Cassazione penale sez. un., 29/02/2024, n.23756

RITENUTO IN FATTO

1. Con ordinanza emessa in data 21 luglio 2023, il Tribunale di Reggio Calabria, ha rigettato le istanze di riesame proposte nellâ??interesse di (*omissis* 1) e (*omissis* 2) avverso lâ??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 lâ??ordinanza impugnata, sussisterebbero gravi indizi di colpevolezza a carico di (*omissis* 1) e (*omissis* 2) in ordine sia alla loro partecipazione ad unâ??associazione per delinquere finalizzata al traffico di cocaina importata dal Sudamerica, il primo nella qualitÃ 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 dellâ??individuazione dei gravi indizi di colpevolezza, lâ??ordinanza impugnata ha richiamato anche elementi costituiti da comunicazioni intercorse sulla rete criptata Sky-Ecc, acquisiti mediante ordine Europeo di indagine (dâ??ora in avanti, o.e.i.) eseguito dallâ??autoritÃ giudiziaria della Repubblica di Francia.

2. Hanno presentato ricorso per cassazione avverso lâ??ordinanza indicata in epigrafe (*omissis* 1) e (*omissis* 2), con un unico atto sottoscritto dagli avvocati M., P. e P.Mo., articolando sei motivi, preceduti da unâ??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 attivitÃ di acquisizione delle comunicazioni effettuate mediante il sistema Sky-Ecc, elementi decisivi per ritenere la sussistenza dei gravi indizi di colpevolezza.

2.1. Con il primo motivo, relativo al solo (*omissis* 2), 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., nonchÃ© vizio di motivazione, a norma dellâ??art. 606, comma 1, lett. c) ed e), cod. proc. pen., avendo riguardo alla impossibilitÃ per la difesa di conoscere le modalitÃ di acquisizione e decriptazione dei messaggi scambiati sul sistema Sky-Ecc.

Si deduce che lâ??impossibilitÃ di conoscere le modalitÃ di acquisizione e decriptazione dei messaggi scambiati sul sistema Sky-Ec. Integra una nullitÃ 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 Sky-Ecc dal 14 giugno 2019, e dei provvedimenti del Tribunale di Parigi, i quali hanno autorizzato lâ??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 attivitÃ investigativa svolta e, quindi, di articolare eccezioni in ordine alla validitÃ ed utilizzabilitÃ delle risultanze della stessa. Si precisa che lâ??osservazione dellâ??ordinanza impugnata, secondo la quale il provvedimento autorizzativo del Tribunale di Lille del 14 giugno 2019 Ã¨ stato depositato in altro procedimento, Ã¨ inadeguata, perchÃ© fa riferimento alla produzione operata in altro procedimento, ed Ã¨ comunque parziale, perchÃ© nulla dice con riguardo ai provvedimenti emessi dal Tribunale di Parigi. Si aggiunge che la presunzione di legittimitÃ degli atti procedimentali compiuti allâ??estero Ã¨ 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. e), cod. proc. pen., nonchÃ© vizio di motivazione, a norma dellâ??art. 606, comma 1, lett. e) ed e), cod. proc. pen., avendo riguardo alla inutilizzabilitÃ 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 dellâ??acquisizione delle conversazioni intercorse sul sistema Sky-Ecc, 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 Ã¨ 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 lâ??evoluzione delle indagini a carico degli stessi. Si osserva poi che il proc. n. 1589-19 R.G.N.R. DDA Reggio Calabria Ã¨ sicuramente in quiescenza, in quanto il R.O.S. ha depositato lâ??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 lâ??esistenza di risalenti notizie di reato a carico dei due ricorrenti sono costituiti, in particolare, dalla sottoposizione di unâ??utenza telefonica in uso a (*omissis* 2) ad intercettazioni tra 1â??8 agosto 2020 ed il 30 maggio 2022, e da una conversazione tra presenti intercettata il 2 maggio 2021 tra (*omissis* 3) e (*omissis* 4), consuocero di (*omissis* 1) Si osserva, ancora, che la strumentale intempestivitÃ della iscrizione del nome di una persona nel registro degli indagati

integra una violazione della disposizione di cui allâ??art. 407 cod. proc. pen. ed Ã¨, come tale sanzionabile, anche per i procedimenti anteriori allâ??entrata in vigore dellâ??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, nonchÃ© vizio di motivazione, a norma dellâ??art. 606, comma 1, lett. b), c) ed e), cod. proc. pen., avendo riguardo alla individuazione della natura delle attivitÃ di acquisizione delle comunicazioni intercorse sul sistema Sky-Ecc.

Si deduce che illegittimamente lâ??ordinanza impugnata qualifica lâ??attivitÃ di acquisizione delle comunicazioni intercorse sul sistema Sky-Ecc come attivitÃ di recupero di dati presenti nella memoria dei due server utilizzati dalla societÃ Sky Global, ubicati in R. Si rileva che tale conclusione Ã¨ viziata in particolare sia perchÃ© non risponde alle specifiche censure della difesa, le quali avevano evidenziato come le conversazioni non si trovassero nella memoria dei precisati server, sia perchÃ© si pone in contrasto con lâ??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 dellâ??ultima utilizzazione di ciascun apparecchio abilitato a connettersi al sistema Sky-Ecc. In premessa, si precisa analiticamente che le comunicazioni trasmesse dallâ??autoritÃ giudiziaria francese sono risultanze di intercettazioni, perchÃ©: a) le operazioni di acquisizione delle comunicazioni si sono caratterizzate per lâ??attivazione di Trojan Horse malaware per un periodo di ben quattro mesi, come risulta dallâ??autorizzazione del Tribunale di Parigi; b) lâ??attivitÃ Ã¨ stata autorizzata sulla base dellâ??art. 706-102-1 del Code de Procedure Penale, il quale regola lâ??impiego del Trojan Horse malaware; c) i server ubicati in Roubaix, utilizzati come â??nodoâ?• di transito delle comunicazioni, secondo quanto emerge dai provvedimenti autorizzativi emessi dal Giudice istruttore del Tribunale di Li Ile, hanno conservato al loro interno esclusivamente i dati della prima e dellâ??ultima utilizzazione di ciascun apparecchio abilitato a connettersi al sistema Sky-Ecc.

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, nonchÃ© vizio di motivazione, a norma dellâ??art. 606, comma l, lett. c) ed e), cod. proc. pen., avendo riguardo alla ritenuta applicabilitÃ della disciplina di cui allâ??art. 234-bis cod. proc. pen.

Si deduce che illegittimamente lâ??ordinanza impugnata ha ritenuto gli atti trasmessi dallâ??autoritÃ giudiziaria francese acquisibili ex art. 234-bis cod. proc. pen. Si osserva che la disciplina di cui allâ??art. 234-bis cod. proc. pen. Ã¨ non solo alternativa a quella dellâ??o.e.i.,

ma, soprattutto, inapplicabile nella specie, in quanto gli atti acquisiti costituiscono le risultanze di attivitÃ 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 qualitÃ solo perchÃ© 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, nonchÃ© vizio di motivazione, a norma dellâ??art. 606, comma 1, lett. b), c) ed e), cod. proc. pen., avendo riguardo alla ritenuta utilizzabilitÃ delle comunicazioni intercorse sul sistema Sky-Ecc.

Si deduce, in primo luogo, che gli o.e.i. aventi ad oggetto la richiesta di acquisire le comunicazioni intercorse sul sistema Sky-Ecc sono illegittimi, con conseguente inutilizzabilitÃ di quanto ottenuto, perchÃ© emessi in violazione dellâ??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 attivitÃ 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 Sky-Ecc. Si osserva che il principio di proporzionalitÃ , enunciato dallâ??art. 6, paragrafo 1, lett. a), Direttiva cit., nella specie, deve essere riferito: 1) alle modalitÃ attraverso cui sono state acquisite nel quadro del procedimento francese le prove oggetto dellâ??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 autoritÃ italiane, aventi ad oggetto il trasferimento dei dati relativi a tutti gli indirizzi degli utilizzatori del sistema Sky-Ecc in Italia. Si rileva, poi, che vi Ã¨ stata violazione del principio di cui allâ??art. 6, paragrafo 1, lett. b), perchÃ© 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 allâ??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 modalitÃ di acquisizione delle comunicazioni scambiate mediante il sistema Sky-Ecc, e per verificare la corrispondenza dei testi acquisiti in originale e dei testi decodificati, nonchÃ© la coincidenza delle utenze dei soggetti identificati come mittenti e destinatari. Si segnala che lâ??effettuazione di intercettazioni in modo generalizzato ed indiscriminato Ã¨ vietata anche dallâ??ordinamento dellâ??Unione Europea, come precisato dalla Corte di giustizia UE (si citano, in particolare, Corte giustizia, Grande Sezione, 02-03-2021, (Omissis), 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 dellâ??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 Sky-Ecc sono illegittimi, con conseguente inutilizzabilitÃ di quanto ottenuto, perchÃ© emessi in violazione dellâ??art. 9, paragrafo 1, Direttiva 2014-41-UE, siccome riguardano atti che non avrebbero potuto essere compiuti dallâ??autoritÃ giudiziaria francese. Si segnala che le comunicazioni intercorse sul sistema Sky-Ecc, siccome costituiscono il risultato di intercettazioni, in Italia sarebbero acquisibili a norma dellâ??art. 270 cod. proc. pen., e che, perÃ², la Francia non ha disposizione analoga. Si aggiunge che la libera trasmigrabilitÃ di risultanze di attivitÃ di intercettazione da un procedimento penale ad un altro Ã¨ stata ritenuta dalla Corte EDU, proprio con riferimento alla Francia, integrare una violazione dellâ??art. 8, paragrafo 2, CEDU (si cita Corte EDU, 29-03-2005, (Omissis) 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 dellâ??Unione Europea, nonchÃ© vizio di motivazione, a norma dellâ??art. 606, comma l, lett. b), c) ed e), cod. proc. pen., avendo riguardo alla ritenuta utilizzabilitÃ delle comunicazioni intercorse sul sistema Sky-Ecc.

Si deduce che gli o.e.i. aventi ad oggetto la richiesta di acquisire le comunicazioni intercorse sul sistema Sky-Ecc sono illegittimi, con conseguente inutilizzabilitÃ di quanto ottenuto, perchÃ© emessi in violazione dellâ??art. 189 cod. proc. pen., siccome attengono necessariamente anche alle attivitÃ di captazione informatica disposte al solo fine di acquisire le chiavi di cifratura custodite nei dispositivi dei singoli utenti. Si premette che la impermeabilitÃ delle comunicazioni transitanti sul sistema Sky-Ecc si fonda sulla presenza di quattro chiavi di cifratura, due presenti nei server di R e due presenti allâ??interno di ciascun dispositivo individuale, e che i captatori informatici installati sui server di R hanno avuto esclusivamente la funzione di â??catturareâ?• le chiavi di cifratura presenti allâ??interno del dispositivo di ciascun utente, mediante lâ??invio di una notifica push al singolo apparecchio, con la quale si induceva lo stesso, quando si autenticava sul sistema Sky-Ecc, a trasmettere le chiavi di cifratura presenti al loro interno. Si precisa che questa tipologia di attivitÃ investigativa Ã¨ diversa da quelle di intercettazione, perchÃ© i captatori informatici diretti ad acquisire le chiavi di cifratura presenti allâ??interno dei singoli dispositivi mobili non hanno captato comunicazioni, e, quindi, attraverso di essi si Ã¨ proceduto ad attivare un mezzo di ricerca della prova atipico. Si osserva che questo mezzo di ricerca della prova atipico Ã¨ in contrasto con la lâ?? Il riserva di legge, garantita dagli artt. 14 Cost., 8, paragrafo 2, CEDU, e 7 Carta dei diritti fondamentali dellâ??Unione Europea, e

che, quindi, sono inutilizzabili gli algoritmi di decodifica delle conversazioni intercorse sul sistema Sky-Ecc.

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

1) Sullâ??interpretazione dellâ??art. 6, par. 1, lett. a), della Direttiva 2014-41-UE:

a) se lâ??art. 6, par. 1, lett. a), della Direttiva 2014-41-UE osti a un o.e.i. volto al trasferimento di dati giÃ disponibili nello Stato di esecuzione (la Francia) derivanti da unâ??intercettazione di comunicazioni â?? in particolare, dati relativi al traffico e allâ??ubicazione, nonchÃ© registrazioni dei contenuti delle comunicazioni Â qualora, in primo luogo, lâ??intercettazione effettuata dallo Stato di esecuzione sia generalizzata e indiscriminata e riguardi perciÃ² tutti gli utenti di un determinato indirizzo di comunicazione; e qualora, in secondo luogo, venga richiesto, tramite lâ??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 nÃ© al momento in cui Ã¨ stata disposta ed eseguita la misura di intercettazione nÃ© al momento dellâ??emissione dellâ??o.e.i.;

b) se lâ??art. 6, par. 1, lett. a), della Direttiva 2014-41-UE osti a tale o.e.i. qualora lâ??integritÃ dei dati ottenuti grazie alla misura di intercettazione non possa essere verificata dalle autoritÃ dello Stato di esecuzione a causa dellâ??assoluta riservatezza dei dati.

2) Sullâ??interpretazione dellâ??art. 6, par. 1, lett. b), della Direttiva 2014-41-UE:

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

3) Sullâ??interpretazione dellâ??art. 31, par. 1 e 3, della Direttiva 2014-41-UE:

se una misura correlata con lâ??accesso clandestino ad apparecchiature terminali volta ad ottenere i dati relativi al traffico, allâ??ubicazione e alle comunicazioni di un servizio di comunicazione via internet costituisca unâ??intercettazione di telecomunicazioni ai sensi dellâ??art. 31 della Direttiva 2014-41-UE.

4) Sulle conseguenze giuridiche di unâ??acquisizione di prove in violazione del diritto dellâ??Unione: a) se il divieto di utilizzo degli elementi di prova ottenuti tramite un o.e.i. contrario al diritto dellâ??Unione, previsto dal diritto interno, sia conforme al principio di

effettivitÃ sancito dal diritto dellâ??Unione; b) se il divieto di utilizzo degli elementi di prova ottenuti tramite un o.e.i. ;

contrario al diritto dellâ??Unione sia conforme al principio di equivalenza qualora il provvedimento su cui si basa lâ??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, lâ??Avvocato M., anche per conto degli altri due co-difensori dei ricorrenti, ha chiesto lâ??anticipazione dellâ??udienza, in considerazione dellâ??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 Sky-Ecc, ottenute dallâ??autoritÃ giudiziaria italiana mediante o.e.i. inviati allâ??autoritÃ giudiziaria francese.

Nellâ??istanza, sviluppata attraverso memoria alla quale Ã¨ allegata ampia documentazione, si chiede di valutare lâ??opportunitÃ di investire le Sezioni Unite di ulteriori questioni problematiche in argomento, cosÃ¬ riassunte:

a) se, alla luce dellâ??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 reitÃ ;

b) se, ai sensi dellâ??art. 6, paragrafo 1, lettere a) e b), Direttiva 2014-41-UE, lâ??ordinamento italiano avrebbe consentito lâ??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 Sky-Ecc;

c) se, lâ??autoritÃ giudiziaria francese, trasmettendo gli esiti dellâ??attivitÃ captativa autonomamente svolta nel quadro del procedimento base transalpino, abbia o meno violato lâ??art. 10, paragrafo 5, Direttiva 2014-41-UE e, nellâ??un tempo, lâ??art. 8, paragrafo 2, CEDU, considerato che la lex loci non conosce un atto di indagine analogo a quello disciplinato dallâ??art. 270 cod. proc. pen.;

d) se, lâ??autoritÃ 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 dellâ??art. 8 paragrafo 2, CEDU, abbia trasgredito lâ??art. 11, paragrafo 1, lettera f), Direttiva 2014-41-UE;

e) se, dopo lâ??esecuzione di un o.e.i., la osservanza delle condizioni stabilite dallâ??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 lâ??esecuzione di un o.e.i., sia possibile denunciare dinanzi allâ??autoritÃ giudiziaria del Paese di emissione la violazione dellâ??art. 10, paragrafo 5, e dellâ??art. 11, paragrafo 1, lettera f), Direttiva 2014-41-UE da parte dellâ??autoritÃ giudiziaria del Paese dâ??esecuzione;

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

h) se debbono ritenersi inutilizzabili le emergenze istruttorie che lâ??autoritÃ giudiziaria del Paese dâ??esecuzione abbia trasmesso, in violazione dellâ??art. 10, paragrafo 5, o dellâ??art 11, paragrafo 1, lettera f), Direttiva 2014-41-UE;

i) quale sia la sorte processuale da riservare alla prova che lâ??autoritÃ giudiziaria francese ha trasmesso trasgredendo allâ??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 giÃ preesistente.

