure dirette ad acquisire dati sul traffico, e sull'ubicazione e sul contenuto delle comunicazioni, la necessità della preventiva autorizzazione del giudice discende già da Corte giustizia, Grande Sezione, 02/03/2021, H.H. Prokuratuur, C-746/18, e quindi era operativa in epoca precedente all'emissione dell'o.e.i. della Procura di Potenza, datato 9 luglio 2021. Si aggiunge che la tutela della segretezza e della libertà delle comunicazioni, e la conseguente ammissibilità di una loro limitazione solo in presenza di atto motivato dell'autorità giudiziaria, assicurata in primo luogo dall'art. 15 Cost. e dall'art. 6 CEDU, prescinde dal mezzo tecnico utilizzato ed è perciò riferibile anche a tutti gli

strumenti messi a disposizione dall'evoluzione tecnologica, quali i messaggi di posta elettronica o inviati mediante l'applicativo *WhatsApp*, come hanno precisato la giurisprudenza costituzionale (si citano Corte cost., sent. n. 170 del 2023 e Corte cost., sent. n. 2 del 2023) e sovranazionale (si citano, tra le altre, Corte EDU, Grande Camera, 05/09/2017, Bărbulescu c. Romania, e Corte EDU, 17/12/2020, Saber c. Norvegia).

Si conclude, pertanto, affermando che sussistono i presupposti per sollevare la questione di legittimità costituzionale, in riferimento agli artt. 3, 15 e 117, primo comma Cost., in relazione agli artt. 5, 6, 8, 9 e 15 Direttiva 2002/58/CE del Parlamento e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, agli artt. 7 e 52 Carta di Nizza e all'art. 8 CEDU, dell'art. 27 d.lgs. 21 giugno 2017, n. 108, nella parte in cui non prevede che l'adozione dell'o.e.i. da parte del pubblico ministero debba essere preceduta da un controllo giurisdizionale sugli elementi relativi alla giustificazione e all'adozione della misura richiesta, qualora questa abbia ad oggetto l'acquisizione di informazioni o prove che siano già in possesso dell'autorità di esecuzione, ovvero siano contenute in banche dati della polizia o delle autorità giudiziarie cui l'autorità di esecuzione può accedere direttamente nel quadro di un procedimento penale, e che inoltre si riferiscano a dati di traffico o di ubicazione o di contenuto di comunicazioni elettroniche.

5.2. Il motivo nuovo connesso al primo motivo del ricorso approfondisce il tema della inapplicabilità dell'art. 234-*bis* cod. proc. pen. e della inutilizzabilità dei dati informatici relativi alle comunicazioni effettuate tramite il sistema Sky-Ecc, ed acquisiti mediante o.e.i.

Si deduce che gli atti ottenuti mediante o.e.i. nel presente processo sono affetti da inutilizzabilità patologica, perché costituiscono "prova incostituzionale", in quanto sono stati acquisiti in violazione delle fonti normative dell'Unione Europea, come interpretate dalla Corte di giustizia UE, e dell'art. 15 Cost. Si segnala, in particolare, che le attività di captazione e di apprensione dei dati da parte delle Autorità estere sono state generalizzate ed indifferenziate, e si pongono perciò in contrasto con l'art. 15, paragrafo 1, Direttiva 2002/58/CE, letto alla luce degli artt. 7, 8, 11 e 52, paragrafo 1, Carta di Nizza, il quale consente la conservazione dei dati relativi al traffico ed all'ubicazione in materia di comunicazioni solo limitatamente a determinate categorie di persone o mediante un criterio geografico, e per un periodo limitato allo stretto necessario (si cita Corte giustizia, Grande Sezione, 05/04/2022, Commissioner of An Garda Síochána, C-140/20).

6. In data 12 febbraio 2024, la Procura generale ha presentato memoria, nella quale si sostiene, con ricchezza di argomenti, che la soluzione della legittimità

dell'acquisizione delle comunicazioni trasmesse dall'autorità giudiziaria francese a seguito di o.e.i. si impone quale che sia la qualificazione giuridica attribuibile alle stesse.

CONSIDERATO IN DIRITTO

1. Le questioni di diritto sottoposte alle Sezioni Unite sono le seguenti:

"Se l'acquisizione di messaggi su chat di gruppo, scambiati con sistema cifrato, attraverso un ordine europeo di indagine presso un'autorità giudiziaria straniera che ne abbia 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";

"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".

2. Le due questioni sottoposte all'esame delle Sezioni Unite, rilevanti ai fini della decisione del ricorso, perché attengono all'utilizzabilità di elementi significativi per l'affermazione di sussistenza dei gravi indizi di colpevolezza a carico del ricorrente, hanno dato luogo ad orientamenti contrastanti in seno alla giurisprudenza di legittimità, dei quali occorre dare conto in questa sede.

Sembra opportuno premettere che le due questioni sono tra loro strettamente connesse, perché le conclusioni sulla natura giuridica da attribuire all'acquisizione, effettuata tramite ordine europeo di indagine, di messaggi scambiati su *chat* di gruppo mediante un sistema cifrato, e già a disposizione dell'autorità giudiziaria straniera, hanno una diretta ricaduta in ordine al tema della necessità di preventiva o successiva verifica giurisdizionale, e che, per questa ragione, ognuno dei diversi indirizzi giurisprudenziali sarà oggetto di esposizione unitaria con riferimento alle soluzioni accolte per entrambi i profili.

3. Secondo l'orientamento espresso per primo in ordine di tempo, quando, in accoglimento di o.e.i., l'autorità giudiziaria straniera trasmette comunicazioni su *chat* di gruppo scambiate con sistema cifrato, le quali siano già in suo possesso nell'ambito di procedimento penale estero, si verte nell'ipotesi di cui all'art. 234-*bis* cod. proc. pen.

3.1. Alcune decisioni (cfr. in particolare: Sez. 1, n. 19082 del 13/01/2023, Costacurta, Rv. 284440-01; Sez. 1, n. 6363 del 13/10/2022, dep. 2023, Minichino, non mass.; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, Rv. 283998-01; Sez. 1, n. 34059 del 01/07/2022, Molisso, non mass.) premettono che, con

riferimento all'attività di acquisizione di messaggi su *chat* di gruppo scambiati con sistema cifrato, occorre distinguere tra due diversi tipi di possibili operazioni.

Da un lato, quando l'attività di captazione e registrazione si riferisce a messaggi in fase di transito dall'apparecchio del mittente a quello del destinatario, la disciplina applicabile è quella relativa alle intercettazioni, e, più precisamente, nel caso in cui l'oggetto sia costituito da flussi di comunicazioni trasmessi in via telematica, mediante cavi o ponti radio, o analoga strumentazione tecnica, occorre far riferimento alla previsione di cui all'art. 266-*bis* cod. proc. pen.

Dall'altro, quando invece l'attività di acquisizione e decifrazione si riferisce a comunicazioni già effettuate o comunque già acquisite dall'autorità giudiziaria estera, la disposizione applicabile è quella di cui all'art. 234-*bis* cod. proc. pen., la quale consente 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».

Le decisioni indicate precisano che, quando l'autorità giudiziaria italiana riceve dall'autorità giudiziaria straniera una «rappresentazione comunicativa incorporata in una base materiale con metodo digitale», ossia dati informatici, si versa nell'ambito dell'acquisizione di un documento informatico. Aggiungono, poi, che, in tal caso, ricorre anche l'ulteriore requisito per l'applicabilità della disciplina di cui all'art. 234-*bis* cod. proc. pen., ossia il consenso all'acquisizione del «legittimo titolare», siccome per «legittimo titolare» deve intendersi anche la persona giuridica che di quei dati e documenti può disporre in forza di un legittimo titolo, incluse, quindi, la polizia giudiziaria o l'autorità giudiziaria dello Stato estero.

Le tre decisioni più recenti (Sez. 1, n. 19082 del 13/01/2023, cit.; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, cit.; Sez. 1, n. 6363 del 13/10/2022, dep. 2023, cit.), inoltre, collegano specificamente la legittimità del procedimento di acquisizione degli atti da parte dell'autorità giudiziaria italiana alla procedura cui questa ha fatto riferimento: l'ordine europeo di indagine. Sottolineano, infatti, che l'o.e.i. deve avere ad oggetto prove acquisibili dello Stato di emissione, deve essere eseguito in conformità della disciplina prevista nello Stato di esecuzione in relazione un atto analogo, e, in linea con il consolidato insegnamento della giurisprudenza di legittimità in tema di rogatorie, deve presumersi adempiuto nel rispetto di questa disciplina e dei diritti fondamentali, salvo concreta verifica di segno contrario.

Due decisioni (Sez. 1, n. 6364 13/10/2022, dep. 2023, cit., e Sez. 1, n. 6363 13/10/2022, dep. 2023, cit.), ancora, rappresentano che: a) la disciplina dell'o.e.i., sulla base sia della Direttiva n. 2014/41/UE, sia del d.lgs. n. 108 del 2017, non vieta di acquisire risultati di attività investigative già compiute; b) è irrilevante se la richiesta di o.e.i. sia avanzata dal pubblico ministero anche quando attiene ad atti acquisibili in Italia solo in forza di provvedimento del giudice, a

norma dell'art. 132 d.lgs. 30 giugno 2003, n. 196, perché, nella specie, l'attività di acquisizione dei dati è avvenuta sotto la direzione del giudice dello Stato estero; c) non sussiste un problema di genuinità del dato informatico, derivante dalla mancata ostensione dell'algoritmo necessario alla decriptazione dei messaggi, in quanto, secondo la scienza informatica, solo l'algoritmo corretto consente di ottenere un testo dotato di significato, per cui è onere della difesa allegare specifici e concreti elementi da cui desumere, nella singola vicenda, rischi di alterazioni.

3.2. Numerose altre decisioni, nel ritenere applicabile la disciplina di cui all'art. 234-*bis* cod. proc. pen. all'acquisizione mediante o.e.i. di messaggi su *chat* di gruppo scambiati con sistema cifrato, già nella disponibilità dell'autorità giudiziaria straniera, aggiungono ulteriori precisazioni.

In particolare, alcune pronunce (Sez. 3, n. 47201 del 19/10/2023, Bruzzaniti, Rv. 285350 - 01; Sez. 4, n. 37503 del 30/05/2023, Iannaci, non mass.; Sez. 4, n. 16347 del 05/04/2023, Papalia, Rv. 284563 - 01; Sez. 4, n. 16345 del 05/04/2023, Liguori, non mass.; Sez. 4, n. 17647 del 28/03/2023, Gulluni, non mass.) segnalano che: a) è irrilevante accertare se l'autorità giudiziaria straniera abbia acquisito i dati *ex post* o in tempo reale, perché l'aspetto dirimente è costituito dall'essere stata la richiesta italiana di o.e.i. avanzata quando i flussi di comunicazione non erano più in corso; b) l'onere di provare l'incompatibilità degli atti compiuti dall'autorità giudiziaria straniera con i principi fondamentali ed inderogabili dell'ordinamento giuridico italiano grava su chi formula la relativa eccezione anche perché il diritto straniero è un "fatto".

Altra decisione (Sez. 4, n. 27775 dell'11/05/2023, Bonifazio, non mass.) aggiunge che la qualificazione dei dati acquisiti dall'autorità giudiziaria italiana come documenti, a norma dell'art. 234-*bis* cod. proc. pen. non pone problemi di compatibilità con i principi espressi dalla Direttiva 2014/41/UE, e quindi esclude la necessità di procedere ad un rinvio pregiudiziale alla Corte di giustizia UE a norma dell'art. 267, paragrafo 3, T.F.U.E. In particolare, in questa decisione, si rappresenta che la qualificazione dei dati ricevuti dall'autorità giudiziaria francese come documenti esclude la necessità per l'autorità giudiziaria italiana di chiedere, ai fini della loro acquisizione mediante o.e.i., una preventiva autorizzazione del giudice. Si rileva, inoltre, che, in linea generale, il pubblico ministero italiano è legittimato a presentare richiesta di o.e.i. perché autorità giudiziaria indipendente, non esposta al rischio di ricevere ordini o istruzioni individuali da parte del potere esecutivo. Si segnala, ancora, che gli obblighi informativi previsti dall'art. 31, paragrafo 1, Direttiva 2014/41/UE in relazione alle attività di intercettazione attuate da uno Stato nel territorio di un altro Stato sono posti a garanzia del principio di reciprocità tra Stati e non a protezione dei diritti individuali dei singoli utenti (per questo rilievo v. anche Sez. 3, n. 47201 del 19/10/2023, Bruzzaniti, Rv. 285350 - 01). La sentenza precisa, altresì, con specifico riguardo al caso

sottoposto al suo esame, che: a) la richiesta dell'autorità giudiziaria italiana non era indeterminata, in quanto relativa a dati transitati su utenze riferibili ad alcuni specifici PIN, ed era stata avanzata nell'ambito di un procedimento nel quale erano emersi già concreti indizi di reato; b) l'integrità dei dati era certificata da un «attestato vidimato dal responsabile dell'organismo tecnico» incaricato dall'autorità giudiziaria francese della materiale acquisizione dei dati.

