23756-24

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

SEZIONI UNITE PENALI

Composta da

Margherita Cassano	- Presidente -	Sent. n. sez. 4
Maria Vessichelli		CC – 29/02/2024
Francesco Maria Ciampi		R.G.N. 41618/2023
Gastone Andreazza		
Giovanna Verga		
Filippo Casa		
Ercole Aprile		
Angelo Caputo		
Antonio Corbo	- Relatore -	

ha pronunciato la seguente

SENTENZA

sui ricorsi proposti da

1. [redacted]
2. [redacted]

avverso l'ordinanza del 21/07/2023 del Tribunale di Reggio Calabria

visti gli atti, il provvedimento impugnato e il ricorso;
udita la relazione svolta dal componente Antonio Corbo;
udito il Pubblico Ministero, in persona dell'Avvocato generale Pietro Gaeta, che ha concluso chiedendo il rigetto del ricorso;
uditi, per i ricorrenti, gli Avvocati [redacted] difensore di [redacted] e [redacted] difensore di [redacted] i quali hanno concluso chiedendo l'accoglimento dei rispettivi ricorsi, nonché l'Avvocato [redacted] difensore di entrambi, il quale ha concluso chiedendo l'accoglimento dei ricorsi, in subordine la rimessione alla Corte di giustizia, ai fini dell'interpretazione e dell'applicazione dell'art. 31 Direttiva 2014/41/UE e degli artt. 47 Carta di Nizza e

13 e 6 CEDU, nonché, in estremo subordine, il rinvio al giudice del merito per disporre una perizia diretta ad assicurare in contraddittorio gli esiti del processo di decriptazione, analisi e selezione delle conversazioni acquisite mediante o.e.i.

RITENUTO IN FATTO

1. Con ordinanza emessa in data 21 luglio 2023, il Tribunale di Reggio Calabria, ha rigettato le istanze di riesame proposte nell'interesse di [redacted] e [redacted] avverso l'ordinanza del G.i.p. del Tribunale di Reggio Calabria che ha applicato loro la misura cautelare della custodia in carcere per i reati di cui agli artt. 73 e 74 d.P.R. n. 309 del 1990.

Secondo l'ordinanza impugnata, sussisterebbero gravi indizi di colpevolezza a carico di [redacted] in ordine sia alla loro partecipazione ad un'associazione per delinquere finalizzata al traffico di cocaina importata dal Sudamerica, il primo nella qualità di organizzatore e di finanziatore, e il secondo come partecipe, sia al loro concorso in numerosi episodi di acquisto, detenzione, importazione e cessione di partite della precisata sostanza stupefacente. Ai fini dell'individuazione dei gravi indizi di colpevolezza, l'ordinanza impugnata ha richiamato anche elementi costituiti da comunicazioni intercorse sulla rete criptata [redacted] acquisiti mediante ordine europeo di indagine (d'ora in avanti, o.e.i.) eseguito dall'autorità giudiziaria della Repubblica di Francia.

2. Hanno presentato ricorso per cassazione avverso l'ordinanza indicata in epigrafe [redacted] con un unico atto sottoscritto dagli avvocati [redacted] articolando sei motivi, preceduti da un'ampia premessa, e seguiti dalla proposizione, in via subordinata, di una questione pregiudiziale *ex* art. 267 T.F.U.E.

Nella premessa, si fornisce un quadro informativo sulla genesi delle indagini e sulla evoluzione del procedimento nel cui ambito sono state emesse le ordinanze custodiali a carico dei ricorrenti, e si affronta il tema della natura delle attività di acquisizione delle comunicazioni effettuate mediante il sistema [redacted] elementi decisivi per ritenere la sussistenza dei gravi indizi di colpevolezza.

2.1. Con il primo motivo, relativo al solo [redacted] si denuncia violazione di legge, con riferimento agli artt. 24 e 111 Cost., 178, lett. *c)*, 291, 293, comma 3, e 294 cod. proc. pen., nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *c)* ed *e)*, cod. proc. pen., avendo riguardo alla impossibilità per la difesa di conoscere le modalità di acquisizione e decriptazione dei messaggi scambiati sul sistema [redacted]

Si deduce che l'impossibilità di conoscere le modalità di acquisizione e decriptazione dei messaggi scambiati sul sistema [redacted] integra una nullità di

ordine generale per violazione del diritto di difesa, prontamente eccepita in sede di interrogatorio di garanzia davanti al G.i.p. Si rappresenta che la mancata acquisizione dei provvedimenti del Tribunale di Lille, i quali hanno autorizzato le intercettazioni delle comunicazioni intercorrenti sul sistema [redacted] dal 14 giugno 2019, e dei provvedimenti del Tribunale di Parigi, i quali hanno autorizzato l'installazione dei captatori informatici per acquisire le chiavi di cifratura interne ai singoli dispositivi mobili in uso agli utenti, ha impedito alla difesa di comprendere il tipo di attività investigativa svolta e, quindi, di articolare eccezioni in ordine alla validità ed utilizzabilità delle risultanze della stessa. Si precisa che l'osservazione dell'ordinanza impugnata, secondo la quale il provvedimento autorizzativo del Tribunale di Lille del 14 giugno 2019 è stato depositato in altro procedimento, è inadeguata, perché fa riferimento alla produzione operata in altro procedimento, ed è comunque parziale, perché nulla dice con riguardo ai provvedimenti emessi dal Tribunale di Parigi. Si aggiunge che la presunzione di legittimità degli atti procedimentali compiuti all'estero è relativa e non assoluta.

2.2. Con il secondo motivo, riferito ad entrambi i ricorrenti, si denuncia violazione di legge, con riferimento agli artt. 407, commi 2 e 3, e 178, lett. *c)*, cod. proc. pen., nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *c)* ed *e)*, cod. proc. pen., avendo riguardo alla inutilizzabilità degli atti acquisiti mediante o.e.i., per il superamento del termine massimo delle indagini.

Si deduce che i termini massimi per lo svolgimento delle indagini, al momento dell'acquisizione delle conversazioni intercorse sul sistema [redacted] erano ormai decorsi in relazione ad entrambi i ricorrenti. Si premette che la mancata definizione del proc. n. 1589/19 R.G.N.R. DDA Reggio Calabria, dal quale è stato separato il proc. n. 3886/22 R.G.N.R. DDA Reggio Calabria, nel cui ambito sono state adottate le misure cautelari a carico dei due attuali ricorrenti, impedisce di ricostruire con precisione l'evoluzione delle indagini a carico degli stessi. Si osserva poi che il proc. n. 1589/19 R.G.N.R. DDA Reggio Calabria è sicuramente in quiescenza, in quanto il R.O.S. ha depositato l'informativa finale in data 15 settembre 2022, e che, quindi, non vi sarebbero stati ostacoli per il Tribunale del riesame a disporre accertamenti in ordine ad esso. Si aggiunge che elementi dai quali desumere l'esistenza di risalenti notizie di reato a carico dei due ricorrenti sono costituiti, in particolare, dalla sottoposizione di un'utenza telefonica in uso a [redacted] ad intercettazioni tra l'8 agosto 2020 ed il 30 maggio 2022, e da una conversazione tra presenti intercettata il 2 maggio 2021 tra [redacted] consuocero di [redacted] Si osserva, ancora, che la strumentale intempestività della iscrizione del nome di una persona nel registro degli indagati integra una violazione della disposizione di cui all'art. 407 cod. proc. pen. ed è, come tale sanzionabile, anche per i procedimenti anteriori all'entrata in vigore dell'art. 335-*quater* cod. proc. pen.

2.3. Con il terzo motivo, riferito ad entrambi i ricorrenti, si denuncia violazione di legge, con riferimento agli artt. 273, 192, 292, 125, comma 3, cod. proc. pen. e 73 e 74 d.P.R. n. 309 del 1990, nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *b)*, *c)* ed e), cod. proc. pen., avendo riguardo alla individuazione della natura delle attività di acquisizione delle comunicazioni intercorse sul sistema [redacted]

Si deduce che illegittimamente l'ordinanza impugnata qualifica l'attività di acquisizione delle comunicazioni intercorse sul sistema [redacted] come attività di recupero di dati presenti nella memoria dei due *server* utilizzati dalla società [redacted] ubicati in [redacted] Si rileva che tale conclusione è viziata in particolare sia perché non risponde alle specifiche censure della difesa, le quali avevano evidenziato come le conversazioni non si trovassero nella memoria dei precisati *server*, sia perché si pone in contrasto con l'informativa del R.O.S. del 15 settembre 2022, secondo la quale detti *server* hanno conservato al loro interno esclusivamente i dati della prima e dell'ultima utilizzazione di ciascun apparecchio abilitato a connettersi al sistema [redacted] In premessa, si precisa analiticamente che le comunicazioni trasmesse dall'autorità giudiziaria francese sono risultanze di intercettazioni, perché: a) le operazioni di acquisizione delle comunicazioni si sono caratterizzate per l'attivazione di *Trojan Horse malaware* per un periodo di ben quattro mesi, come risulta dall'autorizzazione del Tribunale di Parigi; b) l'attività è stata autorizzata sulla base dell'art. 706-102-1 del *Code de Procedure Penale*, il quale regola l'impiego del *Trojan Horse malaware*; c) i *server* ubicati in [redacted] utilizzati come "nodo" di transito delle comunicazioni, secondo quanto emerge dai provvedimenti autorizzativi emessi dal Giudice istruttore del Tribunale di Lille, hanno conservato al loro interno esclusivamente i dati della prima e dell'ultima utilizzazione di ciascun apparecchio abilitato a connettersi al sistema [redacted]

2.4. Con il quarto motivo, riferito ad entrambi i ricorrenti, si denuncia violazione di legge, con riferimento agli artt. 234-*bis* e 191 cod. proc. pen., 32 Convenzione di Budapest, e Direttiva 2014/41/UE, nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *c)* ed *e)*, cod. proc. pen., avendo riguardo alla ritenuta applicabilità della disciplina di cui all'art. 234-*bis* cod. proc. pen.

Si deduce che illegittimamente l'ordinanza impugnata ha ritenuto gli atti trasmessi dall'autorità giudiziaria francese acquisibili *ex* art. 234-*bis* cod. proc. pen. Si osserva che la disciplina di cui all'art. 234-*bis* cod. proc. pen. è non solo alternativa a quella dell'o.e.i., ma, soprattutto, inapplicabile nella specie, in quanto gli atti acquisiti costituiscono le risultanze di attività di intercettazione, come evidenziano con chiarezza i provvedimenti autorizzativi del Tribunale di Lille. Si aggiunge, ancora, che gli atti acquisiti costituiscono corrispondenza, in quanto questa, come ha precisato la giurisprudenza costituzionale (si cita Corte cost.,

sent. n. 170 del 2023), non perde tale qualità solo perché ha raggiunto il recapito del destinatario.