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

Si sottolinea in particolare: a) lâ??illegittimitÃ della intercettazione dellâ??intera utenza della piattaforma Sky-Ecc, siccome non riconducibile, di per sÃ©, al contesto della criminalitÃ 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 â??per determinare il livello di utilizzazione criminale che Ã¨ fatto da questo sistema Sky-Eccâ?•; b) la prevalenza della disciplina dellâ??o.e.i., dettata dalla Direttiva 2014-41-UE, su quella in materia di rogatoria, e, quindi, lâ??inapplicabilitÃ dei principi giurisprudenziali elaborati in relazione a questa; c) la violazione dellâ??art. 31 della Direttiva 2014-41-UE da parte dellâ??autoritÃ giudiziaria francese, in quanto la stessa avrebbe dovuto informare lâ??autoritÃ giudiziaria italiana di svolgere intercettazioni su circa 12.000 utenze Sky-Ecc localizzate in Italia, per consentire a questa di compiere approfondimenti sulla legittimitÃ delle operazioni e di inibirne la prosecuzione in caso di ravvisata illegalitÃ delle stesse; d) la violazione della sovranitÃ nazionale italiana, in quanto le attivitÃ dei captatori informatici installati sui server di R hanno comportato lâ??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 dellâ??art. 618, comma 1, cod. proc. pen., rilevando lâ??esistenza delle seguenti due questioni di diritto idonee a dare luogo ad un contrasto giurisprudenziale, anche per la pluralitÃ degli orientamenti giurisprudenziali emersi in proposito:

a) se lâ??acquisizione, mediante ordine Europeo di indagine, dei risultati di intercettazioni disposte da unâ??autoritÃ giudiziaria straniera su una piattaforma informatica criptata integri lâ??ipotesi disciplinata nellâ??ordinamento interno dallâ??art. 270 cod. proc. pen.;

b) se lâ??acquisizione, mediante ordine Europeo di indagine, dei risultati di intercettazioni disposte da unâ??autoritÃ giudiziaria straniera attraverso lâ??inserimento di un captatore informatico sui server di una piattaforma criptata sia soggetta nellâ??ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine allâ??utilizzabilitÃ dei dati raccolti.

5.1. Lâ??ordinanza di rimessione premette che le questioni processuali formulate in via preliminare rispetto a quelle concernenti lâ??utilizzabilitÃ degli atti acquisiti mediante o.e.i. sono da ritenersi infondate.

La questione posta nel primo motivo di ricorso, e riferita esclusivamente a (*omissis* 2), Ã¨ relativa alla nullitÃ di ordine generale per violazione del diritto di difesa, determinata dalla impossibilitÃ per lâ??indagato ed i suoi difensori di conoscere le modalitÃ di acquisizione e decriptazione dei messaggi scambiati sul sistema Sky-Ecc. La stessa Ã¨ ritenuta infondata perchÃ© Ã¨ indiscussa la presenza, tra gli atti del procedimento depositati a seguito della richiesta di riesame, delle trascrizioni delle comunicazioni intercorse sul sistema Sky-Ecc 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 lâ??inutilizzabilitÃ degli atti acquisiti mediante o.e.i., per il superamento del termine massimo delle indagini, determinato dalla intempestivitÃ dellâ??iscrizione del nome dei ricorrenti nel registro degli indagati. La stessa Ã¨ ritenuta infondata perchÃ© Ã¨ inapplicabile ratione temporis la disciplina di cui allâ??art. 33S-quatercod. 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, (Omissis), Rv. 244376 -01, e Sez. U, n. 16 del 21-06-2000, (Omissis), 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 Ã¨

attribuito, senza che al giudice per le indagini preliminari sia consentito stabilire una diversa decorrenza.

5.2. Lâ??ordinanza di rimessione, poi, passando allâ??esame del tema dellâ??utilizzabilitÃ delle comunicazioni acquisite mediante o.e.i., segnala alcuni profili ritenuti non oggetto di contrasto interpretativo.

Rileva, innanzitutto, che le attivitÃ investigative compiute in Francia sono state autorizzate dal Giudice istruttore ed appaiono legittimamente eseguite nellâ??ambito di quellâ??ordinamento, anche perchÃ© 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 dellâ??8 aprile 2022 del Consiglio Costituzionale).

Osserva, poi, che deve escludersi la violazione dellâ??art. 31 Direttiva 2014-41-UE, e dellâ??art. 100-8 del codice di procedura penale francese, prospettata per la violazione della sovranitÃ e della giurisdizione italiana, determinata dallâ??avere le attivitÃ di intercettazione riguardato numerosi utenti del sistema SkyÂEcc 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 allâ??art. 24, comma 2, D.Lgs. cit., il controllo del giudice italiano, nel caso di notificazione delle attivitÃ di intercettazione disposte dallâ??autoritÃ giudiziaria straniera senza richiesta di assistenza tecnica, Ã¨ limitato alla sola verifica della corrispondenza del titolo di reato per il quale si procede allâ??estero con il catalogo dei reati previsti dallâ??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 proporzionalitÃ determinati dal â??trasferimentoâ?• in Italia delle comunicazioni intercorse sul sistema Sky-Ecc, 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 (lâ??individuazione della disciplina applicabile in tema di acquisizione e di utilizzabilitÃ delle comunicazioni acquisite mediante o.e.i.), lâ??ordinanza di rimessione premette che lâ??istituto giuridico di riferimento non puÃ² essereâ?? costituito dallâ??art. 234-bis cod. proc. pen. Rileva, in proposito, che lâ??art. 27, paragrafo 1, della Convenzione di Budapest esclude la possibilitÃ di applicare le norme pattizie da essa previste, â??qualora vi sia un trattato, un accordo o legislazione in vigoreâ?•, e tale Ã¨ 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,

(Omissis), Rv. 285543 -01, 02, 03; Sez. 6, n. 48838 del 11-10-2023, (Omissis), Rv. 285599 -01, 02; Sez. 6, n. 46482 del 27-09-2023, (Omissis), Rv. 285363 -01, 02, 03, 04).

Lâ??ordinanza, quindi, segnala che due sono le prospettive plausibili.

Secondo un primo orientamento, la disciplina applicabile Ã¨ 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, (Omissis), cit.; Sez. 6, n. 46482 del 27-09-2023, (Omissis), cit.), e, quindi, quella dettata dallâ??art. 254-bis cod. proc. pen. Ad avviso di queste decisioni, non Ã¨ applicabile la disciplina delle intercettazioni, che presuppone la presenza di flussi di comunicazioni in atto, e che non Ã¨ estensibile ai casi in cui vengano acquisite comunicazioni giÃ avvenute, assimilabili, quindi, a corrispondenza.

Lâ??ordinanza evidenzia che questa soluzione comporta lâ??esigenza di valutare il rispetto dei principi di proporzionalitÃ 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 lâ??acquisizione, da parte dellâ??autoritÃ giudiziaria italiana, dei risultati di intercettazioni effettuate dallâ??autoritÃ giudiziaria estera nellâ??ambito di un proprio procedimento.

Lâ??ordinanza di rimessione rileva che questa qualificazione giuridica della vicenda determinerebbe la necessitÃ di valutare le condizioni per la valida trasmigrazione di tali elementi di prova secondo le categorie dellâ??ordinamento processuale italiano, che rinviene una specifica disciplina in tema di intercettazioni nellâ??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 legittimitÃ delle operazioni di intercettazione disposte nel processo originario (si citano Sez. U, n. 45189 del 17-11-2004, (Omissis), Rv. 229245 -01; Sez. 6, n. 36874 del 13-06-2017, (Omissis), Rv. 270812 -01; Sez. 1, n. 42006 del 28-10-2010, (Omissis), Rv. 249109 -01). Aggiunge che la necessitÃ 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, (Omissis), C-746-18, e Corte giustizia, Grande Sezione, 21-12-2023, G.K., C-281-22) .

Lâ??ordinanza di rimessione, perÃ², evidenzia che, secondo una decisione (Sez. 6, n. 46482 del 27-09-2023, (Omissis), Rv. 285363 -02), la verifica di utilizzabilitÃ degli atti â??importatiâ?• non sarebbe necessaria, perchÃ© non prevista dallâ??art. 270 cod. proc. pen. neppure per il trasferimento di intercettazioni nei procedimenti interni.

Osserva, poi, che lâ??inquadramento della vicenda nellâ??ambito del trasferimento dei risultati di intercettazioni di altro procedimento pone un ulteriore problema, ovverossia quello della legittimitÃ dellâ??uso del captatore informatico sul server di una piattaforma elettronica al fine di acquisire le chiavi di decrittazione delle comunicazioni. Si rileva che lâ??uso di questa tecnica investigativa potrebbe essere ritenuta parte dellâ??attivitÃ intercettativa di un flusso di comunicazioni, oppure attivitÃ atipica, anche perchÃ©, 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 Ã¨ autorizzato soltanto ai fini dellâ??inserimento su un dispositivo elettronico portatile.

5.4. Relativamente alla seconda questione (diritto della difesa di poter disporre dellâ??algoritmo per la decrittazione delle comunicazioni), lâ??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, (Omissis), non mass., con riguardo alle comunicazioni sul sistema Sky-Ecc, nonchÃ© Sez. 4, n. 49896 del 05-10-2019, (Omissis), Rv. 277949 -03, in fattispecie relativa a messaggi scambiati mediante il sistema BlackBerry), salva la necessitÃ 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, (Omissis), Rv. 285284 -01).

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

Segnala, infine, che, alla stregua di un ulteriore orientamento, emerso con specifico riferimento alle comunicazioni intercorse sul sistema Sky-Ecc, il diritto ad avere conoscenza dellâ??algoritmo non Ã¨ riconosciuto dalla legge italiana: questa prevede che il difensore dellâ??indagato possa accedere al verbale delle operazioni di cui allâ??art. 268 cod. proc. pen. e alle registrazioni, ma non anche ai mezzi tecnici, hardware e software, utilizzati per lâ??intrusione nelle conversazioni intercettate o per decodificarne il contenuto (si citano Sez. 6, n. 46390 del 26-10-2023, (Omissis), 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 allâ??odierna camera di consiglio.

Con istanze trasmesse il 22 gennaio 2024 e il 23 gennaio 2024, rispettivamente, lâ??Avvocato M., quale difensore di entrambi i ricorrenti, e lâ??Avvocato P., quale difensore di (*omissis* 1), hanno chiesto di poter discutere oralmente la causa.

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

7. In data 12 febbraio 2024, la Procura generale ha presentato memoria, nella quale sostiene, con ricchezza di argomenti, che la soluzione della legittimitÃ dellâ??acquisizione delle comunicazioni trasmesse dallâ??autoritÃ 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 dellâ??Unione Europea, nonchÃ© vizio di motivazione, a norma dellâ??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 lâ??analisi delle comunicazioni intercorse sul sistema Sky-Ecc.

Si premette che: a) secondo quanto rappresentato nellâ??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 attivitÃ 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, Ã¨ illegittimo impedire agli indagati di avere contezza piena dellâ??attivitÃ 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 dellâ??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 autoritÃ olandesi, come indicato dalla dottrina specialistica, presenta margini di fallibilitÃ .

9. In data 23 febbraio 2024, lâ??Avvocato M., nellâ??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 dellâ??art. 6, par. 1, lett. a) e b), Direttiva 2014-41-UE; b) la violazione dellâ??art. 31 Direttiva 2014-41-UE; c) lâ??inutilizzabilitÃ degli algoritmi di decodifica captati dai singoli dispositivi criptati; d) lâ??illegittimitÃ 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:

â??Se lâ??acquisizione, mediante ordine Europeo di indagine, dei risultati di intercettazioni disposte da un â??autoritÃ giudiziaria straniera su una piattaforma informatica criptata integri lâ??ipotesi disciplinata nellâ??ordinamento interno dallâ??art. 270 cod. proc. pen.â?•;

â??Se lâ??acquisizione, mediante ordine Europeo di indagine, dei risultati di intercettazioni disposte da un â??autoritÃ giudiziaria straniera attraverso lâ??inserimento di un captatore informatico sui server di una piattaforma criptata sia soggetta nellâ??ordinamento interno a un controllo giurisdizionale, preventivo o successivo, in ordine allâ??utilizzabilitÃ dei dati raccoltiâ?•.

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

Tuttavia, Ã¨ necessario procedere, in via preliminare, allâ??esame delle censure esposte nei primi due motivi dei ricorsi, perchÃ© il loro eventuale accoglimento renderebbe superfluo lo scrutinio delle questioni relative allâ??utilizzabilitÃ degli elementi posti a base dellâ??affermazione di sussistenza dei gravi indizi di colpevolezza.

3. Le censure formulate nel primo motivo, nellâ??interesse del solo (*omissis* 2), denunciano la violazione del diritto di difesa, giÃ eccepita in sede di interrogatorio di garanzia, con riferimento allâ??omessa acquisizione agli atti del procedimento dei provvedimenti del Tribunale di Lille e del Tribunale di Parigi che hanno disposto lâ??attivitÃ investigativa in Francia, e, comunque, al mancato deposito degli stessi, unitamente allâ??ordinanza cautelare, siccome necessari per poter controllare validitÃ ed utilizzabilitÃ del materiale ricevuto tramite o.e.i.

Le doglianze appena sintetizzate, per come prospettate, non riguardano in realtÃ 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 allâ??autoritÃ giudiziaria francese, gli atti di indagine poi acquisiti dallâ??autoritÃ giudiziaria italiana mediante o.e.i.

CiÃ² posto, va in primo luogo rilevato che non risultano, nÃ© sono indicate, disposizioni da cui desumere la giuridica necessitÃ dellâ??acquisizione e del deposito, nel procedimento in Italia, dei provvedimenti dellâ??autoritÃ giudiziaria straniera aventi ad oggetto lâ??autorizzazione di attivitÃ di indagine in un procedimento pendente davanti ad essa, i cui esiti sono stati successivamente richiesti dallâ??autoritÃ giudiziaria italiana mediante o.e.i.

Lâ??art. 78 disp. att. cod. proc. pen., nel disciplinare lâ??acquisizione di atti di un procedimento penale compiuti da autoritÃ giudiziaria straniera, non richiede anche lâ??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 lâ??acquisizione di atti compiuti o formati in altro procedimento sulla base di un provvedimento dellâ??autoritÃ giudiziaria, ossia quella relativa ai risultati di intercettazioni di conversazioni o di comunicazioni, dettata dallâ??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, lâ??orientamento consolidato della giurisprudenza di questa Corte ritiene che: a) ai fini dellâ??utilizzabilitÃ 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 lâ??AutoritÃ giudiziaria competente per il â??diversoâ?• procedimento, dei verbali e delle registrazioni delle intercettazioni medesime (cosÃ¬, per tutte, Sez. U, n. 45189 del 17-11-2004, (Omissis), Rv. 229244 -01, nonchÃ©, 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, (Omissis), Rv. 2855579 -02); b) spetta alla parte che eccepisce nel procedimento ad quem la mancanza o lâ??illegittimitÃ dellâ??autorizzazione, e si oppone allâ??utilizzabilitÃ degli esiti di intercettazioni di conversazioni o comunicazioni in un procedimento diverso da quello nel quale esse furono disposte, lâ??onere di produrre il decreto autorizzativo, in modo da consentire al giudice di verificare lâ??effettiva inesistenza nel procedimento a quo del controllo giurisdizionale prescritto dallâ??art. 15 Cost. (cfr., tra le tante, Sez. 2, n. 6947 del 29-10-2019, dep. 2020, (Omissis), Rv. 278246 -01, e Sez. 6, n. 41515 del 18-09-2015, (Omissis), Rv. 264741 -01).

4. Le censure esposte nel secondo motivo, nellâ??interesse di entrambi i ricorrenti, denunciano lâ??inutilizzabilitÃ degli atti acquisiti mediante o.e.i., perchÃ© ottenuti successivamente al decorso del termine massimo delle indagini preliminari.

In proposito, occorre premettere che la disciplina in tema di accertamento della tempestivitÃ delle iscrizioni nel registro delle notizie di reato, oggi prevista dallâ??art. 335-quater cod. proc. pen., non si applica, a norma dellâ??art. 88-bis D.Lgs. 10 ottobre 2022, n. 150, cosÃ¬ come inserito dallâ??art. 5-sexies D.L. 31 ottobre 2022, n. 162, convertito, con modificazioni, dalla legge 30 dicembre 2022, n. 199, procedimenti pendenti alla data di entrata in vigore del 30 dicembre 2022 in relazione alle notizie di reato delle quali il pubblico ministero ha giÃ disposto lâ??iscrizione nel registro di cui allâ??art. 335 cod. proc. pen., nonchÃ© in relazione alle notizie di reato iscritte successivamente, quando ricorrono le condizioni previste dallâ??art. 12 cod. proc. pen. e, se si procede per taluno dei delitti indicati nellâ??art. 407, comma 2, cod. proc. pen., anche quando ricorrono le condizioni previste dallâ??art. 371, comma 2, lett. b) e c), cod. proc. pen.