4. Secondo un diverso orientamento, espresso da due pronunce (Sez. 6, n. 44155 del 26/10/2023, Kolgjokaj, Rv. 285362 - 01, 02, e Sez. 6, n. 44154 del 26/10/2023, Iaria, Rv. 285284 - 01, 02, 03), l'acquisizione, effettuata mediante un ordine europeo di indagine, di messaggi su *chat* di gruppo scambiati con sistema cifrato, quando attiene ai risultati di un'attività di apprensione occulta di comunicazioni non "in corso" o al sequestro di dati archiviati in un *server* o in altri supporti informatici, è regolata dalla disciplina di cui all'art. 254-*bis* cod. proc. pen., e non da quella di cui all'art. 234-*bis* cod. proc. pen.

4.1. Si osserva, per un verso, che l'art. 234-*bis* cod. proc. pen. è riferibile solo ad elementi preesistenti rispetto al momento dell'avvio delle indagini dell'autorità giudiziaria straniera, o comunque formati al di fuori di quelle investigazioni, e, sotto altro profilo, che non può parlarsi di acquisizione avvenuta con il consenso del «legittimo titolare», perché questo si identifica nel mittente e nel destinatario del messaggio, nonché nella società di gestione della piattaforma di transito della comunicazione, mentre l'autorità giudiziaria straniera è un mero detentore dei dati a fini di giustizia.

Ad avviso delle due decisioni, l'attività di acquisizione, mediante o.e.i., di messaggi su *chat* di gruppo scambiati con sistema cifrato, se non riferita a comunicazioni "in corso", deve essere, pertanto, qualificata a norma dell'art. 254-*bis* cod. proc. pen., nell'ambito della disciplina del sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni.

Si precisa, innanzitutto, che, se l'acquisizione ha ad oggetto dati "esterni" al traffico telefonico o telematico, occorre far riferimento alle regole di cui all'art. 132 d.lgs. n. 196 del 2003, mentre, se vi è stata una captazione di comunicazioni o di flussi di comunicazioni in corso, la disciplina da applicare è quella di cui agli art. 266 ss. cod. proc. pen.

Si segnala, poi, che l'art. 43, comma 4, d.lgs. n. 108 del 2017, lascia intendere che anche le attività di trascrizione, decodificazione o decrittazione delle comunicazioni intercettate, se richieste dall'autorità giudiziaria italiana a quella estera, debbono essere preventivamente autorizzate dal giudice.

Si sottolinea, ancora, che, con riguardo all'acquisizione presso il *server* dei dati esterni delle telecomunicazioni, la giurisprudenza della Corte di giustizia U.E. (segnatamente, Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur,

causa C-746/18) ha fissato limiti stringenti: in primo luogo, in forza del principio di proporzionalità, occorre che tanto la categoria o le categorie dei soggetti interessati, quanto la durata per la quale è richiesto l'accesso agli atti, siano limitate a ciò che è strettamente necessario ai fini dell'indagine; in secondo luogo, solo un giudice (o un'autorità indipendente e terza rispetto al processo) può garantire un corretto controllo sulla esistenza delle condizioni sostanziali e procedurali per l'accesso ai dati.

Si conclude, quindi, che «l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione de[ve] 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» (così, testualmente, Sez. 6, n. 44154 del 26/10/2023, cit.).

4.2. L'indirizzo in esame rappresenta inoltre che una conferma delle conclusioni raggiunte è fornita dalla più recente giurisprudenza della Corte costituzionale in tema di tutela della libertà e segretezza della corrispondenza, *ex* art. 15 Cost.

Si segnala, in particolare, che secondo Corte cost., sent. n. 170 del 2023, l'art. 15 Cost. tutela la corrispondenza, ivi compresa quella elettronica, anche dopo la sua ricezione da parte del destinatario, almeno fino a quando non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, e che, secondo Corte cost., sent. n. 2 del 2023, tale tutela si connota per la "riserva di giurisdizione", da intendersi come «vaglio dell'autorità giurisdizionale [...] associato alla garanzia del contraddittorio, alla possibile contestazione dei presupposti applicativi della misura, della sua eccessività e proporzione, e, in ultima analisi, consente il pieno dispiegarsi allo stesso diritto di difesa».

Si aggiunge che la giurisprudenza costituzionale si richiama a quella della Corte EDU, la quale 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, 05/09/2017, Barbulescu c. Romania; § 72; Corte EDU, 03/04/2007, Copland c. Regno Unito, § 41), gli *s.m.s.* (Corte EDU, 17/12/2020, Saber c. Norvegia) e la messagistica istantanea inviata e ricevuta tramite *internet* (Corte EDU, Barbulescu, cit., § 74)».

4.3. Sulla base di queste precisazioni in ordine alla natura dell'attività di acquisizione delle comunicazioni elettroniche, le decisioni indicate osservano che l'autorità giudiziaria italiana competente ad emettere l'o.e.i. diretto ad ottenere tali elementi è sì il pubblico ministero, ma potrebbe essere necessaria una previa autorizzazione del giudice.

Si evidenzia che l'illegittimità di un o.e.i. emesso senza la preventiva autorizzazione del giudice, quando questa è necessaria, può essere fatta valere dalla difesa, ma produce conseguenze diversificate: se l'o.e.i. ha determinato lo svolgimento di un'attività investigativa illegittima, la genesi patologica della prova raccolta determina l'inutilizzabilità di questa; se, invece, l'o.e.i. è stato emesso al fine di acquisire una prova «già disponibile» nello Stato di esecuzione, e la questione non è stata fatta valere con successo davanti agli organi di quest'ultimo, la verifica sulla sussistenza delle condizioni di ammissibilità della prova può essere chiesta al giudice italiano.

Si richiama, in particolare, quanto già affermato dalla giurisprudenza di legittimità con riguardo alle intercettazioni eseguite in altro procedimento, e cioè la sindacabilità anche nel processo "ricevente" della legalità del procedimento di autorizzazione ed esecuzione delle attività di captazione (si cita Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229244-01). Sulla base di questo paradigma, si osserva che, nel sistema della Direttiva sull'ordine europeo di indagine, per l'acquisizione dei risultati di un'intercettazione già svolta all'estero, non è sufficiente l'autorizzazione di questa da parte del giudice dello Stato di esecuzione nel rispetto della sua legislazione nazionale, ma occorre anche il controllo del giudice dello Stato di emissione sull'ammissibilità e l'utilizzabilità della prova secondo la propria legislazione, nella specie quella italiana.

4.4. Quanto al regime di utilizzabilità della prova acquisita mediante o.e.i., Sez. 6, n. 44154 del 26/10/2023, cit., aggiunge alcune precisazioni.

Rileva, innanzitutto, che la giurisprudenza della Corte di giustizia riconosce l'autonomia procedurale degli ordinamenti nazionali in tema di ammissibilità e valutazione delle prove, ferma restando la necessità di evitare che «informazioni ed elementi di prova ottenuti in modo illegittimo rechino indebitamente pregiudizio a una persona sospettata di avere commesso reati» (si cita Corte giustizia, Grande Sezione, 06/10/2020, C-511/18, 512/18 e 520/18). Argomenta, poi, che l'ordinamento nazionale si limita ad indicare, nell'art. 36 d.lgs. n. 108 del 2017, quali atti ricevuti mediante o.e.i. possano essere raccolti nel fascicolo per il dibattimento.

Osserva, perciò, che, ai fini in questione, deve soccorrere l'elaborazione consolidata della giurisprudenza in tema di rogatorie, elaborazione secondo la quale l'atto compiuto all'estero può essere eseguito anche applicando le disposizioni processuali dello Stato straniero, ma è utilizzabile in Italia solo se non contrasta con i principi fondamentali del nostro ordinamento, tra i quali quelli della tutela dell'inviolabilità del diritto di difesa e del contraddittorio per la prova.

Segnala, in particolare, che: a) secondo la giurisprudenza di legittimità, la difesa ha diritto di ottenere la versione originale e criptata dei messaggi e le chiavi di sicurezza per la decriptazione, a pena di nullità *ex* art. 178, lett. c), cod. proc.

pen. (si cita Sez. 4, n. 49896 del 15/10/2019, Brandimarte, Rv. 277949-03); b) secondo la Corte EDU, è da ritenere compromesso il diritto di difesa in relazione a dati raccolti in un *server* di messaggistica crittografata, quando di essi non è stata consentita la verifica sotto il profilo del contenuto e della integrità, salva la presenza di interessi concorrenti, quali la sicurezza nazionale o la necessità di mantenere segreti i metodi di indagine sui reati da parte della polizia, e ferma restando, anche in questo caso, la necessità di fornire all'imputato «un'opportunità adeguata» per preparare la sua difesa, a norma dell'art. 6 CEDU (si cita Corte EDU, Grande Camera, 26/09/2023, Yüksel Yalçinkaya c. Turchia).

5. Secondo un ulteriore orientamento, espresso da tre pronunce (Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, Rv. 285543 - 01, 02, 03; Sez. 6, n. 48838 dell'11/10/2023, Brunello, Rv. 285599 - 01, 02; Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363 - 01, 02, 03, 04), l'acquisizione, effettuata mediante un ordine europeo di indagine, di messaggi su *chat* di gruppo scambiati con sistema cifrato, quando attiene ad elementi già raccolti in un procedimento penale pendente davanti all'autorità giudiziaria dello Stato di esecuzione, ha ad oggetto, se riguarda corrispondenza, una prova documentale. Nel caso in cui, invece, si riferisca ai risultati di intercettazioni, il relativo trasferimento nel procedimento nazionale, può essere disposto dal pubblico ministero, senza necessità di preventiva autorizzazione del giudice.

5.1. Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti, cit., premette che, nel sistema giuridico italiano, per l'acquisizione di comunicazioni personali conservate nei dispositivi informatici, anche quando queste costituiscono corrispondenza, si applicano le disposizioni in materia di perquisizione e sequestro, e quindi le previsioni di cui agli artt. 244, 247, comma 1-*bis*, 254-*bis* e 352, comma 1-*bis*, cod. proc. pen., con conseguente superfluità di un provvedimento del giudice.

Osserva che la conclusione appena indicata non si pone in contrasto con l'insegnamento della Corte costituzionale, secondo cui la documentazione relativa a comunicazioni scambiate a distanza di tempo non significativa e conservata dagli utenti, anche se memorizzata in dispositivi portatili ad accesso protetto, ha natura di corrispondenza (si cita, in particolare, Corte cost., sent. n. 170 del 2023). Segnala, infatti, che il principio indicato implica l'applicazione delle garanzie previste dall'art. 15 Cost., e, quindi, impone l'intervento del pubblico ministero, ma non anche l'autorizzazione del giudice.

Rileva, poi, che la corrispondenza, anche informatica, costituisce prova documentale a norma dell'art. 234 cod. proc. pen., e che, però, è inapplicabile la disciplina di cui all'art. 234-*bis* cod. proc. pen., perché questa disposizione attiene a materiale disponibile in rete, ovvero a materiale che, se non liberamente accessibile al pubblico, può essere acquisito con il consenso del «legittimo

titolare». Sulla base di questa premessa, conclude che la documentazione trasmessa dall'autorità giudiziaria francese avrebbe potuto essere acquisita in Italia mediante un provvedimento del pubblico ministero di sequestro probatorio di documentazione/corrispondenza.

La medesima sentenza osserva che, con riguardo all'acquisizione di prove già raccolte nello Stato di esecuzione dell'o.e.i., un fondamentale punto di riferimento per l'individuazione delle regole giuridiche applicabili è costituito dalla disciplina interna in materia di trasferimento di prove tra procedimenti. Evidenzia che, in linea generale, il trasferimento di prove tra procedimenti può essere richiesto con provvedimento del pubblico ministero, anche con riguardo a risultanze di intercettazioni, in quanto l'art. 270 cod. proc. pen., per l'utilizzabilità di queste in un procedimento diverso da quello in cui sono state disposte, pone limiti correlati alla gravità dei reati, ma non richiede alcun provvedimento autorizzatorio del giudice.