2.5. Con il quinto motivo, riferito ad entrambi i ricorrenti, si denuncia violazione di legge, con riferimento agli artt. 234-*bis*, 270, 268, commi 6, 7 e 8, 191 cod. proc. pen., 6, paragrafo 1, lett. *a)* e *b)*, e 10, paragrafo 5, Direttiva 2014/41/UE, e 8, paragrafo 2, CEDU, nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *b)*, *c)* ed *e)*, cod. proc. pen., avendo riguardo alla ritenuta utilizzabilità delle comunicazioni intercorse sul sistema [redacted]

Si deduce, in primo luogo, che gli o.e.i. aventi ad oggetto la richiesta di acquisire le comunicazioni intercorse sul sistema [redacted] sono illegittimi, con conseguente inutilizzabilità di quanto ottenuto, perché emessi in violazione dell'art. 6, paragrafo 1, lett. *a)* e *b)*, Direttiva 2014/41/UE, siccome si riferiscono ad atti che mai avrebbero potuto essere compiuti in Italia. Si segnala, precisamente, che le attività di intercettazione compiute in Francia non avrebbero mai potuto aver luogo in Italia, in quanto massivamente ed indiscriminatamente riferite a tutte le comunicazioni scambiate mediante il sistema [redacted]. Si osserva che il principio di proporzionalità, enunciato dall'art. 6, paragrafo 1, lett. *a)*, Direttiva cit., nella specie, deve essere riferito: 1) alle modalità attraverso cui sono state acquisite nel quadro del procedimento francese le prove oggetto dell'o.e.i., caratterizzate da intercettazioni eseguite in modo generalizzato e indiscriminato nei confronti di tutti gli utenti di una determinata piattaforma di telecomunicazioni; 2) alla richiesta di o.e.i. delle autorità italiane, aventi ad oggetto il trasferimento dei dati relativi a tutti gli indirizzi degli utilizzatori del sistema [redacted] in Italia. Si rileva, poi, che vi è stata violazione del principio di cui all'art. 6, paragrafo 1, lett. *b)*, perché gli atti istruttori richiesti: a) non avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo, in quanto costituiti da intercettazioni eseguite in modo generalizzato e indiscriminato nei confronti di tutti gli utenti di una determinata piattaforma di telecomunicazioni; b) non sono stati acquisiti nel rispetto delle garanzie procedimentali di cui all'art. 268, commi 6, 7 e 8 cod. proc. pen., in quanto alla difesa non sono stati messi a disposizione gli elementi per conoscere le modalità di acquisizione delle comunicazioni scambiate mediante il sistema [redacted] e per verificare la corrispondenza dei testi acquisiti in originale e dei testi decodificati, nonché la coincidenza delle utenze dei soggetti identificati come mittenti e destinatari. Si segnala che l'effettuazione di intercettazioni in modo generalizzato ed indiscriminato è vietata anche dall'ordinamento dell'Unione Europea, come precisato dalla Corte di giustizia UE (si citano, in particolare, Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-746/18, e Corte giustizia, Grande Sezione, 20/09/2022, VD e SR, C-793/19 e C-794/19), e che, secondo un principio dell'ordinamento euro-unitario, informazioni ed elementi di prova ottenuti in modo illegittimo non debbono arrecare indebiti pregiudizi ad un

imputato o ad un indagato (si citano numerose decisioni della Corte di giustizia UE).

Si deduce, in secondo luogo, che gli o.e.i. aventi ad oggetto la richiesta di acquisire le comunicazioni intercorse sul sistema [redacted] sono illegittimi, con conseguente inutilizzabilità di quanto ottenuto, perché emessi in violazione dell'art. 9, paragrafo 1, Direttiva 2014/41/UE, siccome riguardano atti che non avrebbero potuto essere compiuti dall'autorità giudiziaria francese. Si segnala che le comunicazioni intercorse sul sistema [redacted] siccome costituiscono il risultato di intercettazioni, in Italia sarebbero acquisibili a norma dell'art. 270 cod. proc. pen., e che, però, la Francia non ha disposizione analoga. Si aggiunge che la libera trasmigrabilità di risultanze di attività di intercettazione da un procedimento penale ad un altro è stata ritenuta dalla Corte EDU, proprio con riferimento alla Francia, integrare una violazione dell'art. 8, paragrafo 2, CEDU (si cita Corte EDU, 29/03/2005, Matheron c. Francia).

2.6. Con il sesto motivo, riferito ad entrambi i ricorrenti, si denuncia violazione di legge, con riferimento agli artt. 234-*bis*, 189, 191 cod. proc. pen., 6, paragrafo 1, lett. *a)* e *b)*, Direttiva 2014/41/UE, 8, paragrafo 2, CEDU, 11, 14 e 117, primo comma, Cost., e 7 Carta dei diritti fondamentali dell'Unione Europea, nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. *b)*, *c)* ed *e)*, cod. proc. pen., avendo riguardo alla ritenuta utilizzabilità delle comunicazioni intercorse sul sistema [redacted]

Si deduce che gli o.e.i. aventi ad oggetto la richiesta di acquisire le comunicazioni intercorse sul sistema [redacted] sono illegittimi, con conseguente inutilizzabilità di quanto ottenuto, perché emessi in violazione dell'art. 189 cod. proc. pen., siccome attengono necessariamente anche alle attività di captazione informatica disposte al solo fine di acquisire le chiavi di cifratura custodite nei dispositivi dei singoli utenti. Si premette che la impermeabilità delle comunicazioni transitanti sul sistema [redacted] si fonda sulla presenza di quattro chiavi di cifratura, due presenti nei *server* di [redacted] e due presenti all'interno di ciascun dispositivo individuale, e che i captatori informatici installati sui *server* di [redacted] hanno avuto esclusivamente la funzione di "catturare" le chiavi di cifratura presenti all'interno del dispositivo di ciascun utente, mediante l'invio di una notifica *push* al singolo apparecchio, con la quale si induceva lo stesso, quando si autenticava sul sistema [redacted] a trasmettere le chiavi di cifratura presenti al loro interno. Si precisa che questa tipologia di attività investigativa è diversa da quelle di intercettazione, perché i captatori informatici diretti ad acquisire le chiavi di cifratura presenti all'interno dei singoli dispositivi mobili non hanno captato comunicazioni, e, quindi, attraverso di essi si è proceduto ad attivare un mezzo di ricerca della prova atipico. Si osserva che questo mezzo di ricerca della prova atipico è in contrasto con la riserva di legge, garantita dagli artt. 14 Cost., 8, paragrafo 2, CEDU, e 7 Carta dei

diritti fondamentali dell'Unione Europea, e che, quindi, sono inutilizzabili gli algoritmi di decodifica delle conversazioni intercorse sul sistema [redacted]

2.7. In via subordinata, si chiede alla Corte di cassazione di formulare alla Corte di giustizia dell'Unione Europea le seguenti questioni pregiudiziali.

1) Sull'interpretazione dell'art. 6, par. 1, lett. *a)*, della Direttiva 2014/41/UE:

a) se l'art. 6, par. 1, lett. *a)*, della Direttiva 2014/41/UE osti a un o.e.i. volto al trasferimento di dati già disponibili nello Stato di esecuzione (la Francia) derivanti da un'intercettazione di comunicazioni – in particolare, dati relativi al traffico e all'ubicazione, nonché registrazioni dei contenuti delle comunicazioni – qualora, in primo luogo, l'intercettazione effettuata dallo Stato di esecuzione sia generalizzata e indiscriminata e riguardi perciò tutti gli utenti di un determinato indirizzo di comunicazione; e qualora, in secondo luogo, venga richiesto, tramite l'o.e.i., il trasferimento dei dati relativi a tutti gli indirizzi utilizzati sul territorio dello Stato di emissione; ed ancora qualora, in terzo luogo, non vi fossero indizi concreti della commissione di gravi reati da parte di detti singoli utenti né al momento in cui è stata disposta ed eseguita la misura di intercettazione né al momento dell'emissione dell'o.e.i.;

b) se l'art. 6, par. 1, lett. *a)*, della Direttiva 2014/41/UE osti a tale o.e.i. qualora l'integrità dei dati ottenuti grazie alla misura di intercettazione non possa essere verificata dalle autorità dello Stato di esecuzione a causa dell'assoluta riservatezza dei dati.

2) Sull'interpretazione dell'art. 6, par. 1, lett. *b)*, della Direttiva 2014/41/UE:

se l'art. 6, par. 1, lett. *b)*, della Direttiva UE2014/41/UE osti a un o.e.i. volto al trasferimento di dati di telecomunicazione già in possesso dello Stato di esecuzione (la Francia), qualora la misura di intercettazione di detto Stato alla base dell'acquisizione dei dati sarebbe stata illegittima ai sensi del diritto dello Stato di emissione (l'Italia) in un caso interno analogo.

3) Sull'interpretazione dell'art. 31, par. 1 e 3, della Direttiva 2014/41/UE:

se una misura correlata con l'accesso clandestino ad apparecchiature terminali volta ad ottenere i dati relativi al traffico, all'ubicazione e alle comunicazioni di un servizio di comunicazione via *internet* costituisca un'intercettazione di telecomunicazioni ai sensi dell'art. 31 della Direttiva 2014/41/UE.

4) Sulle conseguenze giuridiche di un'acquisizione di prove in violazione del diritto dell'Unione:

a) se il divieto di utilizzo degli elementi di prova ottenuti tramite un o.e.i. contrario al diritto dell'Unione, previsto dal diritto interno, sia conforme al principio di effettività sancito dal diritto dell'Unione;

b) se il divieto di utilizzo degli elementi di prova ottenuti tramite un o.e.i. contrario al diritto dell'Unione sia conforme al principio di equivalenza qualora il

provvedimento su cui si basa l'acquisizione delle prove nello Stato di esecuzione non avrebbe potuto essere disposto nello Stato di emissione in un caso interno analogo e le prove acquisite mediante tale misura nazionale illegittima non sarebbero utilizzabili secondo il diritto dello Stato di emissione.

3. Con istanza depositata in data 19 dicembre 2023, l'Avvocato [redacted] anche per conto degli altri due co-difensori dei ricorrenti, ha chiesto l'anticipazione dell'udienza, in considerazione dell'avvenuta fissazione per il 29 febbraio 2024, davanti alle Sezioni Unite, di un ricorso nel quale si sollevano questioni affini a quelle prospettate dai ricorrenti in tema di acquisizione e di utilizzo di conversazioni intercorse sulla piattaforma [redacted] ottenute dall'autorità giudiziaria italiana mediante o.e.i. inviati all'autorità giudiziaria francese.