Nella specie, secondo quanto rappresentato nellâ??ordinanza impugnata, e non confutato specificamente dalla difesa, la notizia di reato per la quale Ã¨ stata emessa lâ??ordinanza cautelare Ã¨ stata iscritta nei confronti di (*omissis* 2), 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 dellâ??art. 335-quater cod. proc. pen.

Di conseguenza, trova applicazione la precedente disciplina, in forza della quale, secondo il consolidato orientamento della giurisprudenza di legittimitÃ , 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 Ã¨ attribuito, senza che al g.i.p. sia consentito stabilire una diversa decorrenza, sicchÃ© gli eventuali ritardi indebiti nella iscrizione, tanto della notizia di reato che del nome della persona cui il reato Ã¨ attribuito, pur se abnormi, sono privi di conseguenze agli effetti di quanto previsto dallâ??art. 407, comma 3, cod. proc. pen., fermi restando gli eventuali profili di responsabilitÃ disciplinare o penale del magistrato del P.M. che abbia ritardato lâ??iscrizione (Sez. U, n. 40538 del 24-09-2009, (Omissis), Rv. 244376 -01; Sez. U, n. 16 del 21-06-2000, (Omissis), Rv. 216248 -01; Sez. 6, n. 4844 del 14-11-2018, dep. 2019, (Omissis), Rv. 275046 -01).

5. Lâ??infondatezza dei primi due motivi dei ricorsi consente di passare allâ??esame delle due questioni rimesse alle Sezioni Unite e rilevanti ai fini dellâ??utilizzabilitÃ degli elementi posti a base del giudizio di gravitÃ indiziaria da parte dellâ??ordinanza impugnata.

Le due questioni sono tra loro strettamente connesse, perchÃ© le conclusioni sulla natura giuridica da attribuire allâ??acquisizione, effettuata mediante ordine Europeo di indagine (c.d. o.e.i.), di comunicazioni scambiate su chat di gruppo mediante un sistema cifrato, e giÃ a

disposizione dellâ??autoritÃ giudiziaria straniera, hanno una diretta ricaduta sul tema della necessitÃ di preventiva o successiva verifica giurisdizionale ai fini dellâ??utilizzabilitÃ dei dati raccolti.

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

6. Secondo lâ??orientamento espresso per primo in ordine di tempo, quando, in accoglimento di o.e.i., lâ??autoritÃ giudiziaria straniera trasmette comunicazioni su chat di gruppo scambiate con sistema cifrato, le quali siano giÃ in suo possesso nellâ??ambito di procedimento penale estero, si verte nellâ??ipotesi di cui allâ??art. 234Âbis cod. proc. pen.

6.1. Alcune decisioni (cfr. in particolare: Sez. 1, n. 19082 del 13-01-2023, (Omissis), Rv. 284440-01; Sez. 1, n. 6363 del 13-10-2022, dep. 2023, (Omissis), non mass.; Sez. 1, n. 6364 del 13-10-2022, dep. 2023, (Omissis), Rv. 283998-01; Sez. 1, n. 34059 del 01-07-2022, (Omissis), non mass.) premettono che, con riferimento allâ??attivitÃ 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 lâ??attivitÃ di captazione e registrazione si riferisce a messaggi in fase di transito dallâ??apparecchio del mittente a quello del destinatario, la disciplina applicabile Ã¨ quella relativa alle intercettazioni, e, piÃ¹ precisamente, nel caso in cui lâ??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 allâ??art. 266-bis cod. proc. pen.

Dallâ??altro, quando invece lâ??attivitÃ di acquisizione e decifrazione si riferisce a comunicazioni giÃ effettuate o comunque giÃ acquisite dallâ??autoritÃ giudiziaria estera, la disposizione applicabile Ã¨ quella di cui allâ??art. 234-bis cod. proc. pen., la quale consente lâ??acquisizione di documenti e dati informatici conservati allâ??estero, anche diversi da quelli disponibili al pubblico, â??previo consenso, in questâ??ultimo caso, del legittimo titolareâ?•.

Le decisioni indicate precisano che, quando lâ??autoritÃ giudiziaria italiana riceve dallâ??autoritÃ giudiziaria straniera una â??rappresentazione comunicativa incorporata in una base materiale con metodo digitaleâ?•, ossia dati informatici, si versa nellâ??ambito dellâ??acquisizione di un documento informatico. Aggiungono, poi, che, in tal caso, ricorre anche lâ??ulteriore requisito per lâ??applicabilitÃ della disciplina di cui allâ??art. 234-bis cod. proc. pen., ossia il consenso allâ??acquisizione del â??legittimo titolareâ?•, siccome per â??legittimo

titolareâ?• deve intendersi anche la persona giuridica che di quei dati e documenti puÃ² disporre in forza di un legittimo titolo, incluse, quindi, la polizia giudiziaria o lâ??autoritÃ giudiziaria dello Stato estero.

Le tre decisioni piÃ¹ 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 legittimitÃ del procedimento di acquisizione degli atti da parte dellâ??autoritÃ giudiziaria italiana alla procedura cui questa ha fatto riferimento: lâ??ordine Europeo di indagine. Sottolineano, infatti, che lâ??o.e.i. deve avere ad oggetto prove acquisibili dello Stato di emissione, deve essere eseguito in conformitÃ della disciplina prevista nello Stato di esecuzione in relazione un atto analogo, e, in linea con il consolidato insegnamento della giurisprudenza di legittimitÃ 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 dellâ??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 attivitÃ investigative giÃ compiute; b) Ã¨ 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 dellâ??art. 132 D.Lgs. 30 giugno 2003, n. 196, perchÃ©, nella specie, lâ??attivitÃ di acquisizione dei dati Ã¨ avvenuta sotto la direzione del giudice dello Stato estero; c) non sussiste un problema di genuinitÃ del dato informatico, derivante dalla mancata ostensione dellâ??algoritmo necessario alla decriptazione dei messaggi, in quanto, secondo la scienza informatica, solo lâ??algoritmo corretto consente di ottenere un testo dotato di significato, per cui Ã¨ 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 allâ??art. 234-bis cod. proc. pen. allâ??acquisizione mediante o.e.i. di messaggi su chat di gruppo scambiati con sistema cifrato, giÃ nella disponibilitÃ dellâ??autoritÃ giudiziaria straniera, aggiungono ulteriori precisazioni.

In particolare, alcune pronunce (Sez. 3, n. 47201 del 19-10-2023, (Omissis), Rv. 285350 -01; Sez. 4, n. 37503 del 30-05-2023, (Omissis), non mass.; Sez. 4, n. 16347 del 05-04-2023, (Omissis), Rv. 284563 -01; Sez. 4, n. 16345 del 05-04-2023, (Omissis), non mass.; Sez. 4, n. 17647 del 28-03-2023, (Omissis), non mass.) segnalano che: a) Ã¨ irrilevante accertare se lâ??autoritÃ giudiziaria straniera abbia acquisito i dati ex post o in tempo reale, perchÃ© lâ??aspetto dirimente Ã¨ costituito dallâ??essere stata la richiesta italiana di o.e.i. avanzata quando i flussi di comunicazione non erano piÃ¹ in corso; b) lâ??onere di provare lâ??incompatibilitÃ degli atti

compiuti dallâ??autoritÃ giudiziaria straniera con i principi fondamentali ed inderogabili dellâ??ordinamento giuridico italiano grava su chi formula la relativa eccezione anche perchÃ© il diritto straniero Ã¨ un â??fattoâ?•.

Altra decisione (Sez. 4, n. 27775 dellâ??11-05-2023, (Omissis), non mass.) aggiunge che la qualificazione dei dati acquisiti dallâ??autoritÃ giudiziaria italiana come documenti, a norma dellâ??art. 234-bis cod. proc. pen. non pone problemi di compatibilitÃ con i principi espressi dalla Direttiva 2014-41-UE, e quindi esclude la necessitÃ di procedere ad un rinvio pregiudiziale alla Corte di giustizia UE a norma dellâ??art. 267, paragrafo 3, T.F.U.E. In particolare, in questa decisione, si rappresenta che la qualificazione dei dati ricevuti dallâ??autoritÃ giudiziaria francese come documenti esclude la necessitÃ per lâ??autoritÃ 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 Ã¨ legittimato a presentare richiesta di o.e.i. perchÃ© autoritÃ 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 dallâ??art. 31, paragrafo 1, Direttiva 2014-41-UE in relazione alle attivitÃ di intercettazione attuate da uno Stato nel territorio di un altro Stato sono posti a garanzia del principio di reciprocitÃ 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, (Omissis), Rv. 285350 -01). La sentenza precisa, altresÃ¬, con specifico riguardo al caso sottoposto al suo esame, che: a) la richiesta dellâ??autoritÃ giudiziaria italiana non era indeterminata, in quanto relativa a dati transitati su utenze riferibili ad alcuni specifici PIN, ed era stata avanzata nellâ??ambito di un procedimento nel quale erano emersi giÃ concreti indizi di reato; b) lâ??integritÃ dei dati era certificata da un â??attestato vidimato dal responsabile dellâ??organismo tecnicoâ?• incaricato dallâ??autoritÃ giudiziaria francese della materiale acquisizione dei dati.

7. Secondo un diverso orientamento, espresso da due pronunce (Sez. 6, n. 44155 del 26-10-2023, (Omissis), Rv. 285362 -01, 02, e Sez. 6, n. 44154 del 26-10-2023, (Omissis), Rv. 285284 -01, 02, 03), lâ??acquisizione, effettuata mediante un ordine Europeo di indagine, di messaggi su chat di gruppo scambiati con sistema cifrato, quando attiene ai risultati di unâ??attivitÃ di apprensione occulta di comunicazioni non â??in corsoâ?• o al sequestro di dati archiviati in un server o in altri supporti informatici, Ã¨ regolata dalla disciplina di cui allâ??art. 254-bis cod. proc. pen., e non da quella di cui allâ??art. 234-bis cod. proc. pen.

7.1. Si osserva, per un verso, che lâ??art. 234-bis cod. proc. pen. Ã¨ riferibile solo ad elementi preesistenti rispetto al momento dellâ??avvio delle indagini dellâ??autoritÃ giudiziaria straniera, o comunque formati al di fuori di quelle investigazioni, e, sotto altro profilo, che non puÃ²

parlarsi di acquisizione avvenuta con il consenso del â??legittimo titolareâ?•, perchÃ© questo si identifica nel mittente e nel destinatario del messaggio, nonchÃ© nella societÃ di gestione della piattaforma di transito della comunicazione, mentre lâ??autoritÃ giudiziaria straniera Ã¨ un mero detentore dei dati a fini di giustizia.

Ad avviso delle due decisioni, lâ??attivitÃ di acquisizione, mediante o.e.i., di messaggi su chat di gruppo scambiati con sistema cifrato, se non riferita a comunicazioni â??in corsoâ?•, deve essere, pertanto, qualificata a norma dellâ??art. 254Âbis cod. proc. pen., nellâ??ambito della disciplina del sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni.

Si precisa, innanzitutto, che, se lâ??acquisizione ha ad oggetto dati â??esterniâ?• al traffico telefonico o telematico, occorre far riferimento alle regole di cui allâ??art. 132 D.Lgs. n. 196 del 2003, mentre, se vi Ã¨ stata una captazione di comunicazioni o di flussi di comunicazioni in corso, la disciplina da applicare Ã¨ quella di cui agli art. 266 ss. cod. proc. pen.

Si segnala, poi, che lâ??art. 43, comma 4, D.Lgs. n. 108 del 2017, lascia intendere che anche le attivitÃ di trascrizione, decodificazione o decrittazione delle comunicazioni intercettate, se richieste dallâ??autoritÃ giudiziaria italiana a quella estera, debbono essere preventivamente autorizzate dal giudice.

Si sottolinea, ancora, che, con riguardo allâ??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, (Omissis), causa C-746-18) ha fissato limiti stringenti: in primo luogo, in forza del principio di proporzionalitÃ , occorre che tanto la categoria o le categorie dei soggetti interessati, quanto la durata per la quale Ã¨ richiesto lâ??accesso agli atti, siano limitate a ciÃ² che Ã¨ strettamente necessario ai fini dellâ??indagine; in secondo luogo, solo un giudice (o unâ??autoritÃ indipendente e terza rispetto al processo) puÃ² garantire un corretto controllo sulla esistenza delle condizioni sostanziali e procedurali per lâ??accesso ai dati.

Si conclude, quindi, che â??lâ??acquisizione allâ??estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione deve essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per lâ??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 ministeroâ?• (cosÃ¬, testualmente, Sez. 6, n. 44154 del 26-10-2023, cit.).

7.2. Lâ??indirizzo in esame rappresenta inoltre che una conferma delle conclusioni raggiunte Ã¨ fornita dalla piÃ¹ recente giurisprudenza della Corte costituzionale in tema di tutela della libertÃ

e segretezza della corrispondenza, ex art. 15 Cost.

Si segnala, in particolare, che secondo Corte cost., sent. n. 170 del 2023, lâ??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 attualitÃ , in rapporto allâ??interesse alla sua riservatezza, e che, secondo Corte cost., sent. n. 2 del 2023, tale tutela si connota per la â??riserva di giurisdizioneâ?•, da intendersi come â??vaglio dellâ??autoritÃ giurisdizionale (â?¦) associato alla garanzia del contraddittorio, alla possibile contestazione dei presupposti applicativi della misura, della sua eccessivitÃ e proporzione, e, in ultima analisi, consente il pieno dispiegarsi allo stesso diritto di difesaâ?•.

Si aggiunge che la giurisprudenza costituzionale si richiama a quella della Corte EDU, la quale ha ricondotto â??sotto il cono di protezione dellâ??art. 8 CEDU, ove pure si fa riferimento alla â??corrispondenzaâ?• tout court, i messaggi di posta elettronica (Corte EDU, 05-09-2017, (Omissis) c. Romania; par. 72; Corte EDU, 03-04-2007, (Omissis) c. Regno Unito, par. 41), gli s.m.s. (Corte EDU, 17-12-2020, (Omissis) c. Norvegia) e la messagistica istantanea inviata e ricevuta tramite internet (Corte EDU, (Omissis), cit., par. 74)â?•.

7.3. Sulla base di queste precisazioni in ordine alla natura dellâ??attivitÃ di acquisizione delle comunicazioni elettroniche, le decisioni indicate osservano che lâ??autoritÃ giudiziaria italiana competente ad emettere lâ??o.e.i. diretto ad ottenere tali elementi Ã¨ sÃ¬ il pubblico ministero, ma potrebbe essere necessaria una previa autorizzazione del giudice.

Si evidenzia che lâ??illegittimitÃ di un o.e.i. emesso senza la preventiva autorizzazione del giudice, quando questa Ã¨ necessaria, puÃ² essere fatta valere dalla difesa, ma produce conseguenze diversificate: se lâ??o.e.i. ha determinato lo svolgimento di unâ??attivitÃ investigativa illegittima, la genesi patologica della prova raccolta determina lâ??inutilizzabilitÃ di questa; se, invece, lâ??o.e.i. Ã¨ stato emesso al fine di acquisire una prova â??giÃ disponibileâ?• nello Stato di esecuzione, e la questione non Ã¨ stata fatta valere con successo davanti agli organi di questâ??ultimo, la verifica sulla sussistenza delle condizioni di ammissibilitÃ della prova puÃ² essere chiesta al giudice italiano.

Si richiama, in particolare, quanto giÃ affermato dalla giurisprudenza di legittimitÃ con riguardo alle intercettazioni eseguite in altro procedimento, e cioÃ¨ la sindacabilitÃ anche nel processo â??riceventeâ?• della legalitÃ del procedimento di autorizzazione ed esecuzione delle attivitÃ di captazione (si cita Sez. U, n. 45189 del 17-11-2004, (Omissis), Rv. 229244-01). Sulla base di questo paradigma, si osserva che, nel sistema della Direttiva sullâ??ordine Europeo di indagine, per lâ??acquisizione dei risultati di unâ??intercettazione giÃ svolta allâ??estero, non Ã¨ sufficiente lâ??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 sullâ??ammissibilitÃ e lâ??utilizzabilitÃ della prova secondo la propria legislazione, nella specie quella italiana.