Aggiunge, poi, che la necessità di un provvedimento autorizzativo del giudice italiano per l'acquisizione di dati già nella disponibilità dell'autorità giudiziaria estera non può farsi discendere dal diritto sovranazionale. Invero, la Direttiva 2002/58/UE concerne il divieto per gli operatori dei servizi telefonici di conservare dati di traffico e di ubicazione degli utenti, ma non anche le intercettazioni, né «la acquisizione di documentazione elettronica posta nei dispositivi personali dell'utente (o negli spazi virtuali su *server* in suo accesso esclusivo)» (si cita a conferma, tra le altre, Corte giustizia, Grande Sezione, 06/10/2020, La Quadrature du net, C-511/18, C-512/18 e C-520/18, per l'espressa precisazione contenuta nel § 103). Ostacoli non derivano nemmeno dall'elaborazione della giurisprudenza della Corte EDU, e segnatamente da Corte EDU, Grande Camera, 26/09/2023, Yüksel Yalçinkaya c. Turchia, in quanto questa decisione ha ad oggetto una vicenda in cui, nel procedimento nazionale, il materiale acquisito non era stato messo a disposizione della difesa e la pronuncia di colpevolezza era stata fondata sul solo fatto dell'utilizzazione del sistema di messaggistica criptata.

Con specifico riferimento al caso da essa esaminato, la pronuncia sottolinea che: a) la disciplina francese in materia di acquisizione della messaggistica già trasmessa e conservata nei dispositivi personali mediante accesso occulto a sistemi informatici (artt. da 706-95 a 706-95-3 e da 706-102-1 a 706-102-5 del codice di procedura penale) prevede la necessità di un provvedimento motivato del giudice; b) la segretezza del sistema usato per "mettere in chiaro" i messaggi criptati non è in contrasto con la legge italiana, perché gli artt. 268 cod. proc. pen. e 89 disp. att. cod. proc. pen. riconoscono il diritto di accedere al verbale delle operazioni e alle registrazioni, ma non anche ai mezzi tecnici e ai programmi utilizzati per la intrusione nelle conversazioni intercettate; c) la decriptazione delle conversazioni e comunicazioni è attività distinta dalla captazione, e, quindi, non

implica il diritto di conoscere il programma o l'algoritmo a ciò necessario, salvo che siano allegate e provate specifiche anomalie tecniche.

5.2. Conclusioni omogenee, anche se espresse nell'ambito di un ragionamento sviluppato con ordine espositivo diverso, sono raggiunte da Sez. 6, n. 46833 del 26/10/2023, cit., e da Sez. 6, n. 48838 dell'11/10/2023, cit.

Entrambe le decisioni evidenziano che: a) il sistema della Direttiva 2014/41/UE, relativa all'ordine europeo di indagine, «[i]nclude anche l'acquisizione di prove già in possesso dell'autorità di esecuzione», come precisa il settimo Considerando di essa; b) la cooperazione giudiziaria si fonda sulla presunzione del rispetto, da parte dei Paesi membri, del diritto dell'Unione e dei diritti fondamentali (si cita, per un'affermazione relativa proprio ad un procedimento concernente l'o.e.i., Corte giustizia, 23/01/2018, Piotrowski, C-367/16, § 50); c) la mancata conoscenza, da parte della difesa, dell'algoritmo utilizzato per decriptare i messaggi non costituisce limitazione rilevante ai fini del controllo di possibili alterazioni, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun messaggio è inscindibilmente correlato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente; d) l'art. 234-*bis* cod. proc. pen. è inapplicabile perché trova la sua matrice nell'art. 32 della Convenzione di Budapest sul *cybercrime*, la quale si riferisce all'acquisizione di documentazione reperibile in *internet*, e non alla documentazione ottenuta mediante consegna formalmente effettuata dall'autorità giudiziaria straniera.

Sez. 6, n. 48838 dell'11/10/2023, cit., inoltre, precisa che: a) le comunicazioni inviate mediante la posta elettronica o il sistema *WhatsApp* costituiscono corrispondenza, in linea con quanto affermato da Corte cost., sent. n. 170 del 2023; b) nell'ordinamento italiano, il trasferimento della corrispondenza, come delle conversazioni intercettate, è ammissibile sulla base di un provvedimento del pubblico ministero; c) nello spazio comune europeo, la prova costituita da documentazione acquisita presso gli operatori di telecomunicazioni con provvedimento del giudice può circolare senza la necessità di un ulteriore provvedimento del giudice in procedimenti diversi, purché sia rispettato il limite della utilizzazione dei dati per la tutela della sicurezza pubblica e della prevenzione di gravi reati (si citano, specificamente, Corte giustizia, 07/09/2023, A.G., C-162/22, e Corte giustizia, 16/12/2021, H.P., C-724/19); d) non è applicabile la disciplina di cui all'art. 43, comma 4, d.lgs. n. 108 del 2017, la quale, nel dettare le regole relative alla richiesta di intercettazioni mediante o.e.i., stabilisce che la stessa «possa avere ad oggetto la trascrizione, la decodificazione o decrittazione delle comunicazioni intercettate», perché tale disciplina concerne le richieste relative allo svolgimento congiunto sia delle attività di intercettazione, sia di quelle a queste accessorie; e) l'omesso deposito degli atti

concernenti le intercettazioni disposte nel procedimento *a quo* presso l'autorità competente per il procedimento *ad quem* non comporta l'inutilizzabilità dei risultati acquisiti in quest'ultimo, in quanto tale sanzione non è prevista né dall'art. 270, né dall'art. 271 cod. proc. pen.

6. Così riassunti i termini del contrasto, le Sezioni Unite ritengono innanzitutto di precisare che, con riferimento all'acquisizione, effettuata mediante o.e.i., di messaggi scambiati su *chat* di gruppo mediante un sistema cifrato, e già a disposizione dell'autorità giudiziaria straniera, non è applicabile la disciplina di cui all'art. 234-*bis* cod. pen., perché la stessa è alternativa e incompatibile rispetto a quella dettata in tema di o.e.i.

6.1. L'art. 234-*bis* cod. proc. pen., introdotto dall'art. 2, comma 1-*bis*, d.l. 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, prevede testualmente: «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».

Come si evince dal contenuto appena trascritto, la disposizione disciplina non un mezzo di prova, bensì una modalità di acquisizione di particolari tipologie di elementi di prova presenti all'estero, che viene attuata in via "diretta" dall'autorità giudiziaria italiana e prescinde da qualunque forma di collaborazione con le autorità dello Stato in cui tali dati sono custoditi.

Il sistema dell'o.e.i. regola anch'esso una modalità di acquisizione degli elementi di prova "transfrontalieri", che, però, si realizza nell'ambito di rapporti di collaborazione tra autorità giudiziarie di Stati diversi, tutti membri dell'Unione Europea.

Si tratta, quindi, di discipline che si riferiscono a vicende tra loro diverse già per il presupposto di applicazione: l'art. 234-*bis* cod. proc. pen. riguarda l'acquisizione di elementi conservati all'estero che prescinde da forme di collaborazione con l'autorità giudiziaria di altro Stato; la disciplina relativa all'o.e.i. attiene all'acquisizione di elementi conservati all'estero da ottenere od ottenuti con la collaborazione dell'autorità giudiziaria di altro Stato.

Si può aggiungere che il rapporto di alternatività tra acquisizione di elementi istruttori operata in via diretta dall'autorità giudiziaria procedente e acquisizione di elementi istruttori sulla base di rapporti di collaborazione con autorità giudiziarie di altri Stati trova una chiara esplicitazione nella Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001, nella parte in cui la stessa regola i «poteri di indagine» per l'"accesso" a dati informatici ubicati all'estero rispetto all'autorità giudiziaria procedente.

Questa Convenzione, infatti, prevede che l'accesso a dati informatici «immagazzinati» in un sistema informatico ubicato all'estero è effettuato

nell'ambito di rapporti di «mutua assistenza» tra Stati (art. 31), e, nei soli casi di dati disponibili al pubblico o resi disponibili dalla persona legalmente autorizzata alla loro divulgazione, «senza l'autorizzazione di un'altra Parte» (art. 32).

6.2. Ciò posto, occorre inoltre evidenziare che la Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014, relativa all'ordine europeo di indagine, assegna alla disciplina da essa dettata una funzione di preminenza, in materia di acquisizione delle prove nell'ambito di rapporti di collaborazione tra autorità giudiziarie di più Stati dell'Unione Europea.

La volontà della Direttiva 2014/41/UE di regolare in modo organico il sistema di acquisizione delle prove mediante la collaborazione tra Stati, anche con riferimento a quelle già a disposizione dell'autorità giudiziaria destinataria della richiesta, risulta espressa in modo inequivocabile dagli artt. 1 e 3 e dai Considerando (6), (7) e (35).

L'art. 1 precisa che l'o.e.i. può essere emesso anche per ottenere «prove già in possesso delle autorità competenti dello Stato di esecuzione», mentre l'art. 3 precisa che l'o.e.i. «si applica a qualsiasi atto d'indagine, tranne all'istituzione di una squadra investigativa comune e all'acquisizione di prove nell'ambito di tale squadra [...]».

Il Considerando (6), nel terzo periodo, rappresenta: «Il Consiglio europeo ha pertanto chiesto la creazione di un sistema globale in sostituzione di tutti gli strumenti esistenti nel settore, compresa la decisione quadro 2008/978/GAI del Consiglio, che contempli per quanto possibile tutti i tipi di prove, stabilisca i termini di esecuzione e limiti al minimo i motivi di rifiuto».

Il Considerando (7), poi, oltre a ribadire la volontà di predisporre un unico sistema di disciplina per l'acquisizione delle prove "transfrontaliere", precisa che in queste rientrano anche quelle già a disposizione dell'autorità giudiziaria destinataria della richiesta. Così prevede: «Tale nuova impostazione si basa su un unico strumento denominato ordine europeo di indagine (OEI). L'OEI deve essere emesso affinché nello Stato che lo esegue (lo "Stato di esecuzione") siano compiuti uno o più atti di indagine specifici ai fini dell'acquisizione di prove. Ciò include anche l'acquisizione di prove già in possesso dell'autorità di esecuzione».

Il Considerando (35), ancora, stabilisce la prevalenza della Direttiva 2014/41/UE su tutti gli altri strumenti internazionali, statuendo: «Nei casi in cui è fatto riferimento all'assistenza giudiziaria nei pertinenti strumenti internazionali, come nelle convenzioni concluse in seno al Consiglio d'Europa, dovrebbe essere inteso che l'applicazione della presente direttiva tra gli Stati membri vincolati dalla stessa è preminente rispetto a dette convenzioni».

Il principio di completezza della disciplina dell'o.e.i. non è in alcun modo derogato nell'ordinamento italiano, come desumibile dalle seguenti disposizioni.

L'art. 1 d.lgs. 21 giugno 2017, n. 108, rubricato «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», infatti, così statuisce espressamente: «Il presente decreto attua nell'ordinamento interno la direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014, [...] relativa all'ordine europeo di indagine penale [...]». L'art. 2, comma 1, lett. *a)*, d.lgs. cit., a sua volta, precisa che l'ordine europeo di indagine può essere emesso anche «per acquisire informazioni o prove che sono già disponibili».

7. Individuate nella Direttiva 2014/41/UE e nel d.lgs. n. 108 del 2017 le coordinate della disciplina in tema di acquisizione di elementi istruttori effettuata dall'autorità giudiziaria italiana mediante o.e.i., è necessario esaminare innanzitutto quali sono le regole generali di tale sistema normativo.

7.1. Profilo preliminare, e fondamentale, è quello che attiene alle condizioni di ammissibilità dell'o.e.i.: solo se l'o.e.i. è stato legittimamente emesso, gli elementi acquisiti per il suo tramite potranno essere validamente utilizzati nel procedimento o nel processo pendente in Italia.

In proposito, le disposizioni dell'ordinamento nazionale di carattere generale sono estremamente laconiche. In particolare, l'art. 27, comma 1, d.lgs. n. 108 del 2017 si limita a prevedere, in linea generale, che «il pubblico ministero e il giudice che procede possono emettere, nell'ambito delle relative attribuzioni, un ordine di indagine e trasmetterlo direttamente all'autorità di esecuzione». Più in generale, l'art. 1 d.lgs. cit., rubricato «Disposizioni di principio», prevede che il d.lgs. n. 108 del 2017 «attua nell'ordinamento interno la direttiva 2014/41/UE».