Nell'istanza, sviluppata attraverso memoria alla quale è allegata ampia documentazione, si chiede di valutare l'opportunità di investire le Sezioni Unite di ulteriori questioni problematiche in argomento, così riassunte:

a) se, alla luce dell'art. 6, paragrafo 1, lettere *a)* e *b)*, Direttiva 2014/41/UE, la *lex fori* avrebbe consentito di porre sotto intercettazione in maniera massiva e indiscriminata una intera piattaforma messaggistica, senza che la stragrande maggioranza degli abbonati fosse stata raggiunta dal minimo indizio di reità;

b) se, ai sensi dell'art. 6, paragrafo 1, lettere *a)* e *b)*, Direttiva 2014/41/UE, l'ordinamento italiano avrebbe consentito l'acquisizione delle chiavi di cifratura memorizzate nei criptofonini, con la messa in funzione di un mezzo di ricerca della prova atipico che ha violato il domicilio informatico di ogni abbonato alla piattaforma [redacted]

c) se, l'autorità giudiziaria francese, trasmettendo gli esiti dell'attività captativa autonomamente svolta nel quadro del procedimento base transalpino, abbia o meno violato l'art. 10, paragrafo 5, Direttiva 2014/41/UE e, nell'un tempo, l'art. 8, paragrafo 2, CEDU, considerato che la *lex loci* non conosce un atto di indagine analogo a quello disciplinato dall'art. 270 cod. proc. pen.;

d) se, l'autorità giudiziaria francese, dando esecuzione agli o.e.i., e dunque trasmettendo i risultati delle intercettazioni disposte ed eseguite nella inchiesta base transalpina, con la violazione dell'art. 8 paragrafo 2, CEDU, abbia trasgredito l'art. 11, paragrafo 1, lettera *f)*, Direttiva 2014/41/UE;

e) se, dopo l'esecuzione di un o.e.i., la osservanza delle condizioni stabilite dall'art. 6, paragrafo 1, lettere *a)* e *b)*, Direttiva 2014/41/UE possa formare oggetto di vaglio, ad opera del giudice del Paese di emissione;

f) se, dopo l'esecuzione di un o.e.i., sia possibile denunciare dinanzi all'autorità giudiziaria del Paese di emissione la violazione dell'art. 10, paragrafo 5, e dell'art. 11, paragrafo 1, lettera *f)*, Direttiva 2014/41/UE da parte dell'autorità giudiziaria del Paese d'esecuzione;

g) se debbono considerarsi inutilizzabili le prove che siano state acquisite in spregio dell'art. 6, paragrafo 1, lettere *a)* e *b)*, Direttiva 2014/41/UE;

h) se debbono ritenersi inutilizzabili le emergenze istruttorie che l'autorità giudiziaria del Paese d'esecuzione abbia trasmesso, in violazione dell'art. 10, paragrafo 5, o dell'art 11, paragrafo 1, lettera *f)*, Direttiva 2014/41/UE;

i) quale sia la sorte processuale da riservare alla prova che l'autorità giudiziaria francese ha trasmesso trasgredendo all'art. 8, paragrafo 2, CEDU;

j) se la prova captativa, assunta illegittimamente in un procedimento base e trasmigrata in un procedimento derivato, debba limitarsi ad essere considerata una *notitia criminis*, utile a legittimare un nuovo procedimento penale o a convergere con tale limitatissimo valore dimostrativo in un eventuale procedimento penale già preesistente.

4. Con memoria depositata in data 10 gennaio 2024, i difensori dei ricorrenti hanno ulteriormente sviluppato i temi già svolti nel ricorso.

Si sottolinea in particolare: a) l'illegittimità della intercettazione dell'intera utenza della piattaforma [redacted] siccome non riconducibile, di per sé, al contesto della criminalità organizzata, come evidenziato dai provvedimenti del Giudice istruttore del Tribunale di Parigi del 17 dicembre 2020 e del 24 febbraio 2021, che hanno disposto la messa in funzione del captatore informatico «per determinare il livello di utilizzazione criminale che è fatto da questo sistema [redacted]; b) la prevalenza della disciplina dell'o.e.i., dettata dalla Direttiva 2014/41/UE, su quella in materia di rogatoria, e, quindi, l'inapplicabilità dei principi giurisprudenziali elaborati in relazione a questa; c) la violazione dell'art. 31 della Direttiva 2014/41/UE da parte dell'autorità giudiziaria francese, in quanto la stessa avrebbe dovuto informare l'autorità giudiziaria italiana di svolgere intercettazioni su circa 12.000 utenze [redacted] localizzate in Italia, per consentire a questa di compiere approfondimenti sulla legittimità delle operazioni e di inibirne la prosecuzione in caso di ravvisata illegalità delle stesse; d) la violazione della sovranità nazionale italiana, in quanto le attività dei captatori informatici installati sui *server* di [redacted] hanno comportato l'intrusione in 12.000 domicili informatici in Italia, al di fuori di qualunque procedura di cooperazione internazionale.

5. Con ordinanza del 15 gennaio 2024, la Sesta 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 delle seguenti due questioni di diritto idonee a dare luogo ad un contrasto giurisprudenziale, anche per la pluralità degli orientamenti giurisprudenziali emersi in proposito:

a) se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera su una piattaforma informatica criptata integri l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.;

b) se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera attraverso l'inserimento di un captatore informatico sui *server* di una piattaforma criptata sia soggetta nell'ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine all'utilizzabilità dei dati raccolti.

5.1. L'ordinanza di rimessione premette che le questioni processuali formulate in via preliminare rispetto a quelle concernenti l'utilizzabilità degli atti acquisiti mediante o.e.i. sono da ritenersi infondate.

La questione posta nel primo motivo di ricorso, e riferita esclusivamente a [redacted] è relativa alla nullità di ordine generale per violazione del diritto di difesa, determinata dalla impossibilità per l'indagato ed i suoi difensori di conoscere le modalità di acquisizione e decriptazione dei messaggi scambiati sul sistema [redacted] La stessa è ritenuta infondata perché è indiscussa la presenza, tra gli atti del procedimento depositati a seguito della richiesta di riesame, delle trascrizioni delle comunicazioni intercorse sul sistema [redacted] e degli o.e.i. tramite i quali le stesse sono state richieste ed acquisite.

La questione posta nel secondo motivo di ricorso, e riferita ad entrambi i ricorrenti, riguarda l'inutilizzabilità degli atti acquisiti mediante o.e.i., per il superamento del termine massimo delle indagini, determinato dalla intempestività dell'iscrizione del nome dei ricorrenti nel registro degli indagati. La stessa è ritenuta infondata perché è inapplicabile *ratione temporis* la disciplina di cui all'art. 335-*quater* cod. proc. pen., introdotto dal d.lgs. n. 150 del 2022, con conseguente applicazione del principio enunciato dalle Sezioni Unite (Sez. U, n. 40538 del 24/09/2009, Lattanzi, Rv. 244376 – 01, e Sez. U, n. 16 del 21/06/2000, Tammaro, Rv. 216248 – 01), secondo cui il termine di durata delle indagini preliminari decorre dalla data in cui il pubblico ministero ha iscritto, nel registro delle notizie di reato, il nome della persona cui il reato è attribuito, senza che al giudice per le indagini preliminari sia consentito stabilire una diversa decorrenza.

5.2. L'ordinanza di rimessione, poi, passando all'esame del tema dell'utilizzabilità delle comunicazioni acquisite mediante o.e.i., segnala alcuni profili ritenuti non oggetto di contrasto interpretativo.

Rileva, innanzitutto, che le attività investigative compiute in Francia sono state autorizzate dal Giudice istruttore ed appaiono legittimamente eseguite nell'ambito di quell'ordinamento, anche perché tali sono state riconosciute dagli organi giudiziari di vertice di quel Paese (si citano la sentenza del 2 aprile 2022

della Corte di cassazione e la decisione n. 2022-987 QPC dell'8 aprile 2022 del Consiglio Costituzionale).

Osserva, poi, che deve escludersi la violazione dell'art. 31 Direttiva 2014/41/UE, e dell'art. 100/8 del codice di procedura penale francese, prospettata per la violazione della sovranità e della giurisdizione italiana, determinata dall'avere le attività di intercettazione riguardato numerosi utenti del sistema [redacted] che si trovavano non in Francia, ma in Italia. Evidenzia, a tal proposito, che dalla disciplina contenuta nel d.lgs. n. 108 del 2017, recante norme di attuazione della Direttiva 2014/41/UE, e, in particolare da quella di cui all'art. 24, comma 2, d.lgs. cit., il controllo del giudice italiano, nel caso di notificazione delle attività di intercettazione disposte dall'autorità giudiziaria straniera senza richiesta di assistenza tecnica, è limitato alla sola verifica della corrispondenza del titolo di reato per il quale si procede all'estero con il catalogo dei reati previsti dall'art. 266 cod. proc. pen. Aggiunge che, nella specie, i titoli per i quali si procede (reati di cui agli artt. 73 e 74 d.P.R. n. 309 del 1990) consentono di disporre intercettazioni.

Segnala, quindi, che non sussistono problemi di violazione del principio di proporzionalità determinati dal "trasferimento" in Italia delle comunicazioni intercorse sul sistema [redacted] e relative agli indagati, proprio in considerazione dei titoli dei reati per i quali si procede in Italia.

5.3. Con riferimento alla prima delle due questioni controverse (l'individuazione della disciplina applicabile in tema di acquisizione e di utilizzabilità delle comunicazioni acquisite mediante o.e.i.), l'ordinanza di rimessione premette che l'istituto giuridico di riferimento non può essere costituito dall'art. 234-*bis* cod. proc. pen. Rileva, in proposito, che l'art. 27, paragrafo 1, della Convenzione di Budapest esclude la possibilità di applicare le norme pattizie da essa previste, «qualora vi sia un trattato, un accordo o legislazione in vigore», e tale è certamente la disciplina di cui alla Direttiva 2014/41/UE. Richiama, a conferma di questa soluzione, quanto affermato da diverse decisioni (si citano: Sez. 6, n. 46833 del 26/10/2023, Bruzzaniti, Rv. 285543 - 01, 02, 03; Sez. 6, n. 48838 del 11/10/2023, Brunello, Rv. 285599 - 01, 02; Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363 - 01, 02, 03, 04).

L'ordinanza, quindi, segnala che due sono le prospettive plausibili.

Secondo un primo orientamento, la disciplina applicabile è quella relativa al sequestro di corrispondenza informatica e telematica (per questo indirizzo, si citano: Sez. 6, n. 46833 del 26/10/2023, cit.; Sez. 6, n. 48838 del 11/10/2023, Brunello, cit.; Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti, cit.), e, quindi, quella dettata dall'art. 254-*bis* cod. proc. pen. Ad avviso di queste decisioni, non è applicabile la disciplina delle intercettazioni, che presuppone la presenza di flussi di comunicazioni in atto, e che non è estensibile ai casi in cui vengano acquisite comunicazioni già avvenute, assimilabili, quindi, a corrispondenza.

L'ordinanza evidenzia che questa soluzione comporta l'esigenza di valutare il rispetto dei principi di proporzionalità ed adeguatezza rispetto ai dati da acquisire, non essendo consentita una massiva ed indiscriminata apprensione di una massa di informazioni, senza alcuna selezione o indicazione di criteri di selezione.

Secondo una diversa prospettiva, invece, trovano applicazione le disposizioni riguardanti l'acquisizione, da parte dell'autorità giudiziaria italiana, dei risultati di intercettazioni effettuate dall'autorità giudiziaria estera nell'ambito di un proprio procedimento.