7.4. Quanto al regime di utilizzabilitÃ 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 lâ??autonomia procedurale degli ordinamenti nazionali in tema di ammissibilitÃ e valutazione delle prove, ferma restando la necessitÃ di evitare che â??informazioni ed elementi di prova ottenuti in modo illegittimo rechino indebitamente pregiudizio a una persona sospettata di avere commesso reatiâ?• (si cita Corte giustizia, Grande Sezione, 06-10-2020, C-511-18, 512-18 e 520-18). Argomenta, poi, che lâ??ordinamento nazionale si limita ad indicare, nellâ??art. 36 D.Lgs. n. 108 del 2017, quali atti ricevuti mediante o.e.i. possano essere raccolti nel fascicolo per il dibattimento.

Osserva, perciÃ², che, ai fini in questione, deve soccorrere lâ??elaborazione consolidata della giurisprudenza in tema di rogatorie, elaborazione secondo la quale lâ??atto compiuto allâ??estero puÃ² essere eseguito anche applicando le disposizioni processuali dello Stato straniero, ma Ã¨ utilizzabile in Italia solo se non contrasta con i principi fondamentali del nostro ordinamento, tra i quali quelli della tutela dellâ??inviolabilitÃ del diritto di difesa e del contraddittorio per la prova.

Segnala, in particolare, che: a) secondo la giurisprudenza di legittimitÃ , la difesa ha diritto di ottenere la versione originale e criptata dei messaggi e le chiavi di sicurezza per la decriptazione, a pena di nullitÃ ex art. 178, lett. c), cod. proc. pen. (si cita Sez. 4, n. 49896 del 15-10-2019, (Omissis), Rv. 277949-03); b) secondo la Corte EDU, Ã¨ da ritenere compromesso il diritto di difesa in relazione a dati raccolti in un server di messaggistica crittografata, quando di essi non Ã¨ stata consentita la verifica sotto il profilo del contenuto e della integritÃ , salva la presenza di interessi concorrenti, quali la sicurezza nazionale o la necessitÃ di mantenere segreti i metodi di indagine sui reati da parte della polizia, e ferma restando, anche in questo caso, la necessitÃ di fornire allâ??imputato â??unâ??opportunitÃ adeguataâ?• per preparare la sua difesa, a norma dellâ??art. 6 CEDU (si cita Corte EDU, Grande Camera, 26-09-2023, (Omissis)C. Turchia).

8. Secondo un ulteriore orientamento, espresso da tre pronunce (Sez. 6, n. 46833 del 26-10-2023, (Omissis), Rv. 285543 -01, 02, 03; Sez. 6, n. 48838 deIlâ??11-10-2023, (Omissis), Rv. 285599 -01, 02; Sez. 6, n. 46482 del 27-09-2023, (Omissis), Rv. 285363 -01, 02, 03, 04), lâ??acquisizione, effettuata mediante un ordine Europeo di indagine, di messaggi su chat di gruppo scambiati con sistema cifrato, quando attiene ad elementi giÃ raccolti in un procedimento penale pendente davanti allâ??autoritÃ 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, puÃ² essere disposto dal pubblico ministero, senza necessitÃ di preventiva autorizzazione del giudice.

8.1. Sez. 6, n. 46482 del 27-09-2023, (Omissis), cit., premette che, nel sistema giuridico italiano, per lâ??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 superfluitÃ di un provvedimento del giudice.

Osserva che la conclusione appena indicata non si pone in contrasto con lâ??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 lâ??applicazione delle garanzie previste dallâ??art. 15 Cost., e, quindi, impone lâ??intervento del pubblico ministero, ma non anche lâ??autorizzazione del giudice.

Rileva, poi, che la corrispondenza, anche informatica, costituisce prova documentale a norma dellâ??art. 234 cod. proc. pen., e che, perÃ², Ã¨ inapplicabile la disciplina di cui allâ??art. 234-bis cod. proc. pen., perchÃ© questa disposizione attiene a materiale disponibile in rete, ovvero a materiale che, se non liberamente accessibile al pubblico, puÃ² essere acquisito con il consenso del â??legittimo titolareâ?•. Sulla base di questa premessa, conclude che la documentazione trasmessa dallâ??autoritÃ 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 allâ??acquisizione di prove giÃ raccolte nello Stato di esecuzione dellâ??o.e.i., un fondamentale punto di riferimento per lâ??individuazione delle regole giuridiche applicabili Ã¨ costituito dalla disciplina interna in materia di trasferimento di prove tra procedimenti. Evidenzia che, in linea generale, il trasferimento di prove tra procedimenti puÃ² essere richiesto con provvedimento del pubblico ministero, anche con riguardo a risultanze di intercettazioni, in quanto lâ??art. 270 cod. proc. pen., per lâ??utilizzabilitÃ di queste in un procedimento diverso da quello in cui sono state disposte, pone limiti correlati alla gravitÃ dei reati, ma non richiede alcun provvedimento autorizzatorio del giudice.

Aggiunge, poi, che la necessitÃ di un provvedimento autorizzativo del giudice italiano per lâ??acquisizione di dati giÃ nella disponibilitÃ dellâ??autoritÃ giudiziaria estera non puÃ² 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, nÃ© â??la acquisizione di documentazione elettronica posta nei dispositivi personali dellâ??utente (o negli spazi virtuali su server in suo accesso esclusivo)â?• (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 lâ??espressa precisazione contenuta nel par. 103). Ostacoli non derivano nemmeno dallâ??elaborazione della giurisprudenza della Corte EDU, e segnatamente da Corte EDU, Grande Camera, 26-09-2023, (Omissis) 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 dellâ??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 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 necessitÃ di un provvedimento motivato del giudice; b) la segretezza del sistema usato per â??mettere in chiaroâ?• i messaggi criptati non Ã¨ in contrasto con la legge italiana, perchÃ© 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 Ã¨ attivitÃ distinta dalla captazione, e, quindi, non implica il diritto di conoscere il programma o lâ??algoritmo a ciÃ² necessario, salvo che siano allegate e provate specifiche anomalie tecniche.

8.2. Conclusioni omogenee, anche se espresse nellâ??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 dellâ??11-10-2023, cit.

Entrambe le decisioni evidenziano che: a) il sistema della Direttiva 2014-41-UE, relativa allâ??ordine Europeo di indagine, â??include anche lâ??acquisizione di prove giÃ in possesso dellâ??autoritÃ di esecuzioneâ?•, come precisa il settimo Considerando di essa; b) la cooperazione giudiziaria si fonda sulla presunzione del rispetto, da parte dei Paesi membri, del diritto dellâ??Unione e dei diritti fondamentali (si cita, per unâ??affermazione relativa proprio ad un procedimento concernente lâ??o.e.i., Corte giustizia, 23-01-2018, (Omissis), CÂ367-16, par. 50); c) la mancata conoscenza, da parte della difesa, dellâ??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 Ã¨ inscindibilmente correlato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilitÃ di decriptarlo, anche solo parzialmente; d) lâ??art. 234-bis cod. proc. pen. Ã¨

inapplicabile perchÃ© trova la sua matrice nellâ??art. 32 della Convenzione di Budapest sul cybercrime, la quale si riferisce allâ??acquisizione di documentazione reperibile in internet, e non alla documentazione ottenuta mediante consegna formalmente effettuata dallâ??autoritÃ giudiziaria straniera.

Sez. 6, n. 48838 dellâ??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) nellâ??ordinamento italiano, il trasferimento della corrispondenza, come delle conversazioni intercettate, Ã¨ 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 puÃ² circolare senza la necessitÃ I di un ulteriore provvedimento del giudice in procedimenti diversi, purchÃ© 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 Ã¨ applicabile la disciplina di cui allâ??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 â??possa avere ad oggetto la trascrizione, la decodificazione o decrittazione delle comunicazioni intercettateâ?•, perchÃ© tale disciplina concerne le richieste relative allo svolgimento congiunto sia delle attivitÃ di intercettazione, sia di quelle a queste accessorie; e) lâ??omesso deposito degli atti concernenti le intercettazioni disposte nel procedimento a qua presso lâ??autoritÃ competente per il procedimento ad quem non comporta lâ??inutilizzabilitÃ dei risultati acquisiti in questâ??ultimo, in quanto tale sanzione non Ã¨ prevista nÃ© dallâ??art. 270, nÃ© dallâ??art. 271 cod. proc. pen.

9. CosÃ¬ riassunti i termini del contrasto, le Sezioni Unite ritengono innanzitutto di precisare che, con riferimento allâ??acquisizione, effettuata mediante o.e.i., di messaggi scambiati su chat di gruppo mediante un sistema cifrato, e giÃ a disposizione dellâ??autoritÃ giudiziaria straniera, non Ã¨ applicabile la disciplina di cui allâ??art. 234-bis cod. pen., perchÃ© la stessa Ã¨ alternativa e incompatibile rispetto a quella dettata in tema di o.e.i.

9.1. Lâ??art. 234-bis cod. proc. pen., introdotto dallâ??art. 2, comma 1-bis, D.L. 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, prevede testualmente: â??Ã? sempre consentita lâ??acquisizione di documenti e dati informatici conservati allâ??estero, anche diversi da quelli disponibili al pubblico, previo consenso, in questâ??ultimo caso, del legittimo titolareâ?•.

Come si evince dal contenuto appena trascritto, la disposizione disciplina non un mezzo di prova, bensÃ¬ una modalitÃ di acquisizione di particolari tipologie di elementi di prova presenti allâ??estero, che viene attuata in via â??direttaâ?• dallâ??autoritÃ giudiziaria italiana e prescinde da qualunque forma di collaborazione con le autoritÃ dello Stato in cui tali dati sono custoditi.

Il sistema dellâ??o.e.i. regola anchâ??esso una modalitÃ di acquisizione degli elementi di prova â??transfrontalieriâ?•, che, perÃ², si realizza nellâ??ambito di rapporti di collaborazione tra autoritÃ giudiziarie di Stati diversi, tutti membri dellâ??Unione Europea.

Si tratta, quindi, di discipline che si riferiscono a vicende tra loro diverse giÃ per il presupposto di applicazione: lâ??art. 234-bis cod. proc. pen. riguarda lâ??acquisizione di elementi conservati allâ??estero che prescinde da forme di collaborazione con lâ??autoritÃ giudiziaria di altro Stato; la disciplina relativa allâ??o.e.i. attiene allâ??acquisizione di elementi conservati allâ??estero da ottenere od ottenuti con la collaborazione dellâ??autoritÃ giudiziaria di altro Stato.

Si puÃ² aggiungere che il rapporto di alternativitÃ tra acquisizione di elementi istruttori operata in via diretta dallâ??autoritÃ giudiziaria procedente e acquisizione di elementi istruttori sulla base di rapporti di collaborazione con autoritÃ giudiziarie di altri Stati trova una chiara esplicitazione nella Convenzione del Consiglio dâ??Europa sulla criminalitÃ informatica, firmata a Budapest il 23 novembre 2001, nella parte in cui la stessa regola i â??poteri di indagineâ?• per l'â?•accessoâ?• a dati informatici ubicati allâ??estero rispetto allâ??autoritÃ giudiziaria procedente.

Questa Convenzione, infatti, prevede che lâ??accesso a dati informatici â??immagazzinatiâ?• in un sistema informatico ubicato allâ??estero Ã¨ effettuato nellâ??ambito di rapporti di â??mutua assistenzaâ?• tra Stati (art. 31), e, nei soli casi di dati disponibili al pubblico o resi disponibili dalla persona legalmente autorizzata alla loro divulgazione, â??senza lâ??autorizzazione di unâ??altra Parteâ?• (art. 32).

9.2. CiÃ² posto, occorre inoltre evidenziare che la Direttiva 2014-41-UE del Parlamento Europeo e del Consiglio del 3 aprile 2014, relativa allâ??ordine Europeo di indagine, assegna alla disciplina da essa dettata una funzione di preminenza, in materia di acquisizione delle prove nellâ??ambito di rapporti di collaborazione tra autoritÃ giudiziarie di piÃ¹ Stati dellâ??Unione Europea.

La volontÃ 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 giÃ a disposizione dellâ??autoritÃ giudiziaria destinataria della richiesta, risulta espressa in modo inequivocabile dagli artt. 1 e 3 e dai Considerando (6), (7) e (35).

Lâ??art. 1 precisa che lâ??o.e.i. puÃ² essere emesso anche per ottenere â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, mentre lâ??art. 3 precisa che lâ??o.e.i. â??si applica a qualsiasi atto dâ??indagine, tranne allâ??istituzione di una squadra investigativa comune e allâ??acquisizione di prove nellâ??ambito di tale squadra (â?¦)â?•.

Il Considerando (6), nel terzo periodo, rappresenta: â??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 rifiutoâ?•.

Il Considerando (7), poi, oltre a ribadire la volontÃ di predisporre un unico sistema di disciplina per lâ??acquisizione delle prove â??transfrontaliereâ?•, precisa che in queste rientrano anche quelle giÃ a disposizione dellâ??autoritÃ giudiziaria destinataria della richiesta. CosÃ¬ prevede: â??Tale nuova impostazione si basa su un unico strumento denominato ordine Europeo di indagine (OEI). Lâ??OEI deve essere emesso affinchÃ© nello Stato che lo esegue (lo â??Stato di esecuzioneâ?•) siano compiuti uno o piÃ¹ atti di indagine specifici ai fini dellâ??acquisizione di prove. CiÃ² include anche lâ??acquisizione di prove giÃ in possesso dellâ??autoritÃ di esecuzioneâ?•.

Il Considerando (35), ancora, stabilisce la prevalenza della Direttiva 2014-41-UE su tutti gli altri strumenti internazionali, statuendo: â??Nei casi in cui Ã¨ fatto riferimento allâ??assistenza giudiziaria nei pertinenti strumenti internazionali, come nelle convenzioni concluse in seno al Consiglio dâ??Europa, dovrebbe essere inteso che lâ??applicazione della presente direttiva tra gli Stati membri vincolati dalla stessa Ã¨ preminente rispetto a dette convenzioniâ?•.

Il principio di completezza della disciplina dellâ??o.e.i. non Ã¨ in alcun modo derogato nellâ??ordinamento italiano, come desumibile dalle seguenti disposizioni.

Lâ??art. 1 D.Lgs. 21 giugno 2017, n. 108, rubricato â??Norme di attuazione della direttiva 2014-41-UE del Parlamento Europeo e del Consiglio del 3 aprile 2014, relativa allâ??ordine Europeo di indagine penaleâ?•, infatti, cosÃ¬ statuisce espressamente: â??Il presente decreto attua nellâ??ordinamento interno la direttiva 2014-41-UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 (â?¦), relativa allâ??ordine Europeo di indagine penale (â?¦) Lâ??art. 2, comma 1, lett. a), D.Lgs. cit., a sua volta, precisa che lâ??ordine Europeo di indagine puÃ² essere emesso anche â??per acquisire informazioni o prove che sono giÃ disponibiliâ?•.

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 dallâ??autoritÃ giudiziaria italiana mediante o.e.io, Ã¨ necessario esaminare innanzitutto quali sono le regole generali di tale sistema normativo.

10.1. Profilo preliminare, e fondamentale, Ã¨ quello che attiene alle condizioni di ammissibilitÃ dellâ??o.e.i.: solo se lâ??o.e.i. Ã¨ 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 dellâ??ordinamento nazionale di carattere generale sono estremamente laconiche. In particolare, lâ??art. 27, comma 1, D.Lgs. n. 108 del 2017 si limita a prevedere, in linea generale, che â??il pubblico ministero e il giudice che procede possono emettere, nellâ??ambito delle relative attribuzioni, un ordine di indagine e trasmetterlo direttamente allâ??autoritÃ di esecuzioneâ?•. PiÃ¹ in generale, lâ??art. 1 D.Lgs. cito, rubricato â??Disposizioni di principioâ?•, prevede che il D.Lgs. n. 108 del 2017 â??attua nellâ??ordinamento interno la direttiva 2014-41-UEâ?•.

Disposizioni piÃ¹ 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 nellâ??art. 1 D.Lgs. cit. induce a ritenere applicabili anche agli o.e.i. emessi dallâ??autoritÃ giudiziaria italiana t le condizioni di ammissibilitÃ previste dallâ??art. 6, paragrafo 1, Direttiva 2014-41-UE.

10.2. La cogenza delle prescrizioni appena indicate, nella prospettiva di assicurare la effettivitÃ del diritto Euro-unitario, Ã¨ espressamente sottolineata dal paragrafo 2 dellâ??art. 6 della Direttiva (â??Le condizioni di cui al paragrafo 1 sono valutate dallâ??autoritÃ di emissione in ogni casoâ?•).