Disposizioni più dettagliate sono previste in relazione a specifici atti di indagine, quali la richiesta di intercettazioni di telecomunicazioni (art. 43), e la richiesta di documentazione inerente ai dati esterni relativi al traffico telefonico o telematico (art. 45).

Tuttavia, la precisazione di carattere generale contenuta nell'art. 1 d.lgs. cit. induce a ritenere applicabili anche agli o.e.i. emessi dall'autorità giudiziaria italiana le condizioni di ammissibilità previste dall'art. 6, paragrafo 1, Direttiva 2014/41/UE.

7.2. La cogenza delle prescrizioni appena indicate, nella prospettiva di assicurare la effettività del diritto euro-unitario, è espressamente sottolineata dal paragrafo 2 dell'art. 6 della Direttiva («Le condizioni di cui al paragrafo 1 sono valutate dall'autorità di emissione in ogni caso»).

Questo articolo, al paragrafo 1, prevede che l'autorità richiedente «può emettere un o.e.i. solamente quando ritiene soddisfatte le seguenti condizioni: *a*) l'emissione dell'o.e.i. è necessaria e proporzionata ai fini del procedimento di cui all'art. 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata;

e *b*) l'atto o gli atti di indagine richiesti nell'o.e.i. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo».

Il giudizio sulla sussistenza della prima condizione (necessità e proporzionalità) deve essere compiuto avendo riguardo al procedimento nel cui ambito è emesso l'ordine europeo di indagine. In questo senso, univoche sono le indicazioni fornite sia dall'art. 4 Direttiva cit., sia dal Considerando (11) della medesima Direttiva. Invero, l'art. 4 Direttiva cit., espressamente richiamato dall'art. 6, fa riferimento al procedimento nel quale è emesso l'o.e.i. Il Considerando (11) della Direttiva cit., poi, precisa che «[l]'autorità di emissione dovrebbe pertanto accertare se le prove che si intende acquisire sono necessarie e proporzionate ai fini del procedimento, se l'atto di indagine scelto è necessario e proporzionato per l'acquisizione di tali prove, e se è opportuno emettere un o.e.i. affinché un altro Stato membro partecipi all'acquisizione di tali prove».

Il giudizio sulla sussistenza della seconda condizione (ammissibilità dell'atto richiesto alle stesse condizioni in un caso interno analogo) presuppone l'individuazione del "tipo" di atto oggetto di o.e.i.

Come osservato in dottrina, essa postula una valutazione in astratto, ed è quindi logicamente preliminare, mentre l'altra condizione, ossia quella concernente la necessità e la proporzionalità dell'atto richiesto, implica una valutazione in concreto, rapportata allo specifico procedimento nel cui ambito è stato emesso l'o.e.i.

Non mancano, inoltre, disposizioni che dettano condizioni di ammissibilità ulteriori ed aggiuntive con riferimento a specifici atti di indagine, come quelle in tema di intercettazione di comunicazioni, contenute negli artt. 30 e 31 Direttiva 2014/41/UE.

Le ragioni di merito dell'emissione di un o.e.i., secondo quanto precisa l'art. 14, paragrafo 2, Direttiva cit., possono essere oggetto di controllo successivo, e precisamente «impugnate», solo «mediante un'azione introdotta nello Stato di emissione», salvo la necessità di assicurare tutela ai diritti fondamentali nello Stato di esecuzione; e, però, «[u]n'impugnazione non sospende l'esecuzione dell'atto di indagine, a meno che ciò non abbia tale effetto in casi interni analoghi» (art. 14, paragrafo 6, Direttiva cit.).

7.3. La fase di esecuzione di un o.e.i. emesso dall'autorità giudiziaria italiana non riceve puntuale regolamentazione nel d.lgs. n. 108 del 2017.

Piuttosto, il d.lgs. cit., da un lato, sottolinea, in termini generali, all'art. 1, l'esigenza del «rispetto dei principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione europea in tema di diritti fondamentali, nonché in tema di diritti di libertà e di giusto processo».

Per altro verso, detta, all'art. 35, disposizioni sulla utilizzabilità degli atti compiuti e delle prove assunte all'estero. L'art. 35 cit., precisamente, prevede

l'inserimento nel fascicolo del dibattimento: a) dei documenti e degli atti non ripetibili acquisiti mediante o.e.i., senza richiedere particolari condizioni; b) dei verbali degli altri atti acquisiti mediante o.e.i., se agli stessi i difensori sono stati posti in condizione di assistere e di esercitare le facoltà loro consentite dalla legge italiana; c) dei verbali di dichiarazioni non ripetibili assunte all'estero a seguito di o.e.i. e non acquisite in contraddittorio nei casi e con le modalità di cui all'art. 512-*bis* cod. proc. pen.

Per completezza, è utile precisare che la garanzia del rispetto dei principi della Carta dei diritti fondamentali dell'Unione europea in tema di diritti fondamentali (c.d. Carta di Nizza) implica anche la garanzia del rispetto dei principi desumibili, nella medesima materia, dalla Convenzione Europea dei Diritti dell'Uomo. Invero, la Carta di Nizza, come precisa il preambolo e puntualizzano le annesse "Spiegazioni", il cui valore giuridico è formalmente sancito dall'art. 52, paragrafo 7, della Carta, «riafferma» espressamente anche i diritti derivanti dalla Convenzione Europea dei Diritti dell'Uomo e delle Libertà fondamentali, nonché dalla giurisprudenza della Corte europea dei diritti dell'uomo.

7.4. La disciplina posta dalla Direttiva 2014/41/UE, dal canto suo, non contiene regole relative alla fase di esecuzione degli o.e.i. che incidano specificamente sulla utilizzabilità degli atti acquisiti nel procedimento davanti all'autorità di emissione.

In linea generale, l'art. 14 Direttiva cit. fornisce precise indicazioni per ritenere che le questioni concernenti la fase di esecuzione, e quindi anche quelle concernenti la scelta di riconoscere ed eseguire l'o.e.i., siano proponibili esclusivamente nello Stato di esecuzione.

Invero, significative sono le previsioni relative alla esperibilità di mezzi di impugnazione anche nello Stato di esecuzione, a scambi reciproci di informazioni anche sui mezzi di impugnazione contro il riconoscimento e l'esecuzione di un o.e.i., e all'obbligo per lo Stato di emissione di tener conto dell'esito delle impugnazioni concernenti il riconoscimento e l'esecuzione dell'o.e.i.

Né appare seriamente ipotizzabile che identiche questioni possano essere proposte sia nello Stato di esecuzione, sia nello Stato di emissione. Emblematica, in proposito, è la regola che esclude la proponibilità di questioni relative alle ragioni di merito dell'emissione dell'o.e.i. nello Stato di esecuzione, stabilita dall'art. 14, paragrafo 2, Direttiva cit., «fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione».

Tuttavia, la medesima Direttiva evidenzia la necessità di assicurare il rispetto dei «diritti fondamentali» da parte dell'autorità giudiziaria dello Stato di emissione anche con riguardo alle attività compiute nello Stato di esecuzione.

L'art. 14 cit., paragrafo 2, stabilisce che le ragioni di merito in ordine all'emissione dell'o.e.i. possono essere fatte valere «soltanto mediante un'azione

introdotta nello Stato di emissione», «fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione». Ancor più significativamente, però, al paragrafo 7, secondo periodo, con una previsione specificamente riferita alla valutazione delle prove nel procedimento *ad quem*, dispone: «Fatte 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'o.e.i.».

Inoltre, con una regola di principio e di "chiusura" del sistema, l'art. 1, paragrafo 4, Direttiva cit. statuisce: «La presente direttiva non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 T.U.E., compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità giudiziarie».

7.5. In forza del coordinamento normativo tra il d.lgs. n. 108 del 2017 e la Direttiva 2014/41/UE, sembra ragionevole affermare che, ai fini dell'utilizzabilità di atti acquisiti mediante o.e.i. dall'autorità giudiziaria italiana, è necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo, ma non anche l'osservanza, da parte dello Stato di esecuzione, di tutte le disposizioni previste dall'ordinamento giuridico italiano in tema di formazione ed acquisizione di tali atti.

Da un lato, infatti, sia la Direttiva 2014/41/UE, in particolare gli artt. 1 e 14, sia il d.lgs. n. 108 del 2017, in particolare l'art. 1, evidenziano, come principio generale, l'esigenza di assicurare il rispetto dei diritti fondamentali, e, tra questi, i diritti della difesa e ad un giusto processo.

Dall'altro, poi, né l'art. 36 d.lgs. n. 108 del 2017, né altre disposizioni del medesimo d.lgs. o della Direttiva 2014/41/UE prevedono, ai fini dell'utilizzabilità degli atti formati all'estero, la necessità di una puntuale applicazione di tutte le regole che l'ordinamento giuridico italiano fissa, in via ordinaria, per la formazione degli atti corrispondenti formati sul territorio nazionale. Anzi, l'art. 14, paragrafo 7, Direttiva cit., proprio laddove impone allo Stato di emissione di rispettare i diritti della difesa e di garantire un giusto processo nel valutare le prove acquisite tramite l'o.e.i., stabilisce: «[f]atte salve le norme procedurali nazionali» (dizione, quest'ultima, riferita allo Stato di esecuzione).

La soluzione accolta, del resto, corrisponde alla costante tradizione del nostro ordinamento, e alla consolidata elaborazione della giurisprudenza di legittimità, secondo cui, in tema di rogatoria internazionale, trovano applicazione le norme processuali dello Stato in cui l'atto viene compiuto, con l'unico limite che la prova non può essere acquisita in contrasto con i principi fondamentali dell'ordinamento giuridico italiano e dunque con il diritto di difesa (Sez. 2, n. 2173 del 22/12/2016,

dep. 2017, Crupi, Rv. 269000 - 01, la quale ha ritenuto esente da censure il provvedimento impugnato che aveva respinto l'eccezione di inutilizzabilità di intercettazioni ambientali disposte ed acquisite dall'autorità olandese, osservando che la procedura penale olandese in tema di intercettazioni era conforme ai principi garantiti dall'art. 15 della Costituzione, pur se differente da quella italiana, in quanto la motivazione deve essere fornita nella richiesta di autorizzazione del pubblico ministero e non nel provvedimento autorizzativo del giudice, e la durata prevista per le operazioni è di quattro settimane, con possibilità di rinnovo).

Questa Corte ha altresì affermato che, in materia di rogatoria internazionale, l'atto istruttorio assunto all'estero è inutilizzabile solo quando venga prospettata l'assenza nell'ordinamento dello Stato richiesto di una normativa a tutela delle garanzie difensive, non anche quando si contesti la mera inosservanza delle regole dettate dal codice di rito dello Stato italiano richiedente (Sez. 6, n. 43534 del 24/04/2012, Lubiana, Rv. 253797 - 01).

7.6. Ai fini dell'accertamento del rispetto dei diritti fondamentali, assumono rilievo i principi della presunzione relativa di conformità ai diritti fondamentali dell'attività svolta dall'autorità giudiziaria estera nell'ambito di rapporti di collaborazione ai fini dell'acquisizione di prove, e dell'onere per la difesa di allegare e provare il fatto dal quale dipende la violazione denunciata.

Il principio della presunzione di legittimità dell'attività compiuta all'estero ai fini dell'acquisizione di elementi istruttori è oggetto di costante e generale enunciazione da parte della giurisprudenza di questa Corte (cfr., *ex plurimis*: Sez. 6, n. 44882 del 04/10/2023, Barbaro, Rv. 285386 - 01; Sez. 3, n. 1396 del 12/10/2021, dep. 2022, Torzi, Rv. 282886 - 01; Sez. 4, n. 19216 del 06/11/2019, dep. 2020, Ascone, Rv. 279246 - 01).