L'ordinanza di rimessione rileva che questa qualificazione giuridica della vicenda determinerebbe la necessità di valutare le condizioni per la valida trasmigrazione di tali elementi di prova secondo le categorie dell'ordinamento processuale italiano, che rinviene una specifica disciplina in tema di intercettazioni nell'art. 270 cod. proc. pen. Sottolinea, in particolare, che la soluzione in discorso imporrebbe comunque, anche al giudice del processo ricevente, di valutare la sussistenza dei presupposti e delle condizioni di legittimità delle operazioni di intercettazione disposte nel processo originario (si citano Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229245 - 01; Sez. 6, n. 36874 del 13/06/2017, Romeo, Rv. 270812 - 01; Sez. 1, n. 42006 del 28/10/2010, Tavelli, Rv. 249109 - 01). Aggiunge che la necessità di bilanciare la tutela della riservatezza delle comunicazioni e la salvaguardia dei dati personali con le esigenze di repressione dei reati emerge anche dalla elaborazione della giurisprudenza sovranazionale (si citano, in particolare, Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-746/18, e Corte giustizia, Grande Sezione, 21/12/2023, G.K., C-281/22).

L'ordinanza di rimessione, però, evidenzia che, secondo una decisione (Sez. 6, n. 46482 del 27/09/2023, Bruzzaniti, Rv. 285363 - 02), la verifica di utilizzabilità degli atti "importati" non sarebbe necessaria, perché non prevista dall'art. 270 cod. proc. pen. neppure per il trasferimento di intercettazioni nei procedimenti interni.

Osserva, poi, che l'inquadramento della vicenda nell'ambito del trasferimento dei risultati di intercettazioni di altro procedimento pone un ulteriore problema, ovverossia quello della legittimità dell'uso del captatore informatico sul *server* di una piattaforma elettronica al fine di acquisire le chiavi di decrittazione delle comunicazioni. Si rileva che l'uso di questa tecnica investigativa potrebbe essere ritenuta parte dell'attività intercettativa di un flusso di comunicazioni, oppure attività atipica, anche perché, nella disciplina processuale italiana (artt. 266, commi 2 e 2-*bis*, 267, commi 1 e 2-*bis*, cod. proc. pen. e 89 disp. att. cod. proc. pen.), il captatore informatico è autorizzato soltanto ai fini dell'inserimento su un dispositivo elettronico portatile.

5.4. Relativamente alla seconda questione (diritto della difesa di poter disporre dell'algoritmo per la decrittazione delle comunicazioni), l'ordinanza di rimessione segnala che, secondo un primo orientamento, la difesa ha diritto di ottenere, oltre alla versione originale e criptata dei messaggi, anche le chiavi di sicurezza necessarie alla decriptazione (si citano Sez. 4, n. 32915 del 15/07/2022, Lori, non mass., con riguardo alle comunicazioni sul sistema [redacted] nonché Sez. 4, n. 49896 del 05/10/2019, Brandimarte, Rv. 277949 - 03, in fattispecie relativa a messaggi scambiati mediante il sistema *BlackBerry*), salva la necessità del relativo bilanciamento con interessi quali la sicurezza nazionale o la segretezza dei metodi di indagine della polizia (si cita, per questa precisazione, Sez. 6, n. 44154 del 26/10/2023, Iaria, Rv. 285284 - 01).

L'ordinanza, poi, rappresenta che, secondo un diverso indirizzo interpretativo, la disponibilità dell'algoritmo funzionale alla criptazione dei messaggi non costituisce elemento necessario per l'esercizio del diritto di difesa, in quanto, secondo la scienza informatica, solo l'algoritmo corretto consente di poter derivare dal testo criptato un testo intelligibile (si citano: Sez. 3, n. 30395 del 21/04/2022, Chiancano, Rv. 283454 - 01; Sez. 6, n. 14395 del 27/11/2019, Testa, dep. 2020, Rv. 275534 - 01; Sez. 3, n. 38009 del 11/09/2019, Assisi, Rv. 278166 - 02).

Segnala, infine, che, alla stregua di un ulteriore orientamento, emerso con specifico riferimento alle comunicazioni intercorse sul sistema [redacted] il diritto ad avere conoscenza dell'algoritmo non è riconosciuto dalla legge italiana: questa prevede che il difensore dell'indagato possa accedere al verbale delle operazioni di cui all'art. 268 cod. proc. pen. e alle registrazioni, ma non anche ai mezzi tecnici, *hardware* e *software*, utilizzati per l'intrusione nelle conversazioni intercettate o per decodificarne il contenuto (si citano Sez. 6, n. 46390 del 26/10/2023, Rosaci, Rv. 285494 - 01 e Sez. 6, n. 48838 del 11/10/2023, cit.).

6. Con decreto del 22 gennaio 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 istanze trasmesse il 22 gennaio 2024 e il 23 gennaio 2024, rispettivamente, l'Avvocato [redacted] quale difensore di entrambi i ricorrenti, e l'Avvocato [redacted] quale difensore di [redacted] hanno chiesto di poter discutere oralmente la causa.

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

7. In data 12 febbraio 2024, la Procura generale ha presentato memoria, nella quale 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.

8. In data 13 febbraio 2024, i difensori dei ricorrenti hanno depositato un motivo nuovo, con il quale si denuncia violazione di legge, con riferimento agli artt. 6 CEDU, 24 e 111 Cost., e 48, paragrafo 2, Carta dei diritti fondamentali dell'Unione Europea, nonché vizio di motivazione, a norma dell'art. 606, comma 1, lett. c) ed e), cod. proc. pen., avendo riguardo alla violazione del diritto della difesa di accedere al sistema informatico impiegato per l'analisi delle comunicazioni intercorse sul sistema [redacted]

Si premette che: a) secondo quanto rappresentato nell'informativa dei R.O.S. del 15 settembre 2022, depositata nel proc. n. 1589/19 R.G.N.R. DDA Reggio Calabria, i risultati degli atti di indagine autorizzati dal Tribunale di Lille e dal Tribunale di Parigi sono stati trasferiti alla polizia olandese, la quale avrebbe archiviato le centinaia di milioni di messaggi ricevuti in un *warehouse*; b) il sistema informatico olandese, composto da algoritmi di intelligenza artificiale, ha consentito di catalogare le diverse conversazioni in modo da raggrupparle per singole attività delittuose e, verosimilmente, di decrittarle, sulla base di una ricerca informatica completamente automatizzata, sottratta alla supervisione umana.

Si deduce che, in considerazione di quanto appena indicato, è illegittimo impedire agli indagati di avere contezza piena dell'attività informatica svolta in Olanda, e, quindi, di accedere al *software* utilizzato per il trattamento dei dati esaminati in quella sede. Si osserva, a sostegno della censura, che, a norma dell'art. 8 d.lgs. n. 51 del 2018, sono vietate decisioni basate unicamente su un trattamento automatizzato dei dati, e che il sistema utilizzato dalle autorità olandesi, come indicato dalla dottrina specialistica, presenta margini di fallibilità.

9. In data 23 febbraio 2024, l'Avvocato [redacted] nell'interesse di entrambi i ricorrenti, ha depositato memoria, nella quale si approfondisce la ricostruzione dei fatti processuali, a conferma di quanto rappresentato nei ricorsi, nelle precedenti memorie e nel motivo nuovo, si replica alle argomentazioni del Procuratore generale presso la Corte di cassazione e si sviluppano ulteriormente, in particolare, le questioni concernenti: a) la violazione dell'art. 6, par. 1, lett. *a)* e *b)*, Direttiva 2014/41/UE; b) la violazione dell'art. 31 Direttiva 2014/41/UE; c) l'inutilizzabilità degli algoritmi di decodifica captati dai singoli dispositivi criptati; d) l'illegittimità delle operazioni di decodifica, analisi e selezione delle comunicazioni acquisite.

CONSIDERATO IN DIRITTO

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

"Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera su una piattaforma informatica criptata integri l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.";

"Se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera attraverso l'inserimento di un captatore informatico sui server di una piattaforma criptata sia soggetta nell'ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine all'utilizzabilità dei dati raccolti".

2. Le due questioni sottoposte all'esame delle Sezioni Unite sono rilevanti ai fini della decisione del ricorso, in quanto attengono all'utilizzabilità degli elementi posti a fondamento dell'affermazione di sussistenza dei gravi indizi di colpevolezza a carico dei ricorrenti.

Tuttavia, è necessario procedere, in via preliminare, all'esame delle censure esposte nei primi due motivi dei ricorsi, perché il loro eventuale accoglimento renderebbe superfluo lo scrutinio delle questioni relative all'utilizzabilità degli elementi posti a base dell'affermazione di sussistenza dei gravi indizi di colpevolezza.

3. Le censure formulate nel primo motivo, nell'interesse del solo [redacted] denunciano la violazione del diritto di difesa, già eccepita in sede di interrogatorio di garanzia, con riferimento all'omessa acquisizione agli atti del procedimento dei provvedimenti del Tribunale di Lille e del Tribunale di Parigi che hanno disposto l'attività investigativa in Francia, e, comunque, al mancato deposito degli stessi, unitamente all'ordinanza cautelare, siccome necessari per poter controllare validità ed utilizzabilità del materiale ricevuto tramite o.e.i.

Le doglianze appena sintetizzate, per come prospettate, non riguardano in realtà il mancato deposito di atti presenti nel fascicolo del procedimento, ma si riferiscono alla mancata acquisizione allo stesso dei provvedimenti sulla cui base sono stati compiuti, in altro procedimento, pendente davanti all'autorità giudiziaria francese, gli atti di indagine poi acquisiti dall'autorità giudiziaria italiana mediante o.e.i.

Ciò posto, va in primo luogo rilevato che non risultano, né sono indicate, disposizioni da cui desumere la giuridica necessità dell'acquisizione e del deposito, nel procedimento in Italia, dei provvedimenti dell'autorità giudiziaria straniera aventi ad oggetto l'autorizzazione di attività di indagine in un procedimento pendente davanti ad essa, i cui esiti sono stati successivamente richiesti dall'autorità giudiziaria italiana mediante o.e.i.

L'art. 78 disp. att. cod. proc. pen., nel disciplinare l'acquisizione di atti di un procedimento penale compiuti da autorità giudiziaria straniera, non richiede anche l'acquisizione dei provvedimenti giudiziari in forza dei quali tali atti sono stati compiuti.