Questo articolo, al paragrafo 1, prevede che lâ??autoritÃ richiedente â??puÃ² emettere un o.e.i. solamente quando ritiene soddisfatte le seguenti condizioni: a) lâ??emissione dellâ??o.e.i. Ã¨ necessaria e proporzionata ai fini del procedimento di cui allâ??art. 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata; e b) lâ??atto o gli atti di indagine richiesti nellâ??o.e.i. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogoâ?•.

Il giudizio sulla sussistenza della prima condizione (necessitÃ e proporzionalitÃ) deve essere compiuto avendo riguardo al procedimento nel cui ambito Ã¨ emesso lâ??ordine Europeo di indagine. In questo senso, univoche sono le indicazioni fornite sia dallâ??art. 4 Direttiva cit., sia dal Considerando (11) della medesima Direttiva. Invero, lâ??art. 4 Direttiva cit., espressamente richiamato dallâ??art. 6, fa riferimento al procedimento nel quale Ã¨ emesso lâ??o.e.i. Il Considerando (11) della Direttiva cit., poi, precisa che â??Lâ??autoritÃ di emissione dovrebbe pertanto accertare se le prove che si intende acquisire sono necessarie e proporzionate ai fini del

procedimento, se lâ??atto di indagine scelto Ã¨ necessario e proporzionato per lâ??acquisizione di tali prove, e se Ã¨ opportuno emettere un o.e.i. affinchÃ© un altro Stato membro partecipi allâ??acquisizione di tali proveâ?•.

Il giudizio sulla sussistenza della seconda condizione (ammissibilitÃ dellâ??atto richiesto alle stesse condizioni in un caso interno analogo) presuppone lâ??individuazione del â??tipoâ?• di atto oggetto di o.e.i.

Come osservato in dottrina, essa postula una valutazione in astratto, ed Ã¨ quindi logicamente preliminare, mentre lâ??altra condizione, ossia quella concernente la necessitÃ e la proporzionalitÃ dellâ??atto richiesto, implica una valutazione in concreto, rapportata allo specifico procedimento nel cui ambito Ã¨ stato emesso lâ??o.e.i.

Non mancano, inoltre, disposizioni che dettano condizioni di ammissibilitÃ 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 dellâ??emissione di un o.e.i., secondo quanto precisa lâ??art. 14, paragrafo 2, Direttiva cit., possono essere oggetto di controllo successivo, e precisamente â??impugnateâ?•, solo â??mediante unâ??azione introdotta nello Stato di emissioneâ?•, salvo la necessitÃ di assicurare tutela ai diritti fondamentali nello Stato di esecuzione; e, perÃ², â??unâ??impugnazione non sospende lâ??esecuzione dellâ??atto di indagine, a meno che ciÃ² non abbia tale effetto in casi interni analoghiâ?• (art. paragrafo 6, Direttiva cit.).

10.3. La fase di esecuzione di un o.e.i. emesso dallâ??autoritÃ 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, allâ??art. 1, lâ??esigenza del â??rispetto dei principi dellâ??ordinamento costituzionale e della Carta dei diritti fondamentali dellâ??Unione Europea in tema di diritti fondamentali, nonchÃ© in tema di diritti di libertÃ e di giusto processoâ?•.

Per altro verso, detta, allâ??art. 35, disposizioni sulla utilizzabilitÃ degli atti compiuti e delle prove assunte allâ??estero. Lâ??art. 35 cit., precisamente, prevede lâ??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 facoltÃ loro consentite dalla legge italiana; c) dei verbali di dichiarazioni non ripetibili assunte allâ??estero a seguito di o.e.i. e non acquisite in contraddittorio nei casi e con le modalitÃ di cui allâ??art. 512Âbis cod. proc. pen.

Per completezza, Ã¨ utile precisare che la garanzia del rispetto dei principi della Carta dei diritti fondamentali dellâ??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 dellâ??Uomo. Invero, la Carta di Nizza, come precisa il preambolo e puntualizzano le annesse â??Spiegazioniâ?•, il cui valore giuridico Ã¨ formalmente sancito dallâ??art. 52, paragrafo 7, della Carta, â??riaffermaâ?• espressamente anche i diritti derivanti dalla Convenzione Europea dei Diritti dellâ??Uomo e delle LibertÃ fondamentali, nonchÃ© dalla giurisprudenza della Corte Europea dei diritti dellâ??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 utilizzabilitÃ degli atti acquisiti nel procedimento davanti allâ??autoritÃ di emissione.

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

Invero, significative sono le previsioni relative alla esperibilitÃ di mezzi di impugnazione anche nello Stato di esecuzione, a scambi reciproci di informazioni anche sui mezzi di impugnazione contro il riconoscimento e lâ??esecuzione di un o.e.i., e allâ??obbligo per lo Stato di emissione di tener conto dellâ??esito delle impugnazioni concernenti il riconoscimento e lâ??esecuzione dellâ??o.e.i.

NÃ© appare seriamente ipotizzabile che identiche questioni possano essere proposte sia nello Stato di esecuzione, sia nello Stato di emissione. Emblematica, in proposito, Ã¨ la regola che esclude la proponibilitÃ di questioni relative alle ragioni di merito dellâ??emissione dellâ??o.e.i. nello Stato di esecuzione, stabilita dallâ??art. 14, paragrafo 2, Direttiva cit., â??fatte salve le garanzie dei diritti fondamentali nello Stato d i esecuzioneâ?•.

Tuttavia, la medesima Direttiva evidenzia la necessitÃ di assicurare il rispetto dei â??diritti fondamentaliâ?• da parte dellâ??autoritÃ giudiziaria dello Stato di emissione anche con riguardo alle attivitÃ compiute nello Stato di esecuzione.

Lâ??art. 14 cit., paragrafo 2, stabilisce che le ragioni di merito in ordine allâ??emissione dellâ??o.e.i. possono essere fatte valere â??soltanto mediante unâ??azione introdotta nello Stato di emissioneâ?•, â??fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzioneâ?•. Ancor piÃ¹ significativamente, perÃ², al paragrafo 7, secondo periodo, con una previsione specificamente riferita alla valutazione delle prove nel procedimento ad quem, dispone: â??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 lâ??o.e.i.â?•.

Inoltre, con una regola di principio e di â??chiusuraâ?• del sistema, lâ??art. l, paragrafo 4, Direttiva cito statuisce: â??La presente direttiva non ha lâ??effetto di modificare lâ??obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dallâ??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 autoritÃ giudiziarieâ?•.

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 dellâ??utilizzabilitÃ di atti acquisiti mediante o.e.i. dallâ??autoritÃ giudiziaria italiana, Ã¨ necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dellâ??Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo, ma non anche lâ??osservanza, da parte dello Stato di esecuzione, di tutte le disposizioni previste dallâ??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 lâ??art. l, evidenziano, come principio generale, lâ??esigenza di assicurare il rispetto dei diritti fondamentali, e, tra questi, i diritti della difesa e ad un giusto processo.

Dallâ??altro, poi, nÃ© lâ??art. 36 D.Lgs. n. 108 del 2017, nÃ© altre disposizioni del medesimo D.Lgs. o della Direttiva 2014-41-UE prevedono, ai fini dellâ??utilizzabilitÃ degli atti formati allâ??estero, la necessitÃ di una puntuale applicazione di tutte le regole che lâ??ordinamento giuridico italiano fissa, in via ordinaria, per la formazione degli atti corrispondenti formati sul territorio nazionale. Anzi, lâ??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 lâ??o.e.i., stabilisce: â??fatte salve le norme procedurali nazionaliâ?• (dizione, questâ??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 legittimitÃ , secondo cui, in tema di rogatoria internazionale, trovano applicazione le norme processuali dello Stato in cui lâ??atto viene compiuto, con lâ??unico limite che la prova non puÃ² essere acquisita in contrasto con i principi fondamentali dellâ??ordinamento giuridico italiano e dunque con il diritto di difesa (Sez. 2, n. 2173 del 22-12-2016, dep. 2017, (Omissis), Rv. 269000 -01, la quale ha ritenuto esente da censure il provvedimento impugnato che aveva respinto lâ??eccezione di inutilizzabilitÃ di intercettazioni ambientali disposte ed acquisite dallâ??autoritÃ olandese, osservando che la procedura penale olandese in tema di intercettazioni era conforme ai principi garantiti dallâ??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 Ã¨ di quattro settimane, con possibilitÃ di rinnovo).

Questa Corte ha altresÃ¬ affermato che, in materia di rogatoria internazionale, lâ??atto istruttorio assunto allâ??estero Ã¨ inutilizzabile solo quando venga prospettata lâ??assenza nellâ??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, (Omissis), Rv. 253797 -01).

10.6. Ai fini dellâ??accertamento del rispetto dei diritti fondamentali, assumono rilievo i principi della presunzione relativa di conformitÃ ai diritti fondamentali dellâ??attivitÃ svolta dallâ??autoritÃ giudiziaria estera nellâ??ambito di rapporti di collaborazione ai fini dellâ??acquisizione di prove, e dellâ??onere per la difesa di allegare e provare il fatto dal quale dipende la violazione denunciata.

Il principio della presunzione di legittimitÃ dellâ??attivitÃ compiuta allâ??estero ai fini dellâ??acquisizione di elementi istruttori Ã¨ oggetto di costante e generale enunciazione da parte della giurisprudenza di questa Corte (cfr., ex plurimis: Sez. 6, n. 44882 del 04-10-2023, (Omissis), 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, (Omissis), Rv. 279246 -01).

Nel sistema della Direttiva 2014-41-UE, poi, Ã¨ espressamente riconosciuto il principio della â??presunzione relativa che gli altri Stati membri rispettino il diritto dellâ??Unione e, in particolare, i diritti fondamentaliâ?• (Corte giustizia, 11-11-2021, (Omissis), C-852-19, par. 54; cfr., nello stesso senso, Corte giustizia, 08-12-2020,

(Omissis), C-584-19, par. 40). Tale principio, del resto, trova una precisa base testuale nel Considerando (19) della Direttiva cit., il quale afferma:

â??La creazione di uno spazio di libertÃ , di sicurezza e di giustizia nellâ??Unione si fonda sulla fiducia reciproca e su una presunzione di conformitÃ , da parte di tutti gli Stati membri, al diritto dellâ??Unione e, in particolare, ai diritti fondamentali. Tuttavia, tale presunzione Ã¨ relativa. Di conseguenza, se sussistono seri motivi per ritenere che lâ??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, lâ??esecuzione dellâ??o.e.i. dovrebbe essere rifiutataâ?•.

Anche il principio secondo cui grava sulla difesa lâ??onere di allegare e provare il fatto dal quale dipende una causa di nullitÃ o inutilizzabilitÃ da essa eccepita Ã¨ ripetutamente e generalmente ribadito dalla giurisprudenza di legittimitÃ .

Le Sezioni Unite, in particolare, hanno affermato che, nel caso in cui una parte deduca il verificarsi di cause di nullitÃ o inutilizzabilitÃ collegate ad atti non rinvenibili nel fascicolo processuale (perchÃ© appartenenti ad altro procedimento o anche -qualora si proceda con le forme del dibattimento â?? al fascicolo del pubblico ministero), al generale onere di precisa indicazione che incombe su chi solleva lâ??eccezione si accompagna lâ??ulteriore onere di formale produzione delle risultanze documentali â?? positive o negative â?? addotte a fondamento del vizio processuale (cosÃ¬ Sez. U, n. 39061 del 16-07-2009, (Omissis), Rv. 244329 -01, e, in termini analoghi, Sez. U, n. 45189 del 17-11-2004, (Omissis), Rv. 229245 -01; tra le tante successive conformi, cfr. Sez. 5, 23015 del 19-04-2023, (Omissis), Rv. 284519 Â01, e Sez. 6, n. 18187 del 14-12-2017, dep. 2018, (Omissis), Rv. 273007 -01).

A fondamento di questa affermazione, si osserva che, â??per i fatti processuali, a differenza di quanto avviene per i fatti penali, ciascuna parte ha lâ??onere di provare quelli che adduce, quando essi non risultino documentati nel fascicolo degli atti di cui il giudice disponeâ?• (cosÃ¬ Sez. U, n. 45189 del 2004, (Omissis), cit., nonchÃ© Sez. 5, n. 1915 del 18-11-2010, dep. 2011, (Omissis), Rv. 249048 -01, e Sez. S, n. 600 del 17-12-2008, dep. 2009, (Omissis), Rv. 242551 -01). E lâ??osservazione deve essere ribadita perchÃ© lâ??art. 187, comma 2, cod. proc. pen. prevede che i fatti dai quali dipende lâ??applicazione di norme processuali sono oggetto di prova, nÃ© vi sono dati normativi da cui inferire lâ??inversione, in questo specifico ambito, della regola generale secondo cui chi afferma lâ??esistenza di un fatto Ã¨ gravato dellâ??onere della relativa prova.

Muovendo dai principi appena esposti, quindi, appare ragionevole concludere che lâ??onere di allegare e provare i fatti da cui inferire la violazione di diritti fondamentali grava sulla difesa, quando Ã¨ questa a dedurre lâ??inutilizzabilitÃ o lâ??invaliditÃ di atti istruttori acquisiti dallâ??autoritÃ giudiziaria italiana mediante O.e.i.

11. Le precisate regole generali in tema di acquisizione ed utilizzabilitÃ di elementi di prova acquisiti dallâ??autoritÃ giudiziaria italiana mediante o.e.i., se disegnano la disciplina comune di riferimento, evidenziano anche la necessitÃ di individuare il â??tipoâ?• di atto oggetto di richiesta e trasmissione nella singola vicenda.

Invero, Ã¨ in ragione del â??tipoâ?• di atto specificamente richiesto e trasmesso che Ã¨ possibile valutare la sussistenza delle condizioni di ammissibilitÃ dellâ??o.e.i., e, in particolare, quella della possibilitÃ di disporne lâ??assunzione â??alle stesse condizioni in un caso interno analogoâ?•.

Inoltre, il â??tipoâ?• 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 dellâ??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 lâ??acquisizione, da parte dellâ??autoritÃ giudiziaria italiana, di comunicazioni scambiate su chat di gruppo mediante un sistema cifrato, e giÃ a disposizione dellâ??autoritÃ giudiziaria francese.

Il fatto che le comunicazioni fossero a disposizione dellâ??autoritÃ giudiziaria francese giÃ prima della presentazione dellâ??o.e.i. da parte dellâ??autoritÃ giudiziaria italiana costituisce elemento incontroverso: in proposito, concordano lâ??ordinanza impugnata, il ricorrente e il pubblico ministero, nÃ© vi sono elementi agli atti per dubitare di questo assunto.

Risulta quindi possibile un rilievo preliminare: quanto chiesto dallâ??autoritÃ giudiziaria italiana, e consegnato dallâ??autoritÃ giudiziaria francese, attiene a â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?• (per questa definizione cfr. art. 1, paragrafo 1, secondo periodo, Direttiva 2014-41-UE, nonchÃ©, in termini analoghi, art. 2, comma 1, lett. a), D.Lgs. n. 108 del 2017).

Lâ??individuazione dellâ??oggetto dellâ??o.e.i. in â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?• ha importanti conseguenze ai fini della disciplina applicabile.

12.1. Nel sistema dellâ??o.e.i., lâ??acquisizione di â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?• Ã¨ oggetto di alcune specifiche disposizioni, di deroga alla disciplina generale, e funzionali a renderne piÃ¹ agevole la â??circolazioneâ?•.

Innanzitutto, lâ??art. 10 Direttiva 2014-41-UE stabilisce che, nel caso di â??informazioni o prove che sono giÃ in possesso dellâ??autoritÃ 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 dellâ??o.e.i.â?•, Ã¨ esclusa la possibilitÃ , per lâ??autoritÃ di esecuzione, di disporre â??un atto di indagine alternativoâ?• 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 in possesso dello Stato di esecuzione, la loro trasmissione allo Stato di emissione dovrebbe avvenire con immediatezza, perchÃ© non vi Ã¨ alcun atto di indagine da compiere.

12.2. Nella prospettiva interna, pare risolutivo il rilievo che, nellâ??ordinamento giuridico italiano, la â??circolazioneâ?• di prove giÃ formate ha una disciplina specifica e diversa da quella riservata alla â??formazioneâ?• di prove di identica tipologia.

Nel sistema processuale italiano, infatti, il pubblico ministero e, piÃ¹ in generale, la parte che vi ha interesse possono chiedere ed ottenere la disponibilitÃ di prove giÃ formate in un procedimento penale al fine di produrle in un altro procedimento penale, senza necessitÃ di alcuna autorizzazione preventiva da parte del giudice competente per questâ??ultimo. CiÃ² anche nel caso di prove, come le intercettazioni di conversazioni o di comunicazioni, per la cui formazione Ã¨ 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 giÃ 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.