Nel sistema della Direttiva 2014/41/UE, poi, è espressamente riconosciuto il principio della «presunzione relativa che gli altri Stati membri rispettino il diritto dell'Unione e, in particolare, i diritti fondamentali» (Corte giustizia, 11/11/2021, Gavanozov, C-852/19, § 54; cfr., nello stesso senso, Corte giustizia, 08/12/2020, Staatsanwaltschaft Wien, C-584/19, § 40). Tale principio, del resto, trova una precisa base testuale nel Considerando (19) della Direttiva cit., il quale afferma: «La creazione di uno spazio di libertà, di sicurezza e di giustizia nell'Unione si fonda sulla fiducia reciproca e su una presunzione di conformità, da parte di tutti gli Stati membri, al diritto dell'Unione e, in particolare, ai diritti fondamentali. Tuttavia, tale presunzione è relativa. Di conseguenza, se sussistono seri motivi per ritenere che l'esecuzione di un atto di indagine richiesto in un o.e.i. comporti la violazione di un diritto fondamentale e che lo Stato di esecuzione venga meno ai suoi obblighi in materia di protezione dei diritti fondamentali riconosciuti nella Carta, l'esecuzione dell'o.e.i. dovrebbe essere rifiutata».

Anche il principio secondo cui grava sulla difesa l'onere di allegare e provare il fatto dal quale dipende una causa di nullità o inutilizzabilità da essa eccepita è ripetutamente e generalmente ribadito dalla giurisprudenza di legittimità.

Le Sezioni Unite, in particolare, hanno affermato che, nel caso in cui una parte deduca il verificarsi di cause di nullità o inutilizzabilità collegate ad atti non rinvenibili nel fascicolo processuale (perché appartenenti ad altro procedimento o anche - qualora si proceda con le forme del dibattimento - al fascicolo del pubblico ministero), al generale onere di precisa indicazione che incombe su chi solleva l'eccezione si accompagna l'ulteriore onere di formale produzione delle risultanze documentali - positive o negative - addotte a fondamento del vizio processuale (così Sez. U, n. 39061 del 16/07/2009, De Iorio, Rv. 244329 – 01, e, in termini analoghi, Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229245 – 01; tra le tante successive conformi, cfr. Sez. 5, 23015 del 19/04/2023, Bernardi, Rv. 284519 – 01, e Sez. 6, n. 18187 del 14/12/2017, dep. 2018, Nunziato, Rv. 273007 - 01).

A fondamento di questa affermazione, si osserva che, «per i fatti processuali, a differenza di quanto avviene per i fatti penali, ciascuna parte ha l'onere di provare quelli che adduce, quando essi non risultino documentati nel fascicolo degli atti di cui il giudice dispone» (così Sez. U, n. 45189 del 2004, Esposito, cit., nonché Sez. 5, n. 1915 del 18/11/2010, dep. 2011, Durantini, Rv. 249048 – 01, e Sez. 5, n. 600 del 17/12/2008, dep. 2009, Cavallaro, Rv. 242551 – 01). E l'osservazione deve essere ribadita perché l'art. 187, comma 2, cod. proc. pen. prevede che i fatti dai quali dipende l'applicazione di norme processuali sono oggetto di prova, né vi sono dati normativi da cui inferire l'inversione, in questo specifico ambito, della regola generale secondo cui chi afferma l'esistenza di un fatto è gravato dell'onere della relativa prova.

Muovendo dai principi appena esposti, quindi, appare ragionevole concludere che l'onere di allegare e provare i fatti da cui inferire la violazione di diritti fondamentali grava sulla difesa, quando è questa a dedurre l'inutilizzabilità o l'invalidità di atti istruttori acquisiti dall'autorità giudiziaria italiana mediante o.e.i.

8. Le precisate regole generali in tema di acquisizione ed utilizzabilità di elementi di prova acquisiti dall'autorità giudiziaria italiana mediante o.e.i., se disegnano la disciplina comune di riferimento, evidenziano anche la necessità di individuare il "tipo" di atto oggetto di richiesta e trasmissione nella singola vicenda.

Invero, è in ragione del "tipo" di atto specificamente richiesto e trasmesso che è possibile valutare la sussistenza delle condizioni di ammissibilità dell'o.e.i., e, in particolare, quella della possibilità di disporne l'assunzione «alle stesse condizioni in un caso interno analogo».

Inoltre, il "tipo" di atto richiesto costituisce un riferimento essenziale per valutare se si sia verificata una violazione dei diritti fondamentali previsti dalla

Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo.

9. Nella vicenda in esame, l'o.e.i. ha ad oggetto l'acquisizione, da parte dell'autorità giudiziaria italiana, di messaggi scambiati su *chat* di gruppo mediante un sistema cifrato, e già a disposizione dell'autorità giudiziaria francese.

Il fatto che i messaggi fossero a disposizione dell'autorità giudiziaria francese già prima della presentazione dell'o.e.i. da parte dell'autorità giudiziaria italiana costituisce elemento incontroverso: in proposito, concordano l'ordinanza impugnata, il ricorrente e il pubblico ministero, né vi sono elementi agli atti per dubitare di questo assunto.

Risulta quindi possibile un rilievo preliminare: quanto chiesto dall'autorità giudiziaria italiana, e consegnato dall'autorità giudiziaria francese, attiene a «prove già in possesso delle autorità competenti dello Stato di esecuzione» (per questa definizione cfr. art. 1, paragrafo 1, secondo periodo, Direttiva 2014/41/UE, nonché, in termini analoghi, art. 2, comma 1, lett. *a)*, d.lgs. n. 108 del 2017).

L'individuazione dell'oggetto dell'o.e.i. in «prove già in possesso delle autorità competenti dello Stato di esecuzione» ha importanti conseguenze ai fini della disciplina applicabile.

9.1. Nel sistema dell'o.e.i., l'acquisizione di «prove già in possesso delle autorità competenti dello Stato di esecuzione» è oggetto di alcune specifiche disposizioni, di deroga alla disciplina generale, e funzionali a renderne più agevole la "circolazione".

Innanzitutto, l'art. 10 Direttiva 2014/41/UE stabilisce che, nel caso di «informazioni o prove che sono già in possesso dell'autorità di esecuzione quando, in base al diritto dello Stato di esecuzione, tali informazioni o prove avrebbero potuto essere acquisite nel quadro di un procedimento penale o ai fini dell'o.e.i.», è esclusa la possibilità, per l'autorità di esecuzione, di disporre «un atto di indagine alternativo» a quello richiesto.

Dal combinato disposto degli artt. 12, paragrafo 4, e 13, paragrafo 1, Direttiva cit., poi, si evince che, quando le prove richieste mediante o.e.i. siano già in possesso dello Stato di esecuzione, la loro trasmissione allo Stato di emissione dovrebbe avvenire con immediatezza, perché non vi è alcun atto di indagine da compiere.

9.2. Nella prospettiva interna, pare risolutivo il rilievo che, nell'ordinamento giuridico italiano, la "circolazione" di prove già formate ha una disciplina specifica e diversa da quella riservata alla "formazione" di prove di identica tipologia.

Nel sistema processuale italiano, infatti, il pubblico ministero e, più in generale, la parte che vi ha interesse possono chiedere ed ottenere la disponibilità di prove già formate in un procedimento penale al fine di produrle in un altro

procedimento penale, senza necessità di alcuna autorizzazione preventiva da parte del giudice competente per quest'ultimo. Ciò anche nel caso di prove, come le intercettazioni di conversazioni o di comunicazioni, per la cui formazione è indispensabile la preventiva autorizzazione del giudice competente.

Ovviamente, resta impregiudicato il potere del giudice competente per il procedimento penale nel quale le parti intendono avvalersi delle prove già separatamente formate o acquisite in altra sede di valutare se vi siano i presupposti per ammetterle ed utilizzarle ai fini della decisione.

Questo assetto normativo si ricava con chiarezza dal sistema costituito dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen.

L'art. 238 cod. proc. pen. detta le regole generali in tema di circolazione dei verbali di prove di altri procedimenti. La disciplina in esso contenuta, che si riferisce espressamente anche agli atti non ripetibili, non prevede, ai fini dell'acquisizione delle prove formate altrove, alcun intervento preventivo da parte del giudice del procedimento nel quale si vorrebbero utilizzarle. La norma si preoccupa unicamente di fissare condizioni per l'utilizzazione di prove provenienti da altri procedimenti; e, tra queste condizioni, si ribadisce, non è ricompresa la previa autorizzazione.

L'art. 270 cod. proc. pen., a sua volta, indica i requisiti per l'utilizzazione dei risultati delle intercettazioni di conversazioni o di comunicazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte. Anche questa disciplina, speciale rispetto a quella di cui all'art. 238 cod. proc. pen. perché riferita ad uno specifico mezzo di ricerca della prova, non prevede alcun intervento autorizzativo preventivo del giudice del procedimento di "destinazione", che abbia la funzione di autorizzare le parti interessate a procedere all'acquisizione di copia dei relativi atti. L'art. 270, comma 2, cod. proc. pen., infatti, stabilisce che, ai fini della utilizzazione dei risultati di intercettazioni effettuate in procedimenti diversi, le parti interessate hanno l'onere di depositare i verbali e le registrazioni a queste relativi, senza però contenere alcun riferimento ad autorizzazioni preventive del giudice del processo di "destinazione" per ottenere la disponibilità di tali atti. Inoltre, forse ancor più significativamente, l'art. 270, comma 3, cod. proc. pen., riconosce al pubblico ministero e ai difensori delle parti interessate «la facoltà di esaminare i verbali e le registrazioni in precedenza depositati nel procedimento in cui le intercettazioni furono autorizzate», sempre senza prevedere autorizzazioni preventive del giudice del processo di "destinazione".

L'art. 78 disp. att. cod. proc. pen., rubricato «Acquisizione di atti di un procedimento penale straniero», ancora, dispone, in linea generale, al comma 1, che «[l]a documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera può essere acquisita a norma dell'art. 238 del codice», e si limita ad aggiungere, al comma 2, che, per gli atti non ripetibili compiuti dalla

polizia straniera, l'acquisizione nel fascicolo per il dibattimento è subordinata al previo esame in contraddittorio dell'autore degli stessi, o al consenso delle parti.

9.3. In considerazione di quanto precedentemente indicato, può concludersi, in linea generale, che gli atti oggetto dell'o.e.i. costituenti «prove già in possesso delle autorità competenti dello Stato di esecuzione» possono essere legittimamente richiesti e acquisiti dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si vorrebbe utilizzarli.

Ed infatti, unico presupposto di ammissibilità dell'ordine europeo di indagine, sotto il profilo del soggetto legittimato a presentarlo, è che «l'atto o gli atti di indagine richiesti nell'o.e.i. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo».

Ora, come si è rilevato in precedenza nel § 9.2, nell'ordinamento processuale penale italiano, le prove già disponibili in altri procedimenti possono essere richieste ed acquisite dalle parti interessate, e quindi anche dal pubblico ministero, al fine di utilizzarle in un altro e distinto procedimento, senza necessità di preventiva autorizzazione da parte del giudice competente per quest'ultimo.

Di conseguenza, quando l'o.e.i. avanzato dal pubblico ministero italiano riguarda «prove già in possesso delle autorità competenti dello Stato di esecuzione», non vi sono ragioni per ritenere che il medesimo debba munirsi di preventiva autorizzazione del giudice del procedimento nel quale si vorrebbe utilizzarle, siccome condizione non prevista nel nostro ordinamento, né altrimenti desumibile dal sistema dell'o.e.i.

9.4. Senza dubbio, come già segnalato in precedenza al § 9.2. in relazione alla "circolazione" di prove tra procedimenti pendenti in Italia, il giudice al quale si chiede di utilizzare le «prove già in possesso delle autorità competenti dello Stato di esecuzione», ed ottenute dal pubblico ministero mediante o.e.i., conserva integro il potere di valutare se vi siano i presupposti per ammetterle ed utilizzarle ai fini delle decisioni di sua spettanza.

Questo potere, precisamente, sarà esercitato quando il pubblico ministero presenta al giudice italiano le «prove già in possesso delle autorità competenti dello Stato di esecuzione», e ricevute tramite o.e.i. È allora, infatti, che il giudice può controllare se vi fossero le condizioni per emettere l'o.e.i., così da assicurare il pertinente diritto di "impugnazione" nello Stato di emissione previsto dall'art. 14, paragrafo 2, Direttiva 2014/41/UE, nonché se vi sia stata violazione dei diritti fondamentali riconosciuti dalla Costituzione e dalla Carta di Nizza, e, quindi, del diritto di difesa e della garanzia di un giusto processo, in linea con quanto stabilito dall'art. 14, paragrafo 7, Direttiva cit., fermo restando che l'onere dell'allegazione e della prova in ordine ai fatti da cui desumere la violazione di tali diritti grava sulla parte interessata, come già precisato nei §§ 7.2, 7.3, 7.4, 7.5 e 7.6.