La medesima conclusione si evince anche dalla disciplina paradigmatica nel sistema processuale penale italiano per l'acquisizione di atti compiuti o formati in altro procedimento sulla base di un provvedimento dell'autorità giudiziaria, ossia quella relativa ai risultati di intercettazioni di conversazioni o di comunicazioni, dettata dall'art. 270 cod. proc. pen. Questa disposizione, infatti, prevede il deposito dei verbali e delle registrazioni relativi alle intercettazioni effettuate in altri procedimenti, ma non anche il deposito dei relativi provvedimenti autorizzativi. E sulla base di questa disciplina, l'orientamento consolidato della giurisprudenza di questa Corte ritiene che: a) ai fini dell'utilizzabilità degli esiti di intercettazioni di conversazioni o comunicazioni in procedimento diverso da quello nel quale esse furono disposte, non occorre la produzione del relativo decreto autorizzativo, essendo sufficiente il deposito, presso l'Autorità giudiziaria competente per il "diverso" procedimento, dei verbali e delle registrazioni delle intercettazioni medesime (così, per tutte, Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229244 - 01, nonché, da ultimo, con riferimento alla disciplina vigente per effetto delle modifiche recate dalla legge 9 ottobre 2023, n. 137, Sez. 1, n. 49622 del 14/11/2023, Kasli Ramazan, Rv. 2855579 - 02); b) spetta alla parte che eccepisce nel procedimento *ad quem* la mancanza o l'illegittimità dell'autorizzazione, e si oppone all'utilizzabilità degli esiti di intercettazioni di conversazioni o comunicazioni in un procedimento diverso da quello nel quale esse furono disposte, l'onere di produrre il decreto autorizzativo, in modo da consentire al giudice di verificare l'effettiva inesistenza nel procedimento *a quo* del controllo giurisdizionale prescritto dall'art. 15 Cost. (cfr., tra le tante, Sez. 2, n. 6947 del 29/10/2019, dep. 2020, Rossi, Rv. 278246 - 01, e Sez. 6, n. 41515 del 18/09/2015, Lusha, Rv. 264741 - 01).

4. Le censure esposte nel secondo motivo, nell'interesse di entrambi i ricorrenti, denunciano l'inutilizzabilità degli atti acquisiti mediante o.e.i., perché ottenuti successivamente al decorso del termine massimo delle indagini preliminari.

In proposito, occorre premettere che la disciplina in tema di accertamento della tempestività delle iscrizioni nel registro delle notizie di reato, oggi prevista dall'art. 335-*quater* cod. proc. pen., non si applica, a norma dell'art. 88-*bis* d.lgs. 10 ottobre 2022, n. 150, così come inserito dall'art. 5-*sexies* d.l. 31 ottobre 2022, n. 162, convertito, con modificazioni, dalla legge 30 dicembre 2022, n. 199, ai procedimenti pendenti alla data di entrata in vigore del 30 dicembre 2022 in

relazione alle notizie di reato delle quali il pubblico ministero ha già disposto l'iscrizione nel registro di cui all'art. 335 cod. proc. pen., nonché in relazione alle notizie di reato iscritte successivamente, quando ricorrono le condizioni previste dall'art. 12 cod. proc. pen. e, se si procede per taluno dei delitti indicati nell'art. 407, comma 2, cod. proc. pen., anche quando ricorrono le condizioni previste dall'art. 371, comma 2, lett. b) e c), cod. proc. pen.

Nella specie, secondo quanto rappresentato nell'ordinanza impugnata, e non confutato specificamente dalla difesa, la notizia di reato per la quale è stata emessa l'ordinanza cautelare è stata iscritta nei confronti di [redacted] unico dei due attuali ricorrenti a sollevare la questione in sede di riesame, in data 3 marzo 2022, quindi in epoca di gran lunga anteriore a quella di entrata in vigore dell'art. 335-*quater* cod. proc. pen.

Di conseguenza, trova applicazione la precedente disciplina, in forza della quale, secondo il consolidato orientamento della giurisprudenza di legittimità, il termine di durata delle indagini preliminari decorre dalla data in cui il pubblico ministero ha iscritto, nel registro delle notizie di reato, il nome della persona cui il reato è attribuito, senza che al g.i.p. sia consentito stabilire una diversa decorrenza, sicché gli eventuali ritardi indebiti nella iscrizione, tanto della notizia di reato che del nome della persona cui il reato è attribuito, pur se abnormi, sono privi di conseguenze agli effetti di quanto previsto dall'art. 407, comma 3, cod. proc. pen., fermi restando gli eventuali profili di responsabilità disciplinare o penale del magistrato del P.M. che abbia ritardato l'iscrizione (Sez. U, n. 40538 del 24/09/2009, Lattanzi, Rv. 244376 – 01; Sez. U, n. 16 del 21/06/2000, Tammaro, Rv. 216248 – 01; Sez. 6, n. 4844 del 14/11/2018, dep. 2019, Ludovisi, Rv. 275046 – 01).

5. L'infondatezza dei primi due motivi dei ricorsi consente di passare all'esame delle due questioni rimesse alle Sezioni Unite e rilevanti ai fini dell'utilizzabilità degli elementi posti a base del giudizio di gravità indiziaria da parte dell'ordinanza impugnata.

Le due questioni sono tra loro strettamente connesse, perché le conclusioni sulla natura giuridica da attribuire all'acquisizione, effettuata mediante ordine europeo di indagine (c.d. o.e.i.), di comunicazioni scambiate su *chat* di gruppo mediante un sistema cifrato, e già a disposizione dell'autorità giudiziaria straniera, hanno una diretta ricaduta sul tema della necessità di preventiva o successiva verifica giurisdizionale ai fini dell'utilizzabilità dei dati raccolti.

Per questa ragione, ognuno dei diversi indirizzi giurisprudenziali sarà oggetto di esposizione unitaria con riferimento alle soluzioni accolte per entrambi i profili.

6. 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.

6.1. 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.

6.2. 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.

7. 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.

7.1. 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.).

7.2. 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)».

7.3. 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.

7.4. 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).

8. 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.

8.1. 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.

8.2. 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.

9. 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.

9.1. 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).

9.2. 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».

10. 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.

10.1. 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.

10.2. 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.).

10.3. 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.

10.4. 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».

10.5. 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).

10.6. 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.

11. 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.

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

Il fatto che le comunicazioni 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.

12.1. 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.

12.2. 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.

12.3. 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 § 12.2, 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.

12.4. Senza dubbio, come già segnalato in precedenza al § 12.2. 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 §§ 10.2, 10.3, 10.4, 10.5 e 10.6.

13. 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, tenuto conto dell'indisponibilità in questa sede dell'intero materiale acquisito mediante o.e.i., con conseguente impossibilità di definire con certezza se lo stesso consista di risultati di intercettazioni, queste ultime da intendersi come attività di «apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio» (cfr., per questa definizione, in particolare, Sez. U, n. 36747 del 28/05/2003, Torcasio, Rv. 225465-01, e Corte cost., sent. n. 170 del 2023), e l'ininfluenza dell'una o dell'altra qualificazione ai fini della decisione dei ricorsi, come si preciserà in seguito.

14. Secondo l'ordinanza impugnata, gli atti acquisiti mediante o.e.i. dall'autorità giudiziaria francese costituiscono "documenti", e non "intercettazioni di conversazioni o comunicazioni".

14.1. 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).

14.2. 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.

14.3. 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 § 14.2., 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 §§ 12.2 e 12.3, 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 § 10.6.

15. Secondo il ricorso, gli atti acquisiti mediante o.e.i. dall'autorità giudiziaria francese, invece, costituiscono risultati di intercettazioni di conversazioni o di comunicazioni, effettuate anche mediante un captatore informatico inserito sui *server* della piattaforma del sistema [redacted] al fine di acquisire le chiavi di cifratura delle comunicazioni, custodite nei dispositivi dei singoli utenti.

15.1. La qualificazione degli atti in questione come risultati di intercettazioni di conversazioni o di comunicazioni implica che il parametro 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 è costituito dalla disciplina prevista dall'art. 270 cod. proc. pen. (cfr., per questa indicazione, tra le altre, già Sez. 1, n. 4048 del 06/07/1998, Bonelli, Rv. 211301 – 01).

In particolare, a norma dell'art. 270 cod. proc. pen., i risultati delle intercettazioni possono essere utilizzati in procedimenti diversi da quelli nei quali le operazioni sono state disposte solo se «risultino rilevanti ed indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza».

Secondo il consolidato indirizzo di questa Corte, ai fini dell'utilizzabilità degli esiti di intercettazioni di conversazioni o comunicazioni in procedimento diverso da quello nel quale esse furono disposte, non occorre la produzione del relativo decreto autorizzativo, in quanto l'art. 270 cod. proc. pen. prevede esclusivamente il deposito, presso l'autorità giudiziaria competente per il "diverso" procedimento, dei verbali e delle registrazioni delle intercettazioni medesime, né sono altrimenti previste sanzioni di inutilizzabilità (Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229244 – 01, e Sez. 1, n. 49627 del 14/11/2023, Kasli Ramazan, Rv. 285579 – 02). Sempre secondo il costante orientamento di questa Corte, grava sulla parte che eccepisce l'invalidità o l'inutilizzabilità delle intercettazioni provenienti da altro procedimento l'onere di allegare e provare il fatto dal quale dipende la patologia denunciata (Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229245 – 01), e, quindi, nel caso di censura concernente il vizio di motivazione apparente, di

produrre sia il decreto di autorizzazione emesso nel procedimento diverso sia il documento al quale esso rinvia (Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229246 - 01, nonché Sez. 1, n. 11168 del 18/02/2019, Caratelli, Rv. 274996 - 01). Ancora secondo quanto enunciato dalle Sezioni Unite, nel caso di acquisizione degli esiti di intercettazioni di conversazioni o comunicazioni in procedimento diverso da quello nel quale siano state rilasciate le relative autorizzazioni, il controllo del giudice sulla legalità dell'ammissione e dell'esecuzione delle operazioni - di carattere meramente incidentale e, come tale, ininfluente nel procedimento *a quo* - riguarda esclusivamente la serietà e la specificità delle esigenze investigative, come individuate dal P.M. in relazione alla fattispecie criminosa ipotizzata, e non comporta alcuna valutazione di fondatezza, neanche sul piano indiziario, della ipotesi in questione (Sez. U, n. 45189 del 17/11/2004, Esposito, Rv. 229247 - 01).

Numerose decisioni, poi, affermano che, in tema di intercettazioni disposte in altro procedimento, l'omesso deposito degli atti relativi, ivi compresi i nastri di registrazione, presso l'autorità competente per il diverso procedimento, non ne determina l'inutilizzabilità, in quanto detta sanzione non è prevista dall'art. 270 cod. proc. pen. e non rientra nel novero di quelle di cui all'art. 271 cod. proc. pen. aventi carattere tassativo (così *ex plurimis*: Sez. 5, n. 1801 del 16/07/2015, dep. 2016, Tunno, Rv. 266410 - 01; Sez. 5, n. 14783 del 13/03/2009, Badescu, Rv. 243609 - 01; Sez. 6, n. 27042 del 18/02/2008, Morabito, Rv. 240972 - 01).

Ancora, la trasmissione dei risultati delle intercettazioni di conversazioni o comunicazioni dal procedimento in cui sono state disposte ad altro procedimento in cui si intende utilizzarle non richiede alcun intervento preventivo da parte del giudice di quest'ultimo, al fine di autorizzare le parti interessate a procedere all'acquisizione di copia dei relativi atti, perché tale intervento non è previsto dall'art. 270 cod. proc. pen., né è imposto da altre disposizioni o dal sistema normativo, per le ragioni già indicate al § 12.2.

15.2. In materia di ordine europeo di indagine, la Direttiva 2014/41/UE e il d.lgs. n. 108 del 2017 prevedono regole specifiche per il caso che l'atto investigativo richiesto sia costituito da intercettazioni di telecomunicazioni, ma mancano disposizioni espresse per la trasmissione e l'utilizzazione dei risultati delle intercettazioni in procedimenti diversi da quelli in cui sono state effettuate.