Lâ??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 dellâ??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 lâ??utilizzazione di prove provenienti da altri procedimenti; e, tra queste condizioni, si ribadisce, non Ã¨ ricompresa la previa autorizzazione.

Lâ??art. 270 cod. proc. pen., a sua volta, indica i requisiti per lâ??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 allâ??art. 238 cod. proc. pen. perchÃ© riferita ad uno specifico mezzo di ricerca della prova, non prevede alcun intervento autorizzativo preventivo del giudice del procedimento di â??destinazioneâ?•, che abbia la funzione di autorizzare le parti interessate a procedere allâ??acquisizione di copia dei relativi atti. Lâ??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 lâ??onere di depositare i verbali e le registrazioni a queste relativi, senza perÃ² contenere alcun riferimento ad autorizzazioni preventive del giudice del processo di â??destinazioneâ?• per ottenere la disponibilitÃ di tali atti.

Inoltre, forse ancor piÃ¹ significativamente, lâ??art. 270, comma 3, cod. proc. pen., riconosce al pubblico ministero e ai difensori delle parti intere ssate â??la facoltÃ di esaminare i verbali e le registrazioni in precedenza depositati nel procedimento in cui le intercettazioni furono autorizzateâ?•, sempre senza prevedere autorizzazioni preventive del giudice del processo di

â??destinazioneâ?•.

Lâ??art. 78 disp. att. cod. proc. pen., rubricato â??Acquisizione di atti di un procedimento penale stranieroâ?•, ancora, dispone, in linea generale, al comma 1, che â??La documentazione di atti di un procedimento penale compiuti da autoritÃ giudiziaria straniera puÃ² essere acquisita a norma dellâ??art. 238 del codiceâ?•, e si limita ad aggiungere, al comma 2, che, per gli atti non ripetibili compiuti dalla polizia straniera, lâ??acquisizione nel fascicolo per il dibattimento Ã¨ subordinata al previo esame in contraddittorio dellâ??autore degli stessi, o al consenso delle parti.

12.3. In considerazione di quanto precedentemente indicato, puÃ² concludersi, in linea generale, che gli atti oggetto dellâ??o.e.i. costituenti â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?• possono essere legittimamente richiesti e acquisiti dal pubblico ministero italiano senza la necessitÃ di preventiva autorizzazione da parte del giudice del procedimento nel quale si vorrebbe utilizzarli.

Ed infatti, unico presupposto di ammissibilitÃ dellâ??ordine Europeo di indagine, sotto il profilo del soggetto legittimato a presentarlo, Ã¨ che â??lâ??atto o gli atti di indagine richiesti nellâ??o.e.i. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogoâ?•.

Ora, come si Ã¨ rilevato in precedenza nel par. 12.2, nellâ??ordinamento processuale penale italiano, le prove giÃ 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 necessitÃ di preventiva autorizzazione da parte del giudice competente per questâ??ultimo.

Di conseguenza, quando lâ??o.e.i. avanzato dal pubblico ministero italiano riguarda â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, 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, nÃ© altrimenti desumibile dal sistema dellâ??o.e.i.

12.4. Senza dubbio, come giÃ segnalato in precedenza al par. 12.2. in relazione alla â??circolazioneâ?• di prove tra procedimenti pendenti in Italia, il giudice al quale si chiede di utilizzare le â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, 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, sarÃ esercitato quando il pubblico ministero presenta al giudice italiano le â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, e ricevute tramite o.e.i. E allora, infatti, che il giudice puÃ² controllare se vi fossero le condizioni per emettere lâ??o.e.i., cosÃ¬ da assicurare il pertinente diritto di â??impugnazioneâ?• nello Stato di emissione previsto dallâ??art. 14, paragrafo 2, Direttiva 2014-41-UE, nonchÃ© 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 dallâ??art. 14, paragrafo 7, Direttiva cit., fermo restando che lâ??onere dellâ??allegazione e della prova in ordine ai fatti da cui desumere la violazione di tali diritti grava sulla parte interessata, come giÃ precisato nei par. 10.2, 10.3, 10.4, 10.5 e 10.6.

13. Le osservazioni di carattere generale precedentemente compiute con riguardo alla â??circolazioneâ?• delle â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, 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 dellâ??esistenza delle condizioni di ammissibilitÃ dellâ??o.e.i., in particolare di quelle di cui allâ??art. 6, paragrafo 1, Direttiva 2014-41-UE, sia di eventuali violazioni dei diritti fondamentali, occorre prendere in esame il preciso â??tipoâ?• di atto trasmesso, attesa la specificitÃ della disciplina riservata dalla normativa nazionale e sovra-nazionale ad alcuni di essi.

Nel presente procedimento, due sono le qualificazioni prospettate: secondo lâ??ordinanza impugnata, gli atti acquisiti costituiscono â??documenti informaticiâ?•; secondo il ricorrente, invece, si tratterebbe di dati concernenti il traffico, lâ??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 dellâ??indisponibilitÃ in questa sede dellâ??intero materiale acquisito mediante o.e.i., con conseguente impossibilitÃ di definire con certezza se lo stesso consista di risultati di intercettazioni, queste ultime da intendersi come attivitÃ di â??apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o piÃ¹ persone da parte di altri soggetti, estranei al colloquioâ?• (cfr., per questa definizione, in particolare, Sez. U, n. 36747 del 28-05-2003, (Omissis), Rv. 225465-01, e Corte cost., sent. n. 170 del 2023), e lâ??ininfluenza dellâ??una o dellâ??altra qualificazione ai fini della decisione dei ricorsi, come si preciserÃ in seguito.

14. Secondo lâ??ordinanza impugnata, gli atti acquisiti mediante o.e.i. dallâ??autoritÃ giudiziaria francese costituiscono â??documentiâ?•, e non â??intercettazioni di conversazioni o comunicazioniâ?•.

14.1. La qualificazione degli atti in questione come documenti implica che il parametro generale di riferimento nel sistema processuale nazionale per verificare:

lâ??esistenza delle condizioni di ammissibilitÃ dellâ??o.e.i. e lâ??eventuale violazione di diritti fondamentali sia costituito dallâ??art. 234 cod. proc. pen., il quale consente lâ??acquisizione di scritti o di â??entitÃ â?• 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 Ã¨ ostacolata dalla sola circostanza che le â??entitÃ â?• rappresentative siano comunicazioni elettroniche, data la latitudine della nozione di â??prova documentaleâ?• accolta dallâ??art. 234 cod. proc. pen. E in questo senso, infatti, si esprime lâ??orientamento ampiamente consolidato della giurisprudenza di legittimitÃ sia con riguardo ai messaggi di posta elettronica, giÃ 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, (Omissis), Rv. 278808 -02, e Sez. 3, n. 29426 del 16-04-2019, (Omissis), Rv. 276358 Â01), sia in ordine ai messaggi inviati mediante applicativo WhatsApp o s.m.s., giÃ trasmessi e conservati nella memoria di unâ??utenza cellulare (v., ex plurimis, Sez. 6, n. 22417 del 16-03-2022, (Omissis), Rv. 283319 -01, e Sez. 5, n. 1822 del 21-11-2017, dep. 2018, (Omissis), Rv. 272319 -01).

14.2. La disciplina generale di cui allâ??art. 234 cod. proc. pen., perÃ², non sempre Ã¨ 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 dallâ??art. 15 Cost. in materia di â??corrispondenzaâ?•.

Come infatti precisato dalla giurisprudenza costituzionale, â??quello di â??corrispondenzaâ?• Ã¨ concetto ampiamente comprensivo, atto ad abbracciare ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o piÃ¹ persone determinate, attuata in modo diverso dalla conversazione in presenzaâ?•, il quale â??prescinde dalle caratteristiche del mezzo tecnico utilizzatoâ?•, e si estende, perciÃ², anche alla posta elettronica ed ai messaggi inviati tramite lâ??applicativo WhatsApp, o s.m.s. o sistemi simili, â??del tutto assimilabili a lettere o

biglietti chiusiâ?• perchÃ© accessibili solo mediante lâ??uso di codici di accesso o altri meccanismi di identificazione (cosÃ¬ 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 modalitÃ utilizzata, trova applicazione â??la tutela accordata dallâ??art. 15 Cost. â?? che assicura a tutti i consociati la libertÃ e la segretezza â??della corrispondenza e di ogni altra forma di comunicazioneâ?•, consentendone la limitazione â??soltanto per atto motivato dellâ??autoritÃ giudiziaria con le garanzie stabilite dalla legge - (â?¦)â?• (cfr., ancora, testualmente, Corte cost., sent. n. 170 del 2023).

La tutela prevista dallâ??art. 15 Cost., tuttavia, non richiede, per la limitazione della libertÃ e della segretezza della corrispondenza, e, quindi, per lâ??acquisizione di essa ad un procedimento penale, la necessitÃ di un provvedimento del giudice.

Invero, lâ??art. 15 Cost. impiega il sintagma â??autoritÃ giudiziariaâ?•, il quale indica una categoria nella quale sono inclusi sia il giudice, sia il pubblico ministero (per lâ??inclusione del pubblico ministero nella nozione di â??autoritÃ giudiziariaâ?• anche nel diritto Euro-unitario, cfr., proprio con riferimento alla Direttiva 2014-41-UE, Corte giustizia, 08-12-2020, (Omissis), C-584-19).

E questa conclusione trova conferma nella disciplina del codice di rito. Lâ??art. 254 cod. proc. pen. prevede che il sequestro di corrispondenza Ã¨ disposto della â??autoritÃ giudiziariaâ?•, senza fare alcun riferimento alla necessitÃ dellâ??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, lâ??art. 353 cod. proc. pen. statuisce, in modo testuale, che lâ??acquisizione di plichi chiusi e di corrispondenza, anche in forma elettronica o inoltrata per via telematica, Ã¨ autorizzata, nel corso delle indagini, dal â??pubblico ministeroâ?•, il quale Ã¨ titolare del potere di disporne il sequestro.

14.3. La qualificazione degli atti consegnati dallâ??autoritÃ giudiziaria francese in esecuzione di o.e.i. come documenti ha specifiche conseguenze con riguardo ai presupposti di ammissibilitÃ della loro acquisizione e alla garanzia del rispetto dei â??diritti fondamentaliâ?•.

In particolare, con riguardo al presupposto di ammissibilitÃ di cui allâ??art. 6, paragrafo 1, lett. b), Direttiva 2014-41-UE, relativo alla c.d. valutazione in astratto, Ã¨ sufficiente considerare che anche lâ??acquisizione â??originariaâ?• della prova documentale, nel sistema processuale italiano, pur quando abbia ad oggetto â??corrispondenzaâ?•, per quanto appena detto nel par. 14.2., puÃ² essere disposta dal pubblico ministero, con atto motivato, senza alcuna autorizzazione del giudice, salvo il caso di sequestro effettuato nellâ??ufficio di un difensore. Di conseguenza, se lâ??ordine Europeo di indagine presentato dal pubblico ministero ha ad oggetto lâ??acquisizione di

documenti e â??corrispondenzaâ?• non costituenti â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, il rispetto della condizione che esige il potere dellâ??autoritÃ di emissione di disporre â??lâ??atto o gli atti di indagine richiesti nellâ??o.e.i. (â?¦) alle stesse condizioni in un caso interno analogoâ?• Ã¨ assicurato anche in assenza di una autorizzazione del giudice, salvo il caso di sequestro effettuato nellâ??ufficio di un difensore. A maggior ragione, quindi, e in aggiunta alle considerazioni esposte nei par. 12.2 e 12.3, lâ??acquisizione di documenti, pur se relativi a â??corrispondenzaâ?•, quando attiene a â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, puÃ² essere chiesta mediante o.e.i. presentato dal pubblico ministero, senza necessitÃ di autorizzazione del giudice.

Per quanto riguarda il rispetto dei â??diritti fondamentaliâ?•, poi, la qualificazione degli atti consegnati dallâ??autoritÃ giudiziaria francese in esecuzione di o.e.i. come documenti, specie se costituiscono â??corrispondenzaâ?•, comporta lâ??esigenza di specifica attenzione a profili â??contenutisticiâ?• degli stessi. Ad esempio, un principio generale, in materia di tutela di diritto di difesa, positivizzato nel sistema italiano dallâ??art. 103 cod. proc. pen., Ã¨ quello del divieto di sequestro e di ogni forma di controllo della â??corrispondenzaâ?• tra lâ??imputato ed il suo difensore, salvo il fondato motivo che si tratti di corpo del reato. Resta fermo, ovviamente, che lâ??onere dellâ??allegazione e della prova in ordine ai fatti da cui desumere la violazione dei â??diritti fondamentaliâ?• grava sulla parte interessata, per le ragioni indicate in precedenza nel par. 10.6.

15. Secondo il ricorso, gli atti acquisiti mediante o.e.i. dallâ??autoritÃ 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 Sky-Ecc, 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 lâ??esistenza delle condizioni di ammissibilitÃ dellâ??o.e.i. e lâ??eventuale violazione di diritti fondamentali Ã¨ costituito dalla disciplina prevista dallâ??art. 270 cod. proc. pen. (cfr., per questa indicazione, tra le altre, giÃ Sez. 1, n. 4048 del 06-07-1998, (Omissis), Rv. 211301 - 01).

In particolare, a norma dellâ??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 â??risultino rilevanti ed indispensabili per lâ??accertamento di delitti per i quali Ã¨ obbligatorio lâ??arresto in flagranzaâ?•.

Secondo il consolidato indirizzo di questa Corte, ai fini dellâ??utilizzabilitÃ 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 lâ??art. 270 cod. proc. pen. prevede esclusivamente il deposito, presso lâ??autoritÃ giudiziaria competente per il â??diversoâ?• procedimento, dei verbali e delle registrazioni delle intercettazioni medesime, nÃ© sono altrimenti previste sanzioni di inutilizzabilitÃ (Sez. U, n. 45189 del 17-11-2004, (Omissis), Rv. 229244 -01, e Sez. 1, n. 49627 del 14-11-2023, (Omissis), Rv. 285579 Â02). Sempre secondo il costante orientamento di questa Corte, grava sulla parte che eccepisce lâ??invaliditÃ o lâ??inutilizzabilitÃ delle intercettazioni provenienti da altro procedimento lâ??onere di allegare e provare il fatto dal quale dipende la patologia denunciata (Sez. U, n. 45189 del 17-11-2004, (Omissis), 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, (Omissis), Rv. 229246 -01, nonchÃ© Sez. 1, n. 11168 del 18-02-2019, (Omissis), Rv. 274996 Â-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 legalitÃ dellâ??ammissione e dellâ??esecuzione delle operazioni â?? di carattere meramente incidentale e, come tale, ininfluente nel procedimento a qua â?? riguarda esclusivamente la serietÃ e la specificitÃ 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, (Omissis), Rv. 229247 -01).

Numerose decisioni, poi, affermano che, in tema di intercettazioni disposte in altro procedimento, lâ??omesso deposito degli atti relativi, ivi compresi i nastri di registrazione, presso lâ??autoritÃ competente per il diverso procedimento, non ne determina lâ??inutilizzabilitÃ , in quanto detta sanzione non Ã¨ prevista dallâ??art. 270 cod. proc. pen. e non rientra nel novero di quelle di cui allâ??art. 271 cod. proc. pen. aventi carattere tassativo (cosÃ¬ ex plurimis: Sez. 5, n. 1801 del 16-07-2015, dep. 2016, (Omissis), Rv. 266410 -01; Sez. 5, n. 14783 del 13-03-2009, (Omissis), Rv. 243609 -01; Sez. 6, n. 27042 del 18-02-2008, (Omissis), 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 questâ??ultimo, al fine di autorizzare le parti interessate a procedere allâ??acquisizione di copia dei relativi atti, perchÃ© tale intervento non Ã¨ previsto dallâ??art. 270 cod. proc. pen., nÃ© Ã¨ imposto da altre disposizioni o dal sistema normativo, per le ragioni giÃ indicate al par. 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 lâ??atto investigativo richiesto sia costituito da intercettazioni di telecomunicazioni, ma mancano disposizioni espresse per la trasmissione e lâ??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, lâ??art. 30, paragrafo 7, Direttiva cito stabilisce che â??lâ??autoritÃ di emissione puÃ² altresÃ¬ richiedere, se ne ha particolare motivo, una trascrizione, una decodificazione o una decrittazione della registrazione, fatto salvo lâ??accordo dellâ??autoritÃ di esecuzioneâ?•.