10. Le osservazioni di carattere generale precedentemente compiute con riguardo alla "circolazione" delle «prove già in possesso delle autorità competenti dello Stato di esecuzione», ed acquisite dal pubblico ministero mediante o.e.i., non risolvono tutti i profili che vengono in rilievo per il giudice italiano.

Invero, ai fini della verifica sia dell'esistenza delle condizioni di ammissibilità dell'o.e.i., in particolare di quelle di cui all'art. 6, paragrafo 1, Direttiva 2014/41/UE, sia di eventuali violazioni dei diritti fondamentali, occorre prendere in esame il preciso "tipo" di atto trasmesso, attesa la specificità della disciplina riservata dalla normativa nazionale e sovra-nazionale ad alcuni di essi.

Nel presente procedimento, due sono le qualificazioni prospettate: secondo l'ordinanza impugnata, gli atti acquisiti costituiscono «documenti informatici»; secondo il ricorrente, invece, si tratterebbe di dati concernenti il traffico, l'ubicazione, e il contenuto di comunicazioni elettroniche. Entrambe le prospettazioni escludono esplicitamente che gli atti in questione costituiscano risultati di intercettazioni di conversazioni o di comunicazioni.

Le Sezioni Unite ritengono di dover prendere in esame entrambe le prospettazioni, attesa l'indisponibilità in questa sede dell'intero materiale acquisito mediante o.e.i., e tenuto conto dell'irrilevanza dell'una o dell'altra ai fini della decisione del ricorso, come si preciserà in seguito.

11. Secondo l'ordinanza impugnata, gli atti acquisiti mediante o.e.i. dall'autorità giudiziaria francese costituiscono «documenti informatici», e sicuramente non sono risultati di intercettazioni di conversazioni o comunicazioni.

11.1. La qualificazione degli atti in questione come documenti implica che il parametro generale di riferimento nel sistema processuale nazionale per verificare l'esistenza delle condizioni di ammissibilità dell'o.e.i. e l'eventuale violazione di diritti fondamentali sia costituito dall'art. 234 cod. proc. pen., il quale consente l'acquisizione di scritti o di "entità" rappresentative di fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo, salvo che non contengano informazioni sulle voci correnti nel pubblico.

Questa qualificazione non è ostacolata dalla sola circostanza che le "entità" rappresentative siano comunicazioni elettroniche, data la latitudine della nozione di "prova documentale" accolta dall'art. 234 cod. proc. pen. E in questo senso, infatti, si esprime l'orientamento ampiamente consolidato della giurisprudenza di legittimità sia con riguardo ai messaggi di posta elettronica, già trasmessi ed allocati nella memoria del dispositivo del destinatario o del mittente o nel *server* del gestore del servizio (cfr., tra le tante, Sez. 6, n. 12975 del 06/02/2020, Ceriani, Rv. 278808 – 02, e Sez. 3, n. 29426 del 16/04/2019, Moliterno, Rv. 276358 – 01), sia in ordine ai messaggi inviati mediante applicativo *WhatsApp* o *s.m.s.*, già

trasmessi e conservati nella memoria di un'utenza cellulare (v., *ex plurimis*, Sez. 6, n. 22417 del 16/03/2022, Sgromo, Rv. 283319 - 01, e Sez. 5, n. 1822 del 21/11/2017, dep. 2018, Parodi, Rv. 272319 - 01).

11.2. La disciplina generale di cui all'art. 234 cod. proc. pen., però, non sempre è esaustiva, in quanto, per alcune tipologie di documenti, sono previste regole specifiche.

In particolare, quando la prova documentale ha ad oggetto comunicazioni scambiate in modo riservato tra un numero determinato di persone, indipendentemente dal mezzo tecnico impiegato a tal fine, occorre assicurare la tutela prevista dall'art. 15 Cost. in materia di «corrispondenza».

Come infatti precisato dalla giurisprudenza costituzionale, «quello di "corrispondenza" è concetto ampiamente comprensivo, atto ad abbracciare ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza», il quale «prescinde dalle caratteristiche del mezzo tecnico utilizzato», e si estende, perciò, anche alla posta elettronica ed ai messaggi inviati tramite l'applicativo *WhatsApp*, o *s.m.s.* o sistemi simili, «del tutto assimilabili a lettere o biglietti chiusi» perché accessibili solo mediante l'uso di codici di accesso o altri meccanismi di identificazione (così Corte cost., sent. n. 170 del 2023; nello stesso senso, Corte cost., sent. n. 227 del 2023 e Corte cost., sent. n. 2 del 2023).

Di conseguenza, indipendentemente dalla modalità utilizzata, trova applicazione «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 - [...]» (cfr., ancora, testualmente, Corte cost., sent. n. 170 del 2023).

La tutela prevista dall'art. 15 Cost., tuttavia, non richiede, per la limitazione della libertà e della segretezza della corrispondenza, e, quindi, per l'acquisizione di essa ad un procedimento penale, la necessità di un provvedimento del giudice.

Invero, l'art. 15 Cost. impiega il sintagma «autorità giudiziaria», il quale indica una categoria nella quale sono inclusi sia il giudice, sia il pubblico ministero (per l'inclusione del pubblico ministero nella nozione di "autorità giudiziaria" anche nel diritto euro-unitario, cfr., proprio con riferimento alla Direttiva 2014/41/UE, Corte giustizia, 08/12/2020, Staatsanwaltschaft Wien, C-584/19).

E questa conclusione trova conferma nella disciplina del codice di rito. L'art. 254 cod. proc. pen. prevede che il sequestro di corrispondenza è disposto della «autorità giudiziaria», senza fare alcun riferimento alla necessità dell'intervento del giudice, invece espressamente richiesto, ad esempio, in relazione al sequestro da eseguire negli uffici dei difensori (art. 103 cod. proc. pen.). A sua volta, l'art. 353 cod. proc. pen. statuisce, in modo testuale, che l'acquisizione di plichi chiusi

e di corrispondenza, anche in forma elettronica o inoltrata per via telematica, è autorizzata, nel corso delle indagini, dal «pubblico ministero», il quale è titolare del potere di disporne il sequestro.

11.3. La qualificazione degli atti consegnati dall'autorità giudiziaria francese in esecuzione di o.e.i. come documenti ha specifiche conseguenze con riguardo ai presupposti di ammissibilità della loro acquisizione e alla garanzia del rispetto dei «diritti fondamentali».

In particolare, con riguardo al presupposto di ammissibilità di cui all'art. 6, paragrafo 1, lett. *b)*, Direttiva 2014/41/UE, relativo alla c.d. valutazione in astratto, è sufficiente considerare che anche l'acquisizione "originaria" della prova documentale, nel sistema processuale italiano, pur quando abbia ad oggetto "corrispondenza", per quanto appena detto nel § 11.2., può essere disposta dal pubblico ministero, con atto motivato, senza alcuna autorizzazione del giudice, salvo il caso di sequestro effettuato nell'ufficio di un difensore. Di conseguenza, se l'ordine europeo di indagine presentato dal pubblico ministero ha ad oggetto l'acquisizione di documenti e "corrispondenza" non costituenti «prove già in possesso delle autorità competenti dello Stato di esecuzione», il rispetto della condizione che esige il potere dell'autorità di emissione di disporre «l'atto o gli atti di indagine richiesti nell'o.e.i. [...] alle stesse condizioni in un caso interno analogo» è assicurato anche in assenza di una autorizzazione del giudice, salvo il caso di sequestro effettuato nell'ufficio di un difensore. A maggior ragione, quindi, e in aggiunta alle considerazioni esposte nei §§ 9.2 e 9.3, l'acquisizione di documenti, pur se relativi a "corrispondenza", quando attiene a «prove già in possesso delle autorità competenti dello Stato di esecuzione», può essere chiesta mediante o.e.i. presentato dal pubblico ministero, senza necessità di autorizzazione del giudice.

Per quanto riguarda il rispetto dei «diritti fondamentali», poi, la qualificazione degli atti consegnati dall'autorità giudiziaria francese in esecuzione di o.e.i. come documenti, specie se costituiscono "corrispondenza", comporta l'esigenza di specifica attenzione a profili "contenutistici" degli stessi. Ad esempio, un principio generale, in materia di tutela di diritto di difesa, positivizzato nel sistema italiano dall'art. 103 cod. proc. pen., è quello del divieto di sequestro e di ogni forma di controllo della «corrispondenza» tra l'imputato ed il suo difensore, salvo il fondato motivo che si tratti di corpo del reato. Resta fermo, ovviamente, che l'onere dell'allegazione e della prova in ordine ai fatti da cui desumere la violazione dei «diritti fondamentali» grava sulla parte interessata, per le ragioni indicate in precedenza nel § 7.6.

12. Secondo il ricorso, gli atti acquisiti mediante o.e.i. dall'autorità giudiziaria francese, invece, pur non costituendo risultati di intercettazioni di conversazioni o comunicazioni, attengono a dati concernenti il traffico, l'ubicazione, e il

contenuto di comunicazioni elettroniche, e, quindi, debbono essere sottoposti alla relativa disciplina, la quale richiede, come presupposti necessari per la loro acquisizione, sia la necessità degli stessi ai fini dello svolgimento di indagini per un reato «grave», sia la preventiva autorizzazione del giudice.

12.1. In forza della disciplina italiana, i dati relativi al traffico telefonico o telematico possono essere acquisiti presso il fornitore, solo se: a) sussistano sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, o di altri reati specificamente indicati; b) detti dati siano «rilevanti per l'accertamento dei fatti»; c) vi sia stata precedente autorizzazione rilasciata dal giudice con decreto motivato, ovvero il provvedimento del pubblico ministero adottato in caso di qualificata urgenza, sia stato convalidato con decreto motivato del giudice entro il termine massimo di novantasei ore (art. 132 d.lgs. 30 giugno 2003, nel testo vigente a seguito, in particolare, delle modifiche recate dall'art. 1, comma 1, d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178).

Questa disciplina è stata adottata per adeguare l'ordinamento italiano alla giurisprudenza della Corte di giustizia dell'Unione Europea. La Corte di giustizia, infatti, con pronuncia della Grande Sezione, ha affermato che l'art. 15, paragrafo 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, letto alla luce degli articoli 7, 8 e 11, nonché dell'art. 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, osta ad una normativa nazionale che: a) 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, 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; b) renda il pubblico ministero 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 (Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-706/18).

La disciplina di cui all'art. 132 d.lgs. n. 196 del 2003 non può reputarsi derogata da quella di cui all'art. 45 d.lgs. n. 108 del 2017, la quale prevede che l'o.e.i. «al fine di ottenere i dati esterni relativi al traffico telefonico o telematico nonché l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni» possa essere presentato sia dal giudice, sia dal pubblico ministero.

Invero, ritenere che il pubblico ministero abbia l'obbligo di ottenere la preventiva autorizzazione del giudice del procedimento nel quale intende utilizzare dati relativi al traffico telefonico o telematico, quando occorre richiederli ad un

gestore operante in Italia, e non anche quando sia necessario richiederli ad un gestore estero, sarebbe in contrasto con la prescrizione dell'art. 6, paragrafo 1, lett. *b)*, Direttiva 2014/41/UE, la quale esige che l'autorità di emissione abbia il potere di disporre «l'atto o gli atti di indagine richiesti nell'o.e.i. [...] alle stesse condizioni in un caso interno analogo». E in questo senso si è già espressa anche la giurisprudenza euro-unitaria, la quale ha pure precisato che «il riconoscimento da parte dell'autorità di esecuzione di un ordine europeo di indagine, emesso per l'acquisizione dei dati relativi al traffico e all'ubicazione connessi alle telecomunicazioni, non può sostituire i requisiti previsti nello stato di emissione nel caso in cui tale ordine sia stato emesso indebitamente dal pubblico ministero, quando, nell'ambito di una procedura nazionale analoga, l'adozione di un atto di indagine per l'acquisizione di dati siffatti rientra nella competenza esclusiva del giudice» (Corte giustizia, 16/12/2021, HP, C-724/19).

12.2. La disciplina che richiede la preventiva autorizzazione del giudice, però, si riferisce alla acquisizione dei dati presso il gestore dei servizi telefonici e telematici, ma non anche all'utilizzazione dei dati in un procedimento penale diverso da quello in cui sono stati già acquisiti.

L'art. 132 d.lgs. n. 196 del 2003, in effetti, come si evince da un esame combinato di tutte le sue disposizioni, fa riferimento ai dati relativi al traffico telefonico e al traffico telematico «conservati dal fornitore» (così testualmente il comma 1).