La Direttiva 2014/41/UE dedica alla effettuazione di intercettazioni di telecomunicazioni gli artt. 30 e 31.

In particolare, l'art. 30, paragrafo 7, Direttiva cit. stabilisce che «l'autorità di emissione può altresì richiedere, se ne ha particolare motivo, una trascrizione, una decodificazione o una decrittazione della registrazione, fatto salvo l'accordo dell'autorità di esecuzione».

L'art. 31 Direttiva cit., poi, prevede che, quando «l'intercettazione di telecomunicazioni è autorizzata dall'autorità competente di uno Stato membro e l'indirizzo di comunicazione della persona soggetta a intercettazione indicata nell'ordine di intercettazione è utilizzato sul territorio di un altro Stato membro, la cui assistenza tecnica non è necessaria per effettuare l'intercettazione», occorre darne «notifica» all'autorità competente di quest'ultimo. Precisamente, la «notifica» deve precedere l'intercettazione, quando l'autorità procedente, già al momento di disporre l'attività di captazione, è a conoscenza della presenza della persona soggetta a controllo nel territorio di altro Stato membro; deve avvenire «durante l'intercettazione, o ad intercettazione effettuata», quando la conoscenza della presenza della persona soggetta a controllo nel territorio di altro Stato membro si determina durante o al termine dello svolgimento delle operazioni. L'autorità competente dello Stato che riceve la «notifica», «può» comunicare che l'intercettazione non è consentita; in questi casi, l'attività non può essere iniziata o proseguire, e gli eventuali risultati già ottenuti mentre la persona soggetta ad intercettazione si trovava sul territorio dello Stato che ha ricevuto la «notifica» non possono essere utilizzati, o possono esserlo solo alle condizioni specificate dall'autorità competente di quest'ultimo.

Il d.lgs. n. 108 del 2017, a sua volta, regola la materia relativa alle intercettazioni di telecomunicazioni agli artt. 43 e 44, per le procedure attive, e agli artt. 23 e 24, per le procedure passive.

Gli artt. 43 e 44 d.lgs. cit. contengono disposizioni sostanzialmente sovrapponibili a quelle di cui agli artt. 30 e 31 Direttiva 2014/41/UE. In particolare, l'art. 43, al comma 1, precisa che la disciplina si riferisce «all'esecuzione delle operazioni di intercettazione delle conversazioni o comunicazioni o del flusso di comunicazioni relativo a sistemi informatici o telematici, quando nel territorio di un altro Stato membro si trova il dispositivo o il sistema da controllare», e, al comma 4, stabilisce che «[l]a richiesta può avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate».

L'art. 24 d.lgs. cit., poi, con riguardo alle intercettazioni effettuate dall'autorità giudiziaria di altro Stato membro di «un dispositivo, anche di sistema informatico o telematico, in uso a persona che si trovi nel territorio dello Stato», contempla un'unica situazione alla quale consegue la cessazione delle operazioni e la inutilizzabilità ai fini di prova dei risultati già ottenuti: «se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo l'ordinamento interno, le intercettazioni non sono consentite».

15.3. In considerazione di quanto sopra evidenziato, può ritenersi che l'o.e.i. emesso dal pubblico ministero italiano avente ad oggetto l'acquisizione dei risultati di intercettazioni di conversazioni o comunicazioni disposte dall'autorità giudiziaria straniera, anche quando relative a sistemi informatici o telematici, o intercorrenti

tra più sistemi, 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 risultati di intercettazioni ordinate in altro procedimento penale senza necessità di preventiva autorizzazione del giudice competente per il procedimento nel quale intende utilizzarli, deve ritenersi che un o.e.i. presentato dal pubblico ministero italiano, nel quale si chiede, senza preventiva autorizzazione del giudice nazionale, la trasmissione di risultati di intercettazioni ordinate dall'autorità giudiziaria straniera in un procedimento pendente davanti alla stessa, abbia ad oggetto atti che «avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo».

15.4. E questa conclusione, in ordine al rispetto della condizione di cui all'art. 6, paragrafo 1, lett. *b)*, Direttiva 2014/41/UE, resta ferma anche se le operazioni di intercettazione siano state realizzate mediante l'inserimento di un captatore informatico sui *server* della piattaforma di un sistema informatico o telematico, al fine di acquisire le chiavi di cifratura delle comunicazioni, custodite nei dispositivi dei singoli utenti.

15.4.1. Innanzitutto, non può ritenersi che l'inserimento di un captatore informatico sul *server* di una piattaforma di un sistema informatico o telematico costituisca mezzo "atipico" di indagine o di prova, come tale non consentito dall'ordinamento italiano perché incidente sui diritti fondamentali della persona.

In proposito, non assume valenza dirimente il fatto che, nel codice di rito, in materia di intercettazioni, si faccia menzione della sola ipotesi dell'«inserimento di un captatore informatico su un dispositivo elettronico portatile».

Il captatore informatico, infatti, non è un autonomo mezzo di ricerca della prova, e tanto meno un mezzo di prova, bensì uno strumento tecnico attraverso il quale esperire il mezzo di ricerca della prova costituito dalle intercettazioni di conversazioni o di comunicazioni. Sicché non è indispensabile che il legislatore preveda dove lo stesso possa essere "inserito".

E una conferma di questa conclusione può essere desunta dall'elaborazione della giurisprudenza di legittimità, anche delle Sezioni Unite, la quale, già prima che venisse previsto dalla legge l'utilizzo del captatore informatico come strumento per effettuare attività di intercettazione, ne aveva ritenuto legittimo l'impiego a tali fini, precisandone anche l'ammissibilità, nei procedimenti per delitti di criminalità organizzata, con riguardo a captazioni di conversazioni o comunicazioni tra presenti in luoghi di privata dimora (così, per tutte, Sez. U, n. 26889 del 28/04/2016, Scurato, Rv. 266905 - 01).

15.4.2. In secondo luogo, poi, non può ritenersi che l'utilizzo del captatore informatico al fine di acquisire le chiavi di cifratura presenti sui dispositivi mobili dei singoli utenti costituisca mezzo "atipico" di indagine o di prova, come tale non

consentito nell'ordinamento italiano, perché opera un'intrusione nel domicilio informatico di una persona allo scopo di captare non comunicazioni, ma dati necessari per rendere intellegibili le comunicazioni.

Per un verso, sia la Direttiva 2014/41/UE, all'art. 30, paragrafo 7, sia il d.lgs. n. 108 del 2017, all'art. 43, comma 4, prevedono espressamente la possibilità per l'autorità che ha emesso un o.e.i. per l'intercettazione di telecomunicazioni di chiedere la decodificazione o la decrittazione delle comunicazioni intercettate. E così disponendo, riconoscono che l'attività di intercettazione implica anche l'acquisizione degli strumenti necessari per procedere a decodificazione o decrittazione delle conversazioni o comunicazioni.

Sotto altro profilo, poi, va rilevato che, nell'ordinamento italiano, secondo il diffuso orientamento della giurisprudenza di legittimità, l'autorizzazione ad eseguire intercettazioni telefoniche ed ambientali implica anche il compimento di quegli atti che costituiscono una naturale modalità attuativa delle operazioni, sebbene gli stessi comportino l'intrusione nel domicilio di una persona. Invero, numerose decisioni hanno osservato che la finalità di intercettare conversazioni telefoniche e/o ambientali consente all'operatore di polizia la materiale intrusione, per la collocazione dei necessari strumenti di rilevazione, negli ambiti e nei luoghi di privata dimora, oggetto di tali mezzi di ricerca della prova (cfr., in particolare: Sez. 6, n. 39403 del 23/06/2017, Nobile, Rv. 270941 - 01; Sez. 6, n. 41514 del 25/09/2012, Adamo, Rv. 253805 - 01; Sez. 6, n. 15447 del 31/01/2011, Di Maggio, Rv. 250032 - 01). E, anzi, proprio in questa prospettiva, si è più volte affermato che è manifestamente infondata la questione di legittimità costituzionale dell'art. 266, comma 2, cod. proc. pen., sollevata in relazione all'art. 14 della Costituzione, che statuisce il principio dell'inviolabilità del domicilio, perché la collocazione di microspie all'interno di un luogo di privata dimora costituisce una delle naturali modalità di attuazione delle intercettazioni, costituenti mezzo di ricerca della prova funzionale al soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti, tutelato dal principio dell'obbligatorietà dell'azione penale di cui all'art. 112 della Costituzione, con il quale il principio di inviolabilità del domicilio deve necessariamente coordinarsi, subendo la necessaria compressione, al pari di quanto previsto dall'art. 15 della Costituzione in tema di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (così Sez. 2, n. 21644 del 13/02/2013, Badagliacca, Rv. 255541 - 01, e Sez. 1, n. 38716 del 02/10/2007, Biondo, Rv. 238108 - 01).

Deve perciò concludersi che, anche nel nostro sistema, è ammissibile, ai fini dell'utile effettuazione di intercettazioni telefoniche ed ambientali, l'autorizzazione, da parte del giudice, del compimento di quegli atti che ne costituiscono una naturale e necessaria modalità attuativa, pur quando gli stessi comportino l'intrusione nel dispositivo elettronico di una persona.

15.5. Con riferimento al tema concernente la garanzia del rispetto dei «diritti fondamentali», la qualificazione degli atti acquisiti mediante o.e.i. dall'autorità giudiziaria francese come risultati di intercettazioni di conversazioni o di comunicazioni determina l'esigenza, in particolare, di un esame dell'elaborazione in materia della giurisprudenza della Corte EDU e delle condizioni poste dalla specifica disciplina fissata nella Direttiva 2014/41/UE.

15.5.1. La tematica del rispetto dei «diritti fondamentali» in relazione alle attività di intercettazione di conversazioni o di comunicazioni ha costituito oggetto di un ampio approfondimento da parte della Corte EDU.

Innanzitutto, secondo la Corte di Strasburgo, la tutela del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, assicurata dall'art. 8 CEDU, esige sia la previsione di disposizioni "chiare" sui presupposti richiesti per autorizzare le intercettazioni, sia l'adozione di un provvedimento autorizzativo da parte di un'autorità indipendente specificamente motivato sull'esistenza in concreto di tali presupposti (cfr. Corte EDU, 12/01/2023, Potoczká e Adamčo c. Slovacchia, nonché Corte EDU, 15/01/2015, Dragojević c. Croazia). Sempre secondo la Corte EDU, poi, la motivazione del provvedimento autorizzativo deve consentire di verificare se sussistono ragioni "fattuali" per sospettare che una persona progetti, commetta o abbia commesso alcuni gravi reati e se non vi è alcuna prospettiva di accertare i fatti con successo mediante un altro metodo, diverso dalle intercettazioni, o questo sarebbe notevolmente più difficile (così Corte EDU, 12/01/2023, Potoczká e Adamčo c. Slovacchia, § 73).

Da questa elaborazione, si evince, in particolare, che le intercettazioni non autorizzate da un giudice o da un'autorità indipendente, e le intercettazioni disposte sulla base di provvedimenti non motivati in ordine all'esistenza in concreto dei presupposti richiesti dalla legge per procedervi, si pongono in contrasto con i diritti fondamentali garantiti dalla CEDU.