Lâ??art. 31 Direttiva cit., poi, prevede che, quando â??lâ??intercettazione di telecomunicazioni Ã¨ autorizzata dallâ??autoritÃ competente di uno Stato membro e lâ??indirizzo di comunicazione della persona soggetta a intercettazione indicata nellâ??ordine di intercettazione Ã¨ utilizzato sul territorio di un altro Stato membro, la cui assistenza tecnica non Ã¨ necessaria per effettuare lâ??intercettazioneâ?•, occorre darne â??notificaâ?• allâ??autoritÃ competente di questâ??ultimo. Precisamente, la â??notificaâ?• deve precedere lâ??intercettazione, quando lâ??autoritÃ procedente, giÃ al momento di disporre lâ??attivitÃ di captazione, Ã¨ a conoscenza della presenza della persona soggetta a controllo nel territorio di altro Stato membro; deve avvenire â??durante lâ??intercettazione, o ad intercettazione effettuataâ?•, 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.

Lâ??autoritÃ competente dello Stato che riceve la â??notificaâ?•, â??puÃ²â?• comunicare che lâ??intercettazione non Ã¨ consentita; in questi casi, lâ??attivitÃ non puÃ² essere iniziata o proseguire, e gli eventuali risultati giÃ ottenuti mentre la persona soggetta ad intercettazione si trovava sul territorio dello Stato che ha ricevuto la â??notificaâ?• non possono essere utilizzati, o possono esserlo solo alle condizioni specificate dallâ??autoritÃ competente di questâ??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. cito contengono disposizioni sostanzialmente sovrapponibili a quelle di cui agli artt. 30 e 31 Direttiva 2014-41-UE. In particolare, lâ??art. 43, al comma 1, precisa che la disciplina si riferisce â??allâ??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 controllareâ?•, e, al comma 4, stabilisce che â??La richiesta puÃ² avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettateâ?•.

Lâ??art. 24 D.Lgs. cit., poi, con riguardo alle intercettazioni effettuate dallâ??autoritÃ giudiziaria di altro Stato membro di â??un dispositivo, anche di sistema informatico o telematico, in uso a persona che si trovi nel territorio dello Statoâ?•, contempla unâ??unica situazione alla quale consegue la cessazione delle operazioni e la inutilizzabilitÃ ai fini di prova dei risultati giÃ ottenuti: â??se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo lâ??ordinamento interno, le intercettazioni non sono consentiteâ?•.

15.3. In considerazione di quanto sopra evidenziato, puÃ² ritenersi che lâ??o.e.i. emesso dal pubblico ministero italiano avente ad oggetto lâ??acquisizione dei risultati di intercettazioni di conversazioni o comunicazioni disposte dallâ??autoritÃ giudiziaria straniera, anche quando relative a sistemi informatici o telematici, intercorrenti tra piÃ¹ sistemi, soddisfa la condizione di ammissibilitÃ di cui allâ??art. 6, paragrafo 1, lett. b), Direttiva 2014-41-UE.

Invero, siccome il pubblico ministero italiano puÃ² disporre lâ??acquisizione di risultati di intercettazioni ordinate in altro procedimento penale senza necessitÃ 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 dallâ??autoritÃ giudiziaria straniera in un procedimento pendente davanti alla stessa, abbia ad oggetto atti che â??avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogoâ?•.

15.4. E questa conclusione, in ordine al rispetto della condizione di cui allâ??art. 6, paragrafo 1, lett. b), Direttiva 2014-41-UE, resta ferma anche se le operazioni di intercettazione siano state realizzate mediante lâ??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 puÃ² ritenersi che lâ??inserimento di un captatore informatico sul server di una piattaforma di un sistema informatico o telematico costituisca mezzo â??atipicoâ?• di indagine o di prova, come tale non consentito dallâ??ordinamento italiano perchÃ© 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'â?•inserimento di un captatore informatico su un dispositivo elettronico portatileâ?•.

Il captatore informatico, infatti, non Ã¨ un autonomo mezzo di ricerca della prova, e tanto meno un mezzo di prova, bensÃ¬ uno strumento tecnico attraverso il quale esperire il mezzo di ricerca della prova costituito dalle intercettazioni di conversazioni o di comunicazioni. SicchÃ© non Ã¨ indispensabile che il legislatore preveda dove lo stesso possa essere â??inseritoâ?•.

E una conferma di questa conclusione puÃ² essere desunta dallâ??elaborazione della giurisprudenza di legittimitÃ , anche delle Sezioni Unite, la quale, giÃ prima che venisse previsto dalla legge lâ??utilizzo del captatore informatico come strumento per effettuare attivitÃ di intercettazione, ne aveva ritenuto legittimo lâ??impiego a tali fini, precisandone anche lâ??ammissibilitÃ , nei procedimenti per delitti di criminalitÃ organizzata, con riguardo a captazioni di conversazioni o comunicazioni tra presenti in luoghi di privata dimora (cosÃ¬, per tutte, Sez. U, n. 26889 del 28-04-2016, (Omissis), Rv. 266905 -01).

15.4.2. In secondo luogo, poi, non puÃ² ritenersi che lâ??utilizzo del captatore informatico al fine di acquisire le chiavi di cifratura presenti sui dispositivi mobili dei singoli utenti costituisca mezzo â??atipicoâ?• di indagine o di prova, come tale non consentito nellâ??ordinamento italiano, perchÃ© opera unâ??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, allâ??art. 30, paragrafo 7, sia il D.Lgs. n. 108 del 2017, allâ??art. 43, comma 4, prevedono espressamente la possibilitÃ per lâ??autoritÃ che ha emesso un o.e.i. per lâ??intercettazione di telecomunicazioni di chiedere la decodificazione o la decrittazione delle comunicazioni intercettate. E cosÃ¬ disponendo, riconoscono che lâ??attivitÃ di intercettazione implica anche lâ??acquisizione degli strumenti necessari per procedere a decodificazione o decrittazione delle conversazioni o comunicazioni.

Sotto altro profilo, poi, va rilevato che, nellâ??ordinamento italiano, secondo il diffuso orientamento della giurisprudenza di legittimitÃ , lâ??autorizzazione ad eseguire intercettazioni telefoniche ed ambientali implica anche il compimento di quegli atti che costituiscono una naturale modalitÃ attuativa delle operazioni, sebbene gli stessi comportino lâ??intrusione nel domicilio di una persona. Invero, numerose decisioni hanno osservato che la finalitÃ di intercettare conversazioni telefoniche e-o ambientali consente allâ??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, (Omissis), Rv. 270941 -01; Sez. 6, n. 41514 del 25-09-2012, (Omissis), Rv. 253805 -01; Sez. 6, n. 15447 del 31-01-2011, (Omissis), Rv. 250032 -01). E, anzi, proprio in questa prospettiva, si Ã¨ piÃ¹ volte affermato che Ã¨ manifestamente infondata la questione di legittimitÃ costituzionale dellâ??art. 266, comma 2, cod. proc. pen., sollevata in relazione allâ??art. 14 della Costituzione, che statuisce il principio dellâ??inviolabilitÃ del domicilio,

perchÃ© la collocazione di microspie allâ??interno di un luogo di privata dimora costituisce una delle naturali modalitÃ di attuazione delle intercettazioni, costituenti mezzo di ricerca della prova funzionale al soddisfacimento dellâ??interesse pubblico allâ??accertamento di gravi delitti, tutelato dal principio dellâ??obbligatorietÃ dellâ??azione penale di cui allâ??art. 112 della Costituzione, con il quale il principio di inviolabilitÃ del domicilio deve necessariamente coordinarsi, subendo la necessaria compressione, al pari di quanto previsto dallâ??art. 15 della Costituzione in tema di libertÃ e segretezza della corrispondenza e di ogni altra forma di comunicazione (cosÃ¬ Sez. 2, n. 21644 del 13-02-2013, (Omissis), Rv. 255541 -01, e Sez. 1, n. 38716 del 02-10-2007, (Omissis), Rv. 238108 -01).

Deve perciÃ² concludersi che, anche nel nostro sistema, Ã¨ ammissibile, ai fini dellâ??utile effettuazione di intercettazioni telefoniche ed ambientali, lâ??autorizzazione, da parte del giudice, del compimento di quegli atti che ne costituiscono una naturale e necessaria modalitÃ attuativa, pur quando gli stessi comportino lâ??intrusione nel dispositivo elettronico di una persona.

15.5. Con riferimento al tema concernente la garanzia del rispetto dei â??diritti fondamentaliâ?•, la qualificazione degli atti acquisiti mediante o.e.i. dallâ??autoritÃ giudiziaria francese come risultati di intercettazioni di conversazioni o di comunicazioni determina lâ??esigenza, in particolare, di un esame dellâ??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 â??diritti fondamentaliâ?• in relazione alle attivitÃ 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 dallâ??art. 8 CEDU, esige sia la previsione di disposizioni â??chiareâ?• sui presupposti richiesti per autorizzare le intercettazioni, sia lâ??adozione di un provvedimento autorizzativo da parte di unâ??autoritÃ indipendente specificamente motivato sullâ??esistenza in concreto di tali presupposti (cfr. Corte EDU, 12-01-2023, (Omissis) e (Omissis) c. Slovacchia, nonchÃ© Corte EDU, 15-01-2015, (Omissis) c. Croazia).

Sempre secondo la Corte EDU, poi, la motivazione del provvedimento autorizzativo deve consentire di verificare se sussistono ragioni â??fattualiâ?• per sospettare che una persona progetti, commetta o abbia commesso alcuni gravi reati e se non vi Ã¨ alcuna prospettiva di accertare i fatti con successo mediante un altro metodo, diverso dalle intercettazioni, o questo sarebbe notevolmente piÃ¹ difficile (cosÃ¬ Corte EDU, 12-01-2023, (Omissis) e (Omissis) c.

Slovacchia, par. 73).

Da questa elaborazione, si evince, in particolare, che le intercettazioni non autorizzate da un giudice o da unâ??autoritÃ indipendente, e le intercettazioni disposte sulla base di provvedimenti non motivati in ordine allâ??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, purchÃ© siano previste efficaci garanzie contro rischi di abusi e di arbitri nelle fasi dellâ??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, (Omissis) C. Svezia, le quali, sebbene con riguardo ad intercettazioni effettuate dai servizi segreti e non nellâ??ambito di un procedimento penale, hanno escluso che, in generale, le C.d. â??intercettazioni di massaâ?•, anche quando disposte per contrastare attivitÃ delittuose concernenti il traffico di sostanze illecite, integrino una violazione degli artt. 8 e 10 CEDU, se effettuate nel rispetto di â??dovuteâ?• garanzie).

NÃ© risulta affermata lâ??incompatibilitÃ 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 lâ??art. 8 CEDU esiga lâ??autorizzazione ex ante di un giudice alla trasmissione, dal pubblico ministero allâ??autoritÃ amministrativa, di risultati di intercettazioni telefoniche effettuate in un procedimento penale (cfr., per tutte, Corte EDU, 16-05-2023, (Omissis) B.V. c. Paesi Bassi).

Nemmeno lâ??impossibilitÃ , per la difesa, di accedere allâ??algoritmo utilizzato nellâ??ambito di un sistema di comunicazioni per â??criptareâ?• il contenuto delle stesse determina, almeno in linea di principio, una violazione di â??diritti fondamentaliâ?•. Ed infatti, se Ã¨ vero che la disponibilitÃ dellâ??algoritmo di criptazione Ã¨ funzionale al controllo dellâ??affidabilitÃ del contenuto delle comunicazioni acquisite al procedimento, deve perÃ² 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 Ã¨ inscindibilmente abbinato alla sua chiave di cifratura, per cui una chiave errata non ha alcuna possibilitÃ di decriptarlo, anche solo parzialmente (cfr., tra le tante: Sez. 6, n. 46833 del 26-10-2023, (Omissis), non mass. sul punto; Sez. 6 n. 48838 dellâ??1l-10-2023, (Omissis), non mass. sul punto; Sez. 4, n. 16347 del 05-04-2023, (Omissis), non mass. sul punto; Sez. 1, n. 6364 del 13-10-2022, dep. 2023, (Omissis)n, non mass. sul punto). NÃ© la giurisprudenza sovranazionale risulta aver affermato che lâ??indisponibilitÃ dellâ??algoritmo di decriptazione agli atti del processo costituisca, di per sÃ©, violazione dei â??diritti fondamentaliâ?•. In proposito, anzi, puÃ² 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 dellâ??uso di un sistema di messaggistica criptata denominato ByLock, si Ã¨

limitata ad affermare che dare al ricorrente lâ??opportunitÃ 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, (Omissis) C. Turchia, par. 336; il testo originale Ã¨ il seguente: â??The Court is accordingly of the view that giving the applicant the opportunity to acquaint himself with the decrypted ByLock materia â?? in his regard would have constituted an important step in preserving his defence rightsâ?•).

In ogni caso, inoltre, resta fermo che lâ??onere dellâ??allegazione e della prova in ordine ai fatti da cui desumere la violazione dei â??diritti fondamentaliâ?• grava sulla parte interessata, per le ragioni indicate in precedenza nel par. 10.6.

15.5.2. Con riferimento alle garanzie previste dalla Direttiva 2014-41-UE, puÃ² venire in rilievo il profilo, segnalato dai ricorrenti, della violazione dei principi fissati dallâ??art. 31 in ordine alle intercettazioni effettuate nei confronti di persone il cui l'â?•indirizzo di comunicazioneâ?• Ã¨ utilizzato nel territorio di uno Stato diverso da quello nel quale le operazioni di captazione sono state disposte.

Secondo quanto piÃ¹ analiticamente esposto in precedenza al par. 15.2, lâ??art. 31 Direttiva cito prevede che lo Stato nel quale sono state disposte le intercettazioni dia â??notificaâ?• di tali attivitÃ allâ??autoritÃ competente nello Stato nel quale Ã¨ utilizzato lâ??indirizzo di comunicazione sottoposto a controllo, quando viene a conoscenza di tale circostanza, e che questâ??ultima possa vietare il compimento o la prosecuzione delle operazioni, nonchÃ© lâ??utilizzazione dei risultati giÃ ottenuti.

Sulla base di tale disciplina, deve rilevarsi, innanzitutto, che lâ??obbligo di notifica sorge quando lâ??autoritÃ procedente viene a conoscenza che lâ??intercettazione riguarda persone il cui â??indirizzo di comunicazioneâ?• Ã¨ utilizzato nel territorio di un altro Stato.

Va segnalato, poi, che lâ??eventuale intempestivitÃ della comunicazione non Ã¨ sanzionata di per sÃ©, e che, in ogni caso, opera la garanzia della possibile dichiarazione di inutilizzabilitÃ da parte dellâ??autoritÃ competente dello Stato in cui Ã¨ fatto uso dell'â?•indirizzo di comunicazioneâ?•.

Occorre considerare, ancora, che il divieto della Direttiva 2014-41-UE di iniziare o proseguire le attivitÃ di captazione, ovvero di utilizzarne i risultati, Ã¨ previsto solo â??qualora lâ??intercettazione non sia ammessa in un caso interno analogoâ?•. E, nella disciplina italiana di attuazione della Direttiva cit., lâ??art. 24 D.Lgs. n. 108 del 2017 prevede unâ??unica ipotesi vietata: â??se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo lâ??ordinamento interno, le intercettazioni non sono consentiteâ?•.

PuÃ² quindi concludersi che, nellâ??ordinamento italiano, sulla base della disciplina di cui allâ??art. 31 Direttiva 2014-41-UE, lâ??inutilizzabilitÃ dei risultati di intercettazioni disposte da autoritÃ di altro Stato ed effettuate nei confronti di persone il cui â??indirizzo di comunicazioneâ?• Ã¨ attivato in Italia sussiste solo se lâ??autoritÃ giudiziaria italiana rileva che le captazioni non sarebbero state consentite â??in un caso interno analogoâ?•, perchÃ© disposte per un reato per il quale la legge nazionale non prevede la possibilitÃ di ricorrere a tale mezzo di ricerca della prova.

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

â??In materia di ordine Europeo di indagine, lâ??acquisizione dei risultati di intercettazioni disposte da un â??autoritÃ giudiziaria straniera in un procedimento penale pendente davanti ad essa, ed effettuate su una piattaforma informatica criptata e su criptofonini, non rientra nellâ??ambito di applicazione dellâ??art. 234-bis cod. proc. pen., che opera al di fuori delle ipotesi di collaborazione tra autoritÃ giudiziarie, ma Ã¨ assoggettata alla disciplina di cui allâ??art. 270 cod. proc. pen.â?•.

â??In materia di ordine Europeo di indagine, le prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza la necessitÃ di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarleâ?•.

â??Lâ??emissione, da parte del pubblico ministero, di ordine Europeo di indagine diretto ad ottenere i risultati di intercettazioni disposte da un â??autoritÃ giudiziaria straniera in un procedimento penale pendente davanti ad essa, ed effettuate attraverso lâ??inserimento di un captatore informatico sui server di una piattaforma criptata, Ã¨ ammissibile, perchÃ© attiene ad esiti investigativi ottenuti con modalitÃ compatibili con lâ??ordinamento italiano, e non deve essere preceduta da autorizzazione del giudice italiano, quale condizione necessaria ex art. 6 Direttiva 2014-41-UE, perchÃ© tale autorizzazione non Ã¨ richiesta nella disciplina nazionaleâ?•.

â??Lâ??utilizzabilitÃ dei risultati di intercettazioni disposte da unâ??autoritÃ 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 lâ??onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessataâ?•.

â??Lâ??impossibilitÃ per la difesa di accedere allâ??algoritmo utilizzato nellâ??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 Ã¨ inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilitÃ di decriptarlo anche solo parzialmenteâ?•.

17. Sulla base dei principi di diritto enunciati, e degli argomenti esposti a loro fondamento, Ã¨ possibile esaminare le censure enunciate nel terzo, nel quarto, nel quinto e nel sesto motivo dei ricorsi, nonchÃ© 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 lâ??utilizzabilitÃ dei dati informatici relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, sotto vari profili.

In sintesi, le stesse deducono lâ??inapplicabilitÃ della disciplina di cui allâ??art. 234Âbis cod. proc. pen. e lâ??applicabilitÃ di quella relativa allâ??acquisizione dei risultati di intercettazioni, il difetto dei presupposti per lâ??emissione dellâ??o.e.i., in particolare per il carattere generalizzato ed indifferenziato delle attivitÃ di captazione effettuata dallâ??autoritÃ estera, per lâ??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 dellâ??art. 31 Direttiva 2014-41-UE, nonchÃ© ancora la violazione della disciplina francese, priva di disposizioni analoghe allâ??art. 270 cod. proc. pen.

18.1. Il Collegio condivide la tesi della inapplicabilitÃ della disposizione di cui allâ??art. 234-bis cod. proc. pen. in materia di acquisizione ed utilizzabilitÃ dei dati relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, perchÃ© si tratta di disciplina alternativa, e, quindi, incompatibile con quella relativa al sistema dellâ??o.e.i., come precedentemente precisato nei par. 9, 9.1 e 9.2. Tuttavia, questo assunto non rende illegittima lâ??acquisizione, nÃ© preclude lâ??utilizzabilitÃ dei dati relativi alle comunicazioni intercorse attraverso il sistema criptato Sky-Ecc, ottenuti dallâ??autoritÃ giudiziaria francese in esecuzione di o.e.i. emesso dal pubblico ministero italiano. Invero, lâ??errore di qualificazione in cui Ã¨ incorsa lâ??ordinanza impugnata non determina lâ??annullamento della stessa, sulla base di quanto previsto dallâ??art. 619, comma 1, cod. proc. pen: lâ??errore rilevato, precisamente, non ha avuto influenza decisiva sul dispositivo, in quanto, nella specie, sussistono le condizioni di ammissibilitÃ necessarie per emettere legittimamente lâ??o.e.i. e non risultano violazioni dei diritti fondamentali.

18.2. Innanzitutto, deve ritenersi soddisfatta la condizione di ammissibilitÃ posta dallâ??art. 6, paragrafo 1, lett. b), Direttiva 2014-41-UE, che richiede che lâ??atto o gli atti richiesti â??avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogoâ?•.

Invero, gli atti ricevuti dallâ??autoritÃ giudiziaria francese in esecuzione di o.e.i. emesso dal pubblico ministero italiano, per quanto Ã¨ desumibile dal contenuto dellâ??ordinanza impugnata e non Ã¨ contestato nel ricorso, costituiscono â??prove giÃ in possesso delle autoritÃ competenti dello Stato di esecuzioneâ?•, perchÃ© acquisite nellâ??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 puÃ² essere effettuata sulla base di o.e.i. emesso dal pubblico ministero in assenza di preventiva autorizzazione del giudice, in quanto tale autorizzazione non Ã¨ richiesta nellâ??ordinamento italiano per lâ??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 allâ??art. 6, paragrafo 1, lett. b), Direttiva cito anche a voler ritenere che lâ??o.e.i. abbia ad oggetto lâ??acquisizione dei risultati di intercettazioni effettuate attraverso lâ??inserimento di un captatore â?? informatico sui server di una piattaforma criptata. Si Ã¨ infatti evidenziato che questa modalitÃ investigativa Ã¨ compatibile con la disciplina delle intercettazioni prevista nellâ??ordinamento italiano.

NÃ© vi sono dubbi che gli atti ottenuti mediante o.e.i. siano stati richiesti in quanto ritenuti â??rilevanti ed indispensabili per lâ??accertamento di delitti per i quali Ã¨ obbligatorio lâ??arresto in flagranzaâ?•.

Non puÃ² poi ritenersi che lâ??asserita violazione delle garanzie procedimentali di cui allâ??art. 268, commi 6, 7 e 8, cod. proc. pen. possa rilevare ai fini delle condizioni di ammissibilitÃ di cui allâ??art. 6, paragrafo 1, lett. b), Direttiva cit. Le garanzie indicate, infatti, non costituiscono condizioni per lâ??acquisizione dei risultati di intercettazioni disposte in altro procedimento, ma rilevano in una fase successiva e di controllo, e la loro attuazione puÃ² essere differita fino alla chiusura delle indagini preliminari, anche dopo lâ??utilizzazione degli esiti delle captazioni a fini cautelari. Invero, lâ??art. 268 cod. proc. pen. Ã¨ stato dichiarato costituzionalmente illegittimo non nella parte in cui non prevede il deposito degli atti relativi alle intercettazioni effettuate, bensÃ¬, ben piÃ¹ limitatamente, nella parte in cui non prevede che, dopo la notificazione o lâ??esecuzione dellâ??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 dellâ??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 ammissibilitÃ posta dallâ??art. 6, paragrafo 1, lett. a), Direttiva 2014-41-UE, relativa alla necessitÃ e proporzionalitÃ delle attivitÃ richieste mediante o.e.i., anche in considerazione dei diritti degli indagati.

Si Ã¨ detto in precedenza, al par. 10.2, che lâ??esame di tale profilo deve essere compiuto avendo riguardo al procedimento nel cui ambito Ã¨ emesso lâ??ordine Europeo di indagine. E, nella specie, lâ??o.e.i. risulta formulato con espresso riferimento allâ??acquisizione delle comunicazioni relative a persone nominativamente indicate, tra le quali i due attuali ricorrenti, in quel momento giÃ 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 Ã¨ deducibile in questa sede la questione concernente la decisione dellâ??autoritÃ giudiziaria francese di dare esecuzione allâ??o.e.i., prospettata con riguardo alla violazione della legge francese, perchÃ© questa non prevederebbe lâ??utilizzabilitÃ dei risultati di intercettazioni di conversazioni o comunicazioni in procedimenti diversi da quelli in cui le stesse sono stati disposti.

In effetti, come giÃ evidenziato nel par. 10.4, le questioni concernenti la fase di esecuzione, e quindi anche quelle concernenti la scelta di riconoscere ed eseguire, sono proponibili solo nello Stato di esecuzione, salvo che non diano luogo a violazioni di â??diritti fondamentaliâ?• che si ripercuotono sullâ??utilizzazione degli elementi istruttori nel procedimento pendente in Italia.

Peraltro, lâ??elemento indicato dai ricorrenti per affermare la violazione della legge francese, ossia la decisione Corte EDU, 29-03-2005, (Omissis) c. Francia, non dimostra lâ??esistenza di un divieto, nellâ??ordinamento transalpino, di utilizzare i risultati di intercettazioni in procedimenti diversi.

18.5. NÃ© puÃ² dirsi che, nel presente procedimento, sia stata accertata la violazione di â??diritti fondamentaliâ?•.

18.5.1. Innanzitutto, i dati probatori trasmessi dallâ??autoritÃ 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 allâ??esistenza in concreto dei presupposti ritenuti necessari dalla giurisprudenza della Corte EDU.

Invero, dallâ??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 Sky-Ecc, inoltre, per le modalitÃ di accesso, per la impenetrabilitÃ dallâ??esterno, e per lâ??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 puÃ² preliminarmente osservare che il sistema Sky-Ecc, per le garanzie di anonimato assicurate agli utenti, non Ã¨ certamente compatibile con la disciplina italiana, che richiede lâ??identificazione degli stessi, mediante lâ??acquisizione di dati anagrafici riportati su un documento di identitÃ , prima dellâ??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 giÃ indicate ordinanze emesse dal Giudice Istruttore del Tribunale di Parigi. I provvedimenti dellâ??autoritÃ giudiziaria francese, infatti, evidenziano che: a) lâ??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 â??redditi conseguentiâ?•; b) la vendita dei singoli dispositivi avveniva in condizioni di clandestinitÃ , tali da garantire lâ??anonimato del venditore e dellâ??acquirente, anche perchÃ© effettuata dietro pagamenti in contanti, con conseguente esclusione della tracciabilitÃ 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 lâ??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 Sky-Ecc Ã¨ 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 lâ??inserimento del captatore informatico sui server della piattaforma della societÃ Sky-Ecc Ã¨ da ritenere indispensabile perchÃ© 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 societÃ â??Sky Globalâ?• 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 plausibilitÃ della prospettazio ne secondo cui le autoritÃ francesi avrebbero effettuato intercettazioni generalizzate ed indiscriminate.

Dette ordinanze, infatti, come precisato nel par. 18.5.1, evidenziano specifici elementi indizianti anche nei confronti dei singoli utenti del sistema Sky-Ecc in ordine al coinvolgimento dei medesimi nella commissione di gravi reati, in particolare in materia di traffico di sostanze stupefacenti. Invero, non puÃ² 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 impenetrabilitÃ ; 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 societÃ preposta alla gestione del sistema Sky-Ecc e a precisare il loro livello di coinvolgimento nelle attivitÃ illecite degli utenti.

18.5.3. Deve poi escludersi che lâ??indisponibilitÃ 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 giÃ indicato in precedenza al par. 15.5.1, la conoscibilitÃ dellâ??algoritmo di criptazione attiene non allâ??acquisibilitÃ o allâ??utilizzabilitÃ dei dati relativi alle comunicazioni, ma alla verifica di affidabilitÃ del loro contenuto; inoltre, la asserita alterazione dei dati Ã¨ stata unicamente ipotizzata dal ricorrente, che non ha nÃ© allegato, nÃ© 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 dallâ??autoritÃ giudiziaria francese siano qualificabili come risultati di intercettazioni di conversazioni o comunicazioni, deve escludersi, in

forza di quanto osservato in precedenza al par. 15.5.2, che sia configurabile lâ??unica fattispecie di inutilizzabilitÃ prevista dalla legge per il caso di captazioni disposte allâ??estero ed effettuate nei confronti di persone il cui â??indirizzo di comunicazioneâ?• Ã¨ attivato in Italia. Non puÃ² sostenersi, infatti, che, nella specie, le operazioni non sarebbero state consentite â??in un caso interno analogoâ?•, perchÃ© le stesse sono state disposte in ordine a reati per i quali la legge italiana prevede la possibilitÃ 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 necessitÃ di formulare alla Corte di giustizia dellâ??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 dallâ??autoritÃ giudiziaria francese in modo generalizzato ed indiscriminato, ovvero in difetto di indizi concreti nei confronti degli utenti del sistema Sky-Ecc o comunque in violazione di â??diritti fondamentaliâ?• o di principi costituzionali dellâ??ordinamento nazionale, o in contrasto con le garanzie assicurate dallâ??art. 31 Direttiva 2014-41-UE, per le ragioni indicate nei par. 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 giÃ 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 dallâ??art. 6, paragrafo 1, lett. a) e b), Direttiva 2014-41-UE, o di interpretazione ed applicazione dellâ??art. 31 Direttiva cit.

Deve pertanto escludersi che ricorrano ragionevoli dubbi in ordine alla interpretazione del diritto dellâ??Unione Europea concretamente applicabile nel caso in esame, e che, quindi, sussista lâ??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 giÃ Corte giustizia, 06-10-1982, (Omissis) e (Omissis), C-283-81).

20. Prive di specificitÃ , e comunque manifestamente infondate, sono le censure esposte nel motivo nuovo, che contestano la violazione del diritto di difesa â?? per lâ??impossibilitÃ di accedere al sistema informatico impiegato per lâ??analisi delle comunicazioni intercorse sul

sistema Sky-Ecc, 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 attivitÃ compiute in procedimenti penali pendenti allâ??estero o comunque dallâ??autoritÃ giudiziaria estera in esecuzione dellâ??o.e.i., e, quindi, attivitÃ in linea generale non sindacabili dallâ??autoritÃ giudiziaria italiana per le ragioni indicate nel par. 10.4. In ogni caso, poi, la difesa non ha nemmeno allegato di aver presentato istanza di accesso al sistema informatico asseritamente impiegato per lâ??analisi delle comunicazioni intercorse sul sistema Sky-Ecc.

21. Del tutto inammissibile, infine, Ã¨ la richiesta, formulata per la prima volta in udienza, di annullamento con rinvio dellâ??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 indispensabilitÃ di tale atto istruttorio; e, come si Ã¨ evidenziato in precedenza nei par. 15.5.1 e 18.5.4, la asserita alterazione dei dati Ã¨ stata unicamente ipotizzata dal ricorrente, che non ha nÃ© allegato, nÃ© provato elementi utili a rendere concreta tale evenienza. In secondo luogo, presuppone lâ??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 dallâ??autoritÃ estera. In terzo luogo, non considera che il tribunale del riesame Ã¨ privo di poteri istruttori in ordine ai fatti relativi allâ??imputazione, siccome incompatibili con la speditezza del procedimento incidentale de libertate (cosÃ¬, tra le tantissime, Sez. 6, n. 46036 del 26-10-2023, (Omissis), Rv. 285475 -01, e Sez. 1, n. 23869 del 22-04-2016, (Omissis), 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 dellâ??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 allâ??art. 94, comma 1-ter, disp. att. cod. proc. pen.

CosÃ¬ deciso in Roma, il 29 febbraio 2024.

Depositato in Cancelleria il 14 giugno 2024

Campi meta

Massima : ***Il diniego di autorizzazione per l'installazione di infrastrutture di comunicazione elettronica Ã¨ illegittimo se non preceduto dal preavviso di rigetto (art. 10-bis L. 241/90) e se fondato esclusivamente sulla tipizzazione urbanistica dell'area o sulla generica collocazione in fascia di rispetto cimiteriale, poichÃ© tali opere, equiparate a quelle di urbanizzazione primaria, sono compatibili con qualsiasi zona del territorio comunale, salvo specifici e motivati vincoli di inedificabilitÃ assoluta.***

Supporto Alla Lettura :

Ciberecurity

Il quadro regolamentare che tutela la sicurezza informatica Ã¨ articolato su piÃ¹ livelli, con una forte spinta allâ??armonizzazione da parte dellâ??Unione Europea. Il Regolamento (UE) 2016/679 (GDPR) stabilisce il primo e fondamentale ponte tra la protezione dei dati personali (Privacy) e la Cybersecurity, imponendo a Titolari e Responsabili lâ??obbligo di adottare â??misure tecniche e organizzative adeguateâ?• (Art. 32) per prevenire le violazioni e assicurare la sicurezza del trattamento. Lâ??elemento centrale della legislazione settoriale Ã¨ la Direttiva (UE) 2022/2555 (Direttiva NIS 2). Questa Direttiva ha sostituito la precedente NIS, ampliando significativamente il suo campo di applicazione a un vasto numero di settori critici, classificandoli come EntitÃ Essenziali (es. energia, sanitÃ) o EntitÃ Importanti (es. servizi digitali, fornitori ICT). La NIS 2 introduce requisiti di gestione del rischio piÃ¹ rigorosi e stabilisce stringenti obblighi di notifica degli incidenti cibernetici significativi. A supporto della NIS 2 e per rafforzare la sicurezza dei prodotti digitali, opera il Regolamento (UE) 2019/881 (Cybersecurity Act), che conferisce un mandato permanente allâ??ENISA (Agenzia dellâ??Unione Europea per la Cybersecurity) e istituisce un quadro europeo di certificazione per prodotti, servizi e processi ICT, essenziale per la sicurezza di tutta la catena di approvvigionamento. In Italia, il recepimento degli obblighi europei e la definizione di una strategia nazionale si concretizzano in diversi atti, tra cui: La Legge sulla Cybersecurity (Legge n