Né questa lettura dell'art. 132 cit. appare porsi in contrasto con il diritto euro-unitario. La Corte di giustizia, infatti, come già ricordato sopra, ha dichiarato che l'art. 15, paragrafo 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, letto alla luce degli articoli 7, 8 e 11, nonché dell'art. 52, paragrafo 1, della Carta dei diritti fondamentali, osta ad una normativa nazionale che renda il pubblico ministero 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 (Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-706/18). Quando, però, i dati in questione sono già stati acquisiti in un procedimento penale, non si pone più la questione dell'autorizzazione all'accesso di un'autorità pubblica, siccome gli stessi sono già a disposizione di un'autorità pubblica.

Di conseguenza, può concludersi che, nel sistema processuale italiano, il pubblico ministero può acquisire da altra autorità giudiziaria dati relativi al traffico o all'ubicazione, concernenti comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica, senza dover chiedere preventiva autorizzazione al giudice competente per il procedimento nel quale intende utilizzarli, in forza dei principi generali indicati in precedenza nel § 9.2, e in difetto di regole o principi di segno diverso nella specifica materia.

12.3. Sulla base delle osservazioni precedentemente compiute, può ritenersi che l'o.e.i. emesso dal pubblico ministero italiano avente ad oggetto l'acquisizione di dati relativi al traffico o all'ubicazione, concernenti comunicazioni elettroniche, pur se manchi una preventiva autorizzazione del giudice competente per il procedimento nel quale si intende utilizzarli, soddisfa la condizione di ammissibilità di cui all'art. 6, paragrafo 1, lett. *b)*, Direttiva 2014/41/UE.

Invero, siccome il pubblico ministero italiano può disporre l'acquisizione di dati relativi al traffico o all'ubicazione, concernenti comunicazioni elettroniche, già disponibili in altro procedimento penale pendente in Italia, senza necessità di preventiva autorizzazione del giudice competente per il procedimento nel quale intende utilizzarli, deve ritenersi che un o.e.i. formulato dal pubblico ministero italiano nel quale si chiede, senza preventiva autorizzazione del giudice nazionale, la trasmissione di dati della medesima tipologia, già acquisiti dall'autorità giudiziaria straniera in un procedimento penale pendente davanti ad essa, abbia ad oggetto atti che «avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo».

12.4. Quanto indicato nei §§ 12.1 e 12.2, poi, è utile per l'esame del tema concernente la garanzia del rispetto dei «diritti fondamentali».

In particolare, può ritenersi, anche in ragione della specifica elaborazione della giurisprudenza della Corte di giustizia, che l'originaria acquisizione presso il gestore dei servizi telefonici e telematici dei dati relativi al traffico o all'ubicazione, concernenti comunicazioni elettroniche, deve essere stata preventivamente autorizzata da un giudice o da un'autorità amministrativa indipendente non coinvolta nelle indagini e in posizione di terzietà rispetto all'esito del procedimento (Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-706/18; cfr., nello stesso senso, Corte giustizia, Grande Sezione 05/04/2022, Commissioner of An Garda Síochána, C-140/20, §§ 107, 108, 109 e 110, nonché Corte giustizia, 16/12/2021, HP, C-724/19, § 42).

Non risulta invece costituire violazione di «diritti fondamentali» l'acquisizione dei dati in questione da parte del pubblico ministero senza previa autorizzazione del giudice competente per il procedimento nel quale si intende utilizzarli, quando gli stessi siano già stati acquisiti in altro procedimento previa autorizzazione di un giudice. Invero, come si è detto in precedenza al § 12.2, in questo caso l'accesso ai dati relativi al traffico e all'ubicazione, concernenti comunicazioni elettroniche, da parte dell'autorità statuale istituzionalmente preposta a dirigere le indagini, è già avvenuto in forza del preventivo controllo di un giudice a tutela dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone interessate. Sembra significativo osservare, in proposito, che la Corte di giustizia, quando si è occupata dell'uso successivo a fini amministrativi di dati relativi al traffico e all'ubicazione, concernenti comunicazioni elettroniche, già

acquisiti ai fini della lotta alla criminalità grave, non ha segnalato il difetto di preventiva autorizzazione del giudice come profilo di criticità, sebbene, nella vicenda da essa esaminata, la trasmissione dei dati fosse rimessa alle esclusive determinazioni del pubblico ministero (cfr., per queste indicazioni, Corte giustizia, 07/09/2023, A.G., C-162/22, §§ 11, 13 e 15).

Neppure l'accesso ad un'ampia mole di dati relativi al traffico e all'ubicazione, concernenti comunicazioni elettroniche, integra, di per sé, violazione di «diritti fondamentali». In proposito, la giurisprudenza della Corte di giustizia non pone limiti quantitativi, ma, diversamente, richiede «criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione», ed indica, come accessibili, «i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere» (così Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-706/18, § 50, e Corte giustizia, Grande Sezione, 05/04/2022, Commissioner of An Garda Síochána, C-140/20, § 105).

Anche l'impossibilità, per la difesa, di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per "criptare" il contenuto delle stesse non determina, almeno in linea di principio, una violazione di «diritti fondamentali». Ed infatti, se è vero che la disponibilità dell'algoritmo di criptazione è funzionale al controllo dell'affidabilità del contenuto delle comunicazioni acquisite al procedimento, deve però osservarsi, in linea con quanto evidenziato da numerose decisioni, che il pericolo di alterazione dei dati non sussiste, salvo specifiche allegazioni di segno contrario, in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilità di decriptarlo, anche solo parzialmente (cfr., tra le tante: Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, non mass. sul punto; Sez. 6 n. 48838 dell'11/10/2023, Brunello, non mass. sul punto; Sez. 4, n. 16347 del 05/04/2023, Papalia, non mass. sul punto; Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, non mass. sul punto). D'altra parte, la giurisprudenza sovranazionale non risulta aver affermato che l'indisponibilità dell'algoritmo di decriptazione agli atti del processo costituisce, di per sé, violazione dei «diritti fondamentali». In proposito, anzi, la Corte EDU, pronunciandosi in relazione ad una vicenda in cui i dati acquisiti non erano stati messi a disposizione della difesa e la pronuncia di colpevolezza era stata fondata sul mero fatto dell'uso di un sistema di messaggistica criptata denominato *ByLock*, si è limitata ad affermare che dare al ricorrente l'opportunità di prendere conoscenza del materiale decriptato nei suoi confronti poteva costituire un passo importante per preservare i suoi diritti di difesa senza avere, al contempo, affermato che tale mancata messa a disposizione integrasse un *vulnus* dei diritti

fondamentali (Corte EDU, Grande Camera, 26/09/2023, Yüksel Yalçinkaya c. Turchia, § 336; il testo originale è il seguente: «*The Court is accordingly of the view that giving the applicant the opportunity to acquaint himself with the decrypted ByLock material in his regard would have constituted an important step in preserving his defence rights*»).

In ogni caso, poi, resta fermo che l'onere dell'allegazione e della prova dei fatti da cui desumere la violazione dei «diritti fondamentali» grava sulla parte interessata, per le ragioni indicate in precedenza nel § 7.6.

13. In considerazione delle argomentazioni fin qui esposte, vanno affermati i seguenti principi di diritto:

"*La trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non rientra nell'ambito di applicazione dell'art. 234-bis cod. proc. pen., che opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie, bensì nella disciplina relativa alla circolazione delle prove tra procedimenti penali, quale desumibile dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen.*".

"*In materia di ordine europeo di indagine, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle*".

"*L'emissione, da parte del pubblico ministero, di ordine europeo di indagine diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria a norma dell'art. 6 Direttiva 2014/41/UE, perché tale autorizzazione, nella disciplina nazionale relativa alla circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento*".

"*La disciplina di cui all'art. 132 d.lgs. n. 196 del 2003, relativa all'acquisizione dei dati concernenti il traffico di comunicazioni elettroniche e l'ubicazione dei dispositivi utilizzati, si applica alle richieste rivolte ai fornitori del servizio, ma non anche a quelle dirette ad altra autorità giudiziaria che già detenga tali dati, sicché, in questo caso, il pubblico ministero può legittimamente accedere agli stessi senza chiedere preventiva autorizzazione al giudice davanti al quale intende utilizzarli*".

"*L'utilizzabilità del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, e trasmesse sulla base di ordine*

europeo di indagine, deve essere esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali, fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata".

"L'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse non determina una violazione dei diritti fondamentali, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente".

14. Sulla base dei principi di diritto enunciati, è possibile esaminare l'oggetto del ricorso rimesso all'esame delle Sezioni Unite.

15. Complessivamente infondate sono le censure formulate nel primo, nel secondo e nel quarto motivo di ricorso, nonché nei due motivi nuovi, con le quali si contesta l'utilizzabilità dei dati informatici relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc.

In sintesi, le censure indicate deducono l'inapplicabilità della disciplina di cui all'art. 234-*bis* cod. proc. pen., la mancata acquisizione degli originali dei *file* rappresentativi delle comunicazioni e delle chiavi di decifrazione, il difetto dei presupposti per l'emissione di un o.e.i., in particolare per la mancanza di un preventivo provvedimento del giudice italiano, la violazione dei principi fondamentali, anche per il carattere generalizzato ed indifferenziato delle attività di captazione e di apprensione dei dati effettuata dall'autorità estera.

15.1. Il Collegio condivide la tesi della inapplicabilità della disposizione di cui all'art. 234-*bis* cod. proc. pen. in materia di acquisizione ed utilizzabilità dei dati relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, perché si tratta, come già detto sopra nei §§ 6, 6.1 e 6.2, di disciplina alternativa, e, quindi, incompatibile con quella relativa al sistema dell'o.e.i.

Tuttavia, questo assunto non rende illegittima l'acquisizione, né preclude l'utilizzabilità dei dati relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, ottenuti dall'autorità giudiziaria francese in esecuzione di o.e.i. emesso dal pubblico ministero italiano. Invero, l'errore di qualificazione in cui è incorsa l'ordinanza impugnata non determina l'annullamento della stessa, sulla base di quanto previsto dall'art. 619, comma 1, cod. proc. pen: l'errore rilevato, precisamente, non ha avuto influenza decisiva sul dispositivo, in quanto, nella specie, sussistono le condizioni di ammissibilità necessarie per emettere legittimamente l'o.e.i. e non risultano violazioni dei diritti fondamentali.

15.2. La condizione di ammissibilità, posta dall'art. 6, paragrafo 1, lett. *b)*, Direttiva 2014/41/UE, la quale richiede che l'atto o gli atti richiesti «avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo», può ritenersi soddisfatta.

Invero, i dati ricevuti dall'autorità giudiziaria francese in esecuzione di o.e.i. emesso dal pubblico ministero italiano, per quanto è desumibile dal contenuto dell'ordinanza impugnata, non contestata sul punto dal ricorso, costituiscono «prove già in possesso delle autorità competenti dello Stato di esecuzione», perché acquisite nell'ambito di un procedimento penale pendente in quello Stato (cfr., in particolare, pag. 33 dell'ordinanza impugnata).

Ora, secondo i principi di diritto precedentemente enunciati, l'emissione, da parte del pubblico ministero, di o.e.i. diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, non deve essere preceduta da autorizzazione del giudice italiano, perché tale autorizzazione non è richiesta, nell'ordinamento italiano, per l'acquisizione del contenuto di comunicazioni telefoniche già acquisite in altro procedimento, eventualmente anche se, a norma dell'art. 132 d.lgs. n. 196 del 2003, presso i gestori di servizi telefonici o telematici.

15.3. Pure l'altra condizione di ammissibilità, quella relativa alla necessità e proporzione dell'o.e.i., è rispettata.

Si è detto in precedenza, al § 7.2, che l'esame di tale profilo deve essere compiuto avendo riguardo al procedimento nel cui ambito è emesso l'ordine europeo di indagine. Nella specie, nessuna precisa questione risulta posta in relazione a questo aspetto; in ogni caso, l'ordinanza impugnata evidenzia che l'o.e.i. è stato emesso dopo l'acquisizione di precisi elementi a carico di Marsel Hajri per il reato di partecipazione ad associazione per delinquere finalizzata al narcotraffico, in qualità di capo e promotore, e con specifico riferimento ai soli dati ed alle sole comunicazioni già intercorse relativi ad uno *smartphone* del tipo utilizzato per l'accesso al *network* Sky-Ecc e rinvenuto nell'abitazione del medesimo (cfr., in particolare, pagg. 33 e 34 dell'ordinanza impugnata).

15.4. Non può neppure dirsi che, nel presente procedimento, sia stata accertata la violazione dei diritti fondamentali, così come sostenuto nel ricorso.

Innanzitutto, non è nemmeno allegato che i dati trasmessi dall'autorità giudiziaria francese siano stati acquisiti nel procedimento penale pendente davanti ad essa in difetto di un provvedimento autorizzativo di un giudice.

In secondo luogo, l'ordinanza impugnata rappresenta che l'acquisizione dei dati relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc è stata effettuata dall'autorità giudiziaria estera in relazione ad indagini concernenti, in particolare, il narcotraffico (cfr., specificamente, pag. 33 dell'ordinanza

impugnata); e i fatti per i quali la stessa è stata adottata si riferiscono proprio al narcotraffico e ad un'associazione a tal fine costituita.

In terzo luogo, l'affermazione difensiva secondo cui l'autorità estera avrebbe effettuato attività di captazione e di apprensione dei dati in modo generalizzato ed indifferenziato è meramente assertiva ed aspecifica e, in quanto tale, inidonea a soddisfare gli oneri di allegazione e di prova dei fatti dai quali inferire che l'accesso a tali dati da parte dell'autorità giudiziaria francese sia avvenuto in modo arbitrario, o in radicale difetto dei presupposti necessari.

In quarto luogo, le modalità di consegna dei *file* relativi alle comunicazioni, siccome trasfusi in una consulenza tecnica avente ad oggetto la loro decrittazione, e l'indisponibilità delle chiavi di cifratura necessarie per renderle intelligibili non sono circostanze relative all'acquisibilità o all'utilizzabilità di tale tipologia di elementi, ma attengono alla verifica di affidabilità di questi ultimi e del loro contenuto. Come già indicato in precedenza al § 12.4, la asserita alterazione dei dati è stata unicamente ipotizzata dal ricorrente, che non ha né allegato, né provato elementi utili a rendere concreta tale evenienza.

16. Per le ragioni precedentemente esposte, deve escludersi anche la necessità di formulare alla Corte di giustizia dell'Unione Europea i quesiti prospettati dalla difesa, ovvero di sollevare questione di legittimità costituzionale.

Invero, i dati oggetto dell'o.e.i. contestato: a) sono stati acquisiti dall'autorità francese nell'ambito di indagini concernenti un traffico internazionale di stupefacenti e sono stati successivamente trasmessi all'autorità italiana in relazione ad un procedimento concernente un'associazione per delinquere finalizzata al narcotraffico; b) sono stati richiesti ed ottenuti mediante o.e.i. dall'autorità giudiziaria italiana competente ad acquisirli «alle stesse condizioni in un caso interno analogo», in applicazione della disciplina sulla "circolazione" delle prove.

Di conseguenza, nella vicenda in esame, non si pongono problemi né di acquisizione di dati elettronici relativi al traffico, all'ubicazione o al contenuto di comunicazioni già in possesso della autorità di esecuzione, al di fuori di procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, né di mancato rispetto delle condizioni previste dall'art. 6 Direttiva 2014/41/UE.

Deve pertanto escludersi che ricorrano ragionevoli dubbi in ordine alla interpretazione del diritto dell'Unione Europea concretamente applicabile nel caso in esame, e che, quindi, sussista l'obbligo di rinvio pregiudiziale alla Corte di giustizia U.E. (cfr., in questo senso, Corte giustizia, Grande Sezione, 06/10/2021, Consorzio Italian Management, C-561/19, ma già Corte giustizia, 06/10/1982, s.r.l Cilfit e Lanificio di Gavarso s.p.a., C-283/81).

17. Diverse da quelle consentite in sede di legittimità sono le censure esposte nel terzo motivo, che contestano l'affermazione della sussistenza dei gravi indizi di colpevolezza in ordine alla partecipazione dell'attuale ricorrente all'associazione per delinquere finalizzata al traffico di stupefacenti diretta da Marsel Hajri e da Gerti Hajri, deducendo l'equivocità degli elementi valorizzati a tal fine.

17.1. L'ordinanza impugnata ricostruisce l'esistenza dell'associazione per delinquere di cui all'art. 74 d.P.R. n. 309 del 1990 indicando l'organigramma del gruppo, i quantitativi di sostanze stupefacenti trattati, e diversi reati fine.

Il Tribunale, in particolare, rappresenta che il vertice dell'illecito sodalizio è costituito dai fratelli Marsel Hajri e Gerti Hajri, il primo operante in Italia ed il secondo in Albania, i quali si occuperebbero di sovraintendere al reperimento di eroina, cocaina, hashish e marijuana in Albania, al trasporto di tali sostanze in Italia ed al rifornimento degli organizzatori delle singole piazze di spaccio, attive, in particolare, ad Altamura, San Cataldo di Lecce e Frigole.

Segnala, poi, che il gruppo si avvarrebbe del contributo di più persone, tra le quali sono indicati Anxhela Balla ed Ervis Balla, rispettivamente sorella e cognato dei fratelli Hajri, addetti alla riscossione dei corrispettivi delle vendite, alla contabilità e ai rapporti con gli organizzatori delle piazze di spaccio, nonché Myrteza Balliu e Kleidi Musaku, quali corrieri e "chimici". Precisa che Kleidi Musaku, in occasione delle perquisizioni e dei sequestri del 30 marzo 2023, è risultato disporre di ingenti quantitativi di eroina e di marijuana e di un "laboratorio", in cui vi erano, tra l'altro, bilancine di precisione, attrezzi da taglio, una maschera con filtri e un motore di maceratore/frullatore industriale.

Espone, ancora, che, sulla base di quanto emerge dalle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, il gruppo criminale, nel solo periodo compreso tra il 12 dicembre 2019 e l'8 marzo 2021, avrebbe trattato 526,5 kg. di droga, cedendone 142,5 kg. a terzi e praticando prezzi pari a 44.250,00 euro al kg. per la cocaina, a 20.000,00 euro al kg. per l'eroina e 3.575,00 euro al kg. per marijuana e hashish.

Evidenzia, altresì, che l'organizzazione illecita si servirebbe, come base operativa per lo svolgimento di riunioni, per il riciclaggio di denaro e per il deposito della droga, dell'azienda agricola dell'attuale ricorrente Ermal Gjuzi.

17.2. L'ordinanza impugnata afferma, sulla base di specifici elementi, che sussistono gravi indizi di colpevolezza nei confronti di Ermal Gjuzi quale partecipe dell'associazione finalizzata al narcotraffico di cui si è appena detto, sulla base anche della messa a disposizione della sua azienda agricola per le riunioni del gruppo criminale e per la custodia dello stupefacente. In tal modo, avrebbe assicurato una "copertura" ad esponenti del sodalizio, assumendoli come

braccianti agricoli, e sarebbe concorso nel reimpiego dei proventi dei traffici illeciti dell'organizzazione.

A tal fine, innanzitutto, rappresenta che Ermal Gjuzi, in data 19 giugno 2020, ha consegnato la somma in contanti di 150.000,00 euro ad un agente sotto copertura, in funzione dell'acquisto di una partita di cocaina proveniente dal Sud America, ottenendo, quale ricevuta della consegna, una banconota di 5 euro. Segnala che questa condotta è significativa sia perché, lo stesso giorno, i fratelli Hajri, mediante comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, si sono scambiati diverse fotografie di denaro impacchettato in quindici mazzette da 10.000,00 euro ciascuna, nonché del numero seriale della banconota da 5 euro utilizzata come ricevuta, sia perché, per quanto emerso dall'attività di osservazione svolta dalla polizia giudiziaria, Marsel Hajri, nei giorni precedenti, aveva incassato somme di denaro riconducibili all'attività di spaccio.

L'ordinanza impugnata, poi, segnala che Ermal Gjuzi ha assunto come braccianti agricoli presso la sua azienda agricola sia Marsel Hajri, capo del gruppo criminale, sia Myrteza Balliu, altro membro della consorteria, e, in data 15 marzo 2021, dopo essere stato contattato dai Carabinieri della Stazione territorialmente competente, è stato oggetto di una comunicazione intercorsa attraverso il sistema criptato Sky-Ecc tra i due fratelli Marsel e Gerti Hajri, i quali hanno commentato una fuga di notizia relativa allo stesso.

Il medesimo provvedimento, ancora, rileva che, mediante conversazioni intercorse attraverso il sistema criptato Sky-Ecc tra Marsel Hajri e Gerti Hajri tra il 3 ed il 12 aprile 2020, nonché tra Marsel Hajri ed Ervis Gjuzi tra il 6 e l'8 agosto 2020, sono state scambiate fotografie documentanti l'utilizzo di terreni, di teli di plastica neri e di serre di fragole riferibili all'azienda dell'attuale ricorrente Ermal Gjuzi quali luoghi e mezzi per il deposito di sostanza stupefacente.

Il Tribunale del riesame, infine, segnala che, dopo l'arresto di Kleidi Musaku, avvenuto nel tardo pomeriggio del 30 marzo 2023, all'esito di perquisizioni e sequestri che avevano fatto rinvenire nella disponibilità di costui 32 panetti di eroina per complessivi 15,30 kg., 5 kg. di marijuana ed un laboratorio dotato di diversi attrezzi da taglio, Marsel Hajri, Gerti Hajri, Myrteza Balliu e l'attuale ricorrente Ermal Gjuzi, in piena notte, si sono recati nei terreni dove erano installate le serre di fragole dell'azienda di quest'ultimo. Precisa che la riunione deve ritenersi avere avuto un oggetto illecito, per la sua stretta conseguenzialità con l'arresto di Kleidi Musaku, e che la giustificazione fornita dagli indagati in proposito, ossia la riparazione della recinzione danneggiata dai cinghiali, non è stata supportata da alcun elemento di riscontro. L'ordinanza impugnata evidenzia, altresì, che Kleidi Musaku è il fratello della convivente di Myrteza Balliu, e, sulla base di risultanze di intercettazioni tra presenti, in data 6 marzo 2023, avrebbe cooperato con quest'ultimo nel caricare, trasportare e consegnare al gestore di

una piazza di spaccio 20 pezzi di eroina per complessivi 10 kg., e nell'incassare il relativo prezzo (cfr. pagg. 112-113 dell'ordinanza impugnata).

17.3. Ciò posto, le censure formulate nel motivo di ricorso in esame, più che denunciare vizi logico-giuridici, tendono ad ottenere una diversa valutazione delle risultanze acquisite.

I rilievi formulati, infatti, deducono che non vi sarebbero elementi idonei a dimostrare la consapevolezza di Ermal Gjuzi in ordine alla illiceità della provenienza o della destinazione del denaro consegnato all'agente sotto copertura, e neppure la riferibilità al medesimo della materiale attività di dazione della somma, ovvero che le conversazioni acquisite sono poco significative, perché non offrono certezze sulla presenza di droga nell'azienda agricola dell'attuale ricorrente, e comunque sono intercorse tra altre persone, ovvero ancora che la sua partecipazione al "sopralluogo" notturno nei terreni della ditta da lui gestita costituisce un dato neutro. In altri termini, detti rilievi non evidenziano violazioni di norme giuridiche, manifeste illogicità, contraddittorietà o lacune nell'attività di ricostruzione del quadro gravemente indiziario nell'ordinanza impugnata, e, quindi, si traducono nella mera prospettazione di una interpretazione alternativa degli elementi acquisiti, diversa da quella accolta dal Tribunale del riesame, e non consentita in sede di legittimità (cfr., per l'inammissibilità delle censure che, pur investendo formalmente la motivazione dell'ordinanza del tribunale del riesame, si risolvono nella prospettazione di una diversa valutazione di circostanze già esaminate dal giudice di merito, tra le tantissime, Sez. 2, n. 27866 del 17/06/2019, Mazzelli, Rv. 276976 - 01, e Sez. fer., n. 47748 dell'11/08/2014, Contarini, Rv. 261400 - 01).

18. Alla complessiva infondatezza delle censure seguono il rigetto del ricorso e la condanna del ricorrente al pagamento delle spese processuali, a norma dell'art. 616 cod. proc. pen.

P.Q.M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese processuali. Manda alla cancelleria per gli adempimenti di cui all'art. 94, comma 1-*ter*, disp. att. cod. proc. pen.

Così deciso il 29/02/2024.

Il Componente estensore
Antonio Corbo

La Presidente
Margherita Cassano

SEZIONI UNITE PENALI
Depositato in cancelleria
Roma, il 14 GIU. 2024
IL FUNZIONARIO GIUDIZIARIO
Rosa Maria D'Amore