Tuttavia, dalla giurisprudenza della Corte EDU non emerge un divieto di effettuare intercettazioni di vaste proporzioni, purché siano previste efficaci garanzie contro rischi di abusi e di arbitri nelle fasi dell'adozione della misura, della sua esecuzione e del controllo successivo (cfr. Corte EDU, Grande Camera, 25/05/2021, Big Brother Watch ed altri c. Regno Unito, e Corte EDU, Grande Camera, 25/05/2021, Centrum för Rättvisa c. Svezia, le quali, sebbene con riguardo ad intercettazioni effettuate dai servizi segreti e non nell'ambito di un procedimento penale, hanno escluso che, in generale, le c.d. "intercettazioni di massa", anche quando disposte per contrastare attività delittuose concernenti il traffico di sostanze illecite, integrino una violazione degli artt. 8 e 10 CEDU, se effettuate nel rispetto di "dovute" garanzie).

Né risulta affermata l'incompatibilità con le garanzie della CEDU della trasmissione dei risultati di intercettazioni disposte in un procedimento penale ad

un diverso procedimento penale da parte di un pubblico ministero. Anzi, allo stato, alcune decisioni hanno escluso che l'art. 8 CEDU esiga l'autorizzazione *ex ante* di un giudice alla trasmissione, dal pubblico ministero all'autorità amministrativa, di risultati di intercettazioni telefoniche effettuate in un procedimento penale (cfr., per tutte, Corte EDU, 16/05/2023, Janssen De Jong Groep B.V. c. Paesi Bassi).

Nemmeno l'impossibilità, per la difesa, di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per "criptare" il contenuto delle stesse 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). Né la giurisprudenza sovranazionale risulta aver affermato che l'indisponibilità dell'algoritmo di decriptazione agli atti del processo costituisca, di per sé, violazione dei «diritti fondamentali». In proposito, anzi, può rilevarsi che 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 [redacted] 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* [redacted] *material in his regard would have constituted an important step in preserving his defence rights*»).

In ogni caso, inoltre, resta fermo 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 § 10.6.

15.5.2. Con riferimento alle garanzie previste dalla Direttiva 2014/41/UE, può venire in rilievo il profilo, segnalato dai ricorrenti, della violazione dei principi fissati dall'art. 31 in ordine alle intercettazioni effettuate nei confronti di persone il cui

«indirizzo di comunicazione» è utilizzato nel territorio di uno Stato diverso da quello nel quale le operazioni di captazione sono state disposte.

Secondo quanto più analiticamente esposto in precedenza al § 15.2, l'art. 31 Direttiva cit. prevede che lo Stato nel quale sono state disposte le intercettazioni dia «notifica» di tali attività all'autorità competente nello Stato nel quale è utilizzato l'indirizzo di comunicazione sottoposto a controllo, quando viene a conoscenza di tale circostanza, e che quest'ultima possa vietare il compimento o la prosecuzione delle operazioni, nonché l'utilizzazione dei risultati già ottenuti.

Sulla base di tale disciplina, deve rilevarsi, innanzitutto, che l'obbligo di notifica sorge quando l'autorità procedente viene a conoscenza che l'intercettazione riguarda persone il cui «indirizzo di comunicazione» è utilizzato nel territorio di un altro Stato.

Va segnalato, poi, che l'eventuale intempestività della comunicazione non è sanzionata di per sé, e che, in ogni caso, opera la garanzia della possibile dichiarazione di inutilizzabilità da parte dell'autorità competente dello Stato in cui è fatto uso dell'«indirizzo di comunicazione».

Occorre considerare, ancora, che il divieto della Direttiva 2014/41/UE di iniziare o proseguire le attività di captazione, ovvero di utilizzarne i risultati, è previsto solo «[q]ualora l'intercettazione non sia ammessa in un caso interno analogo». E, nella disciplina italiana di attuazione della Direttiva cit., l'art. 24 d.lgs. n. 108 del 2017 prevede un'unica ipotesi vietata: «se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo l'ordinamento interno, le intercettazioni non sono consentite».

Può quindi concludersi che, nell'ordinamento italiano, sulla base della disciplina di cui all'art. 31 Direttiva 2014/41/UE, l'inutilizzabilità dei risultati di intercettazioni disposte da autorità di altro Stato ed effettuate nei confronti di persone il cui «indirizzo di comunicazione» è attivato in Italia sussiste solo se l'autorità giudiziaria italiana rileva che le captazioni non sarebbero state consentite «in un caso interno analogo», perché disposte per un reato per il quale la legge nazionale non prevede la possibilità di ricorrere a tale mezzo di ricerca della prova.

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

"*In materia di ordine europeo di indagine, l'acquisizione dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera in un procedimento penale pendente davanti ad essa, ed effettuate su una piattaforma informatica criptata e su criptofonini, 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, ma è assoggettata alla disciplina di cui all'art. 270 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 i risultati di intercettazioni disposte da un'autorità giudiziaria straniera in un procedimento penale pendente davanti ad essa, ed effettuate attraverso l'inserimento di un captatore informatico sui server di una piattaforma criptata, è ammissibile, perché attiene ad esiti investigativi ottenuti con modalità compatibili con l'ordinamento italiano, e non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria ex art. 6 Direttiva 2014/41/UE, perché tale autorizzazione non è richiesta nella disciplina nazionale".

"L'utilizzabilità dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera in un procedimento penale pendente davanti ad essa, ed effettuate su una piattaforma informatica criptata e su criptofonini, deve essere esclusa se il giudice del procedimento nel quale dette risultanze istruttorie vengono acquisite rileva che, in relazione ad esse, si sia verificata la 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".

17. Sulla base dei principi di diritto enunciati, e degli argomenti esposti a loro fondamento, è possibile esaminare le censure enunciate nel terzo, nel quarto, nel quinto e nel sesto motivo dei ricorsi, nonché le ulteriori richieste formulate nei ricorsi, nelle memorie e nelle conclusioni orali rese in udienza.

18. Complessivamente infondate sono le censure esposte nel terzo, nel quarto, nel quinto e nel sesto motivo dei ricorsi, e sviluppate nelle memorie, le quali contestano l'utilizzabilità dei dati informatici relativi alle comunicazioni intercorse attraverso il sistema criptato [redacted] sotto vari profili.

In sintesi, le stesse deducono l'inapplicabilità della disciplina di cui all'art. 234-*bis* cod. proc. pen. e l'applicabilità di quella relativa all'acquisizione dei risultati di intercettazioni, il difetto dei presupposti per l'emissione dell'o.e.i., in particolare per il carattere generalizzato ed indifferenziato delle attività di captazione

effettuata dall'autorità estera, per l'utilizzo di un captatore informatico inserito al fine esclusivo di acquisire le chiavi di cifratura delle comunicazioni, per la mancata messa a disposizione della difesa dei testi criptati delle comunicazioni, e per la violazione dell'art. 31 Direttiva 2014/41/UE, nonché ancora la violazione della disciplina francese, priva di disposizioni analoghe all'art. 270 cod. proc. pen.

18.1. 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 [redacted] perché si tratta di disciplina alternativa, e, quindi, incompatibile con quella relativa al sistema dell'o.e.i., come precedentemente precisato nei §§ 9, 9.1 e 9.2.

Tuttavia, questo assunto non rende illegittima l'acquisizione, né preclude l'utilizzabilità dei dati relativi alle comunicazioni intercorse attraverso il sistema criptato [redacted] 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.

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

Invero, gli atti 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 e non è contestato nel 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.

Ora, secondo i principi di diritto precedentemente enunciati, anche a voler ritenere che detti atti siano qualificabili come risultati di intercettazioni di conversazioni o comunicazioni, la loro acquisizione può essere effettuata sulla base di o.e.i. emesso dal pubblico ministero in assenza di preventiva autorizzazione del giudice, in quanto tale autorizzazione non è richiesta nell'ordinamento italiano per l'utilizzazione degli esiti di intercettazioni in procedimenti diversi da quelli in cui sono state disposte.

Inoltre, sempre sulla base dei principi di diritto precedentemente enunciati, deve escludersi il mancato rispetto del requisito di cui all'art. 6, paragrafo 1, lett. *b)*, Direttiva cit. anche a voler ritenere che l'o.e.i. abbia ad oggetto l'acquisizione dei risultati di intercettazioni effettuate attraverso l'inserimento di un captatore informatico sui *server* di una piattaforma criptata. Si è infatti evidenziato che

questa modalità investigativa è compatibile con la disciplina delle intercettazioni prevista nell'ordinamento italiano.

Né vi sono dubbi che gli atti ottenuti mediante o.e.i. siano stati richiesti in quanto ritenuti «rilevanti ed indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza».

Non può poi ritenersi che l'asserita violazione delle garanzie procedimentali di cui all'art. 268, commi 6, 7 e 8, cod. proc. pen. possa rilevare ai fini delle condizioni di ammissibilità di cui all'art. 6, paragrafo 1, lett. *b)*, Direttiva cit. Le garanzie indicate, infatti, non costituiscono condizioni per l'acquisizione dei risultati di intercettazioni disposte in altro procedimento, ma rilevano in una fase successiva e di controllo, e la loro attuazione può essere differita fino alla chiusura delle indagini preliminari, anche dopo l'utilizzazione degli esiti delle captazioni a fini cautelari. Invero, l'art. 268 cod. proc. pen. è stato dichiarato costituzionalmente illegittimo non nella parte in cui non prevede il deposito degli atti relativi alle intercettazioni effettuate, bensì, ben più limitatamente, nella parte in cui non prevede che, dopo la notificazione o l'esecuzione dell'ordinanza che dispone una misura cautelare personale, il difensore possa ottenere la trasposizione su nastro magnetico delle registrazioni di conversazioni o comunicazioni intercettate, utilizzate ai fini dell'adozione del provvedimento cautelare, anche se non depositate (Corte cost., sent. n. 336 del 2008).

18.3. In secondo luogo, deve ritenersi soddisfatta la condizione di ammissibilità posta dall'art. 6, paragrafo 1, lett. *a)*, Direttiva 2014/41/UE, relativa alla necessità e proporzionalità delle attività richieste mediante o.e.i., anche in considerazione dei diritti degli indagati.

Si è detto in precedenza, al § 10.2, che l'esame di tale profilo deve essere compiuto avendo riguardo al procedimento nel cui ambito è emesso l'ordine europeo di indagine. E, nella specie, l'o.e.i. risulta formulato con espresso riferimento all'acquisizione delle comunicazioni relative a persone nominativamente indicate, tra le quali i due attuali ricorrenti, in quel momento già tutte sottoposte ad indagini per i reati di partecipazione ad associazione per delinquere finalizzata al traffico internazionale di cocaina e di acquisto, detenzione, importazione e cessione di partite di tale sostanza stupefacente.

18.4. Non è deducibile in questa sede la questione concernente la decisione dell'autorità giudiziaria francese di dare esecuzione all'o.e.i., prospettata con riguardo alla violazione della legge francese, perché questa non prevederebbe l'utilizzabilità dei risultati di intercettazioni di conversazioni o comunicazioni in procedimenti diversi da quelli in cui le stesse sono stati disposti.

In effetti, come già evidenziato nel § 10.4, le questioni concernenti la fase di esecuzione, e quindi anche quelle concernenti la scelta di riconoscere ed eseguire l'o.e.i., sono proponibili solo nello Stato di esecuzione, salvo che non diano luogo

a violazioni di «diritti fondamentali» che si ripercuotono sull'utilizzazione degli elementi istruttori nel procedimento pendente in Italia.

Peraltro, l'elemento indicato dai ricorrenti per affermare la violazione della legge francese, ossia la decisione Corte EDU, 29/03/2005, Matheron c. Francia, non dimostra l'esistenza di un divieto, nell'ordinamento transalpino, di utilizzare i risultati di intercettazioni in procedimenti diversi.

18.5. Né può dirsi che, nel presente procedimento, sia stata accertata la violazione di «diritti fondamentali».

18.5.1. Innanzitutto, i dati probatori trasmessi dall'autorità giudiziaria francese sono stati acquisiti in un procedimento penale pendente davanti ad essa sulla base di provvedimenti autorizzativi adottati da un giudice in relazione ad indagini per gravi reati, ed ampiamente motivati in ordine all'esistenza in concreto dei presupposti ritenuti necessari dalla giurisprudenza della Corte EDU.

Invero, dall'esame alle ordinanze emesse dal Giudice Istruttore del Tribunale di Parigi, allegate dalla difesa alla richiesta di riesame, e prodotte in questa sede, si evince che i reati per i quali le operazioni sono state disposte sono quelli di associazione per delinquere finalizzata al traffico di sostanze stupefacenti, di traffico di sostanze stupefacenti, di fornitura di prestazioni di crittografia non autorizzate, e di fornitura e importazione di mezzi di crittografia non autorizzati.

Il ricorso al sistema [redacted] inoltre, per le modalità di accesso, per la impenetrabilità dall'esterno, e per l'utilizzo che risulta esserne stato fatto, costituisce una concreta e specifica fonte indiziante a carico dei singoli utenti proprio con riguardo a tali reati.

Si può preliminarmente osservare che il sistema [redacted] per le garanzie di anonimato assicurate agli utenti, non è certamente compatibile con la disciplina italiana, che richiede l'identificazione degli stessi, mediante l'acquisizione di dati anagrafici riportati su un documento di identità, prima dell'attivazione anche di singole componenti di servizi di telefonia mobile (cfr. art. 98-*undetricies* d.lgs. 1 agosto 2003, n. 259).

Ma, soprattutto, estremamente significative sono le circostanze esposte nelle già indicate ordinanze emesse dal Giudice Istruttore del Tribunale di Parigi. I provvedimenti dell'autorità giudiziaria francese, infatti, evidenziano che: a) l'acquisto del singolo dispositivo richiedeva il versamento di parecchie migliaia di euro in funzione di una utilizzazione limitata ad alcuni mesi e, quindi, lasciava presupporre la percezione di elevati «redditi conseguenti»; b) la vendita dei singoli dispositivi avveniva in condizioni di clandestinità, tali da garantire l'anonimato del venditore e dell'acquirente, anche perché effettuata dietro pagamenti in contanti, con conseguente esclusione della tracciabilità delle operazioni; c) il gestore del sistema di crittografia garantiva il massimo anonimato delle comunicazioni, in quanto precisava esplicitamente sul sito *internet* di non conservare alcun dato

diverso da quello concernente l'apertura del rapporto e da quello della sua ultima utilizzazione; d) il sistema di crittografia era estremamente sofisticato, in quanto caratterizzato da ben quattro chiavi di cifratura, memorizzate in luoghi diversi.

Le medesime ordinanze, poi, anche facendo richiamo ad episodi specifici, rappresentano che il sistema [redacted] è stato utilizzato da organizzazioni criminali operanti in Francia, in Belgio, nei Paesi Bassi e a livello internazionale, proprio in materia di traffico di sostanze stupefacenti. Espongono, ancora, che l'inserimento del captatore informatico sui *server* della piattaforma della società [redacted] è da ritenere indispensabile perché unico mezzo per decifrare i messaggi individuali degli utilizzatori del sistema di crittografia in questione, determinare il livello di utilizzazione criminale dello stesso, identificare i dirigenti della società [redacted] che lo gestisce e conoscere i legami di costoro con le organizzazioni criminali.

18.5.2. Le motivazioni esposte nelle ordinanze emesse dal Giudice Istruttore del Tribunale di Parigi escludono anche la plausibilità della prospettazione secondo cui le autorità francesi avrebbero effettuato intercettazioni generalizzate ed indiscriminate.

Dette ordinanze, infatti, come precisato nel § 18.5.1, evidenziano specifici elementi indizianti anche nei confronti dei singoli utenti del sistema [redacted] in ordine al coinvolgimento dei medesimi nella commissione di gravi reati, in particolare in materia di traffico di sostanze stupefacenti. Invero, non può ritenersi abnorme il riferimento alle onerosissime condizioni economiche sostenute dai singoli utenti per fruire di un servizio caratterizzato da elevatissimi livelli di anonimato e di impenetrabilità; e questo a maggior ragione se si considera che, sempre alla luce di quanto indicato nelle precisate ordinanze, il sistema risulta essere stato ripetutamente utilizzato da organizzazioni criminali insediate in vari Stati e dedite al traffico anche internazionale di sostanze stupefacenti. Non va trascurato, inoltre, che, come precisato dal Giudice Istruttore del Tribunale di Parigi, le indagini miravano anche ad individuare i dirigenti della società preposta alla gestione del sistema [redacted] e a precisare il loro livello di coinvolgimento nelle attività illecite degli utenti.

18.5.3. Deve poi escludersi che l'indisponibilità delle chiavi di cifratura necessarie per rendere le comunicazioni acquisite intelligibili costituisca una violazione dei diritti di difesa e della garanzia di un giusto processo.

Come già indicato in precedenza al § 15.5.1, la conoscibilità dell'algoritmo di criptazione attiene non all'acquisibilità o all'utilizzabilità dei dati relativi alle comunicazioni, ma alla verifica di affidabilità del loro contenuto; inoltre, 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.

18.5.4. Ancora, non risulta configurabile la violazione delle garanzie previste dalla Direttiva 2014/41/UE.

Invero, anche a voler ritenere che gli atti ricevuti dall'autorità giudiziaria francese siano qualificabili come risultati di intercettazioni di conversazioni o comunicazioni, deve escludersi, in forza di quanto osservato in precedenza al § 15.5.2, che sia configurabile l'unica fattispecie di inutilizzabilità prevista dalla legge per il caso di captazioni disposte all'estero ed effettuate nei confronti di persone il cui «indirizzo di comunicazione» è attivato in Italia. Non può sostenersi, infatti, che, nella specie, le operazioni non sarebbero state consentite «in un caso interno analogo», perché le stesse sono state disposte in ordine a reati per i quali la legge italiana prevede la possibilità di ricorrere a tale mezzo di ricerca della prova, e, in particolare, per reati di associazione per delinquere finalizzata al traffico di sostanze stupefacenti e di traffico di sostanze stupefacenti.

19. Per le ragioni precedentemente esposte, deve escludersi anche la necessità di formulare alla Corte di giustizia dell'Unione Europea i quesiti prospettati dalla difesa nei ricorsi e nelle conclusioni rese in udienza.

Invero, anche ad accogliere la qualificazione giuridica prospettata dai ricorrenti, i dati ottenuti mediante o.e.i.: a) non possono in alcun modo ritenersi risultati di intercettazioni disposte dall'autorità giudiziaria francese in modo generalizzato ed indiscriminato, ovvero in difetto di indizi concreti nei confronti degli utenti del sistema [redacted] o comunque in violazione di «diritti fondamentali» o di principi costituzionali dell'ordinamento nazionale, o in contrasto con le garanzie assicurate dall'art. 31 Direttiva 2014/41/UE, per le ragioni indicate nei §§ 18.5.1, 18.5.2, 18.5.3 e 18.5.4; b) sono stati acquisiti sulla base di richieste relative a persone nominativamente indicate, tra le quali i due attuali ricorrenti, in quel momento già tutte sottoposte ad indagini in Italia per i reati di partecipazione ad associazione per delinquere finalizzata al traffico internazionale di cocaina e di acquisto, detenzione, importazione e cessione di partite di tale tipo di droga.

Di conseguenza, nella vicenda in esame, non si pongono problemi di mancato rispetto delle condizioni previste dall'art. 6, paragrafo 1, lett. *a)* e *b)*, Direttiva 2014/41/UE, o di interpretazione ed applicazione dell'art. 31 Direttiva cit.

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).

20. Prive di specificità, e comunque manifestamente infondate, sono le censure esposte nel motivo nuovo, che contestano la violazione del diritto di difesa per l'impossibilità di accedere al sistema informatico impiegato per l'analisi delle

comunicazioni intercorse sul sistema [redacted] anche al fine di verificare se le stesse siano state raggruppate e decrittate sulla base di trattamenti automatizzati, sottratti alla supervisione umana.

Innanzitutto, occorre evidenziare che la richiesta ha ad oggetto attività compiute in procedimenti penali pendenti all'estero o comunque dall'autorità giudiziaria estera in esecuzione dell'o.e.i., e, quindi, attività in linea generale non sindacabili dall'autorità giudiziaria italiana per le ragioni indicate nel § 10.4. In ogni caso, poi, la difesa non ha nemmeno allegato di aver presentato istanza di accesso al sistema informatico asseritamente impiegato per l'analisi delle comunicazioni intercorse sul sistema [redacted]

21. Del tutto inammissibile, infine, è la richiesta, formulata per la prima volta in udienza, di annullamento con rinvio dell'ordinanza impugnata per far disporre perizia al fine di assicurare in contraddittorio gli esiti del processo di decriptazione, analisi e selezione delle conversazioni acquisite.

La richiesta, in primo luogo, non espone ragioni specificamente indicative della indispensabilità di tale atto istruttorio; e, come si è evidenziato in precedenza nei §§ 15.5.1 e 18.5.4, 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. In secondo luogo, presuppone l'esame di dati non trasmessi in Italia, come le chiavi di cifratura, ed ha inoltre ad oggetto operazioni, quelle di analisi e cifratura delle comunicazioni, effettuate dall'autorità estera. In terzo luogo, non considera che il tribunale del riesame è privo di poteri istruttori in ordine ai fatti relativi all'imputazione, siccome incompatibili con la speditezza del procedimento incidentale *de libertate* (così, tra le tantissime, Sez. 6, n. 46036 del 26/10/2023, Valentino, Rv. 285475 - 01, e Sez. 1, n. 23869 del 22/04/2016, Perricciolo, Rv. 267993 - 01).

22. Alla complessiva infondatezza delle censure seguono il rigetto dei ricorsi e la condanna dei ricorrenti al pagamento delle spese processuali, a norma dell'art. 616 cod. proc. pen.

P.Q.M.

Rigetta i ricorsi e condanna i ricorrenti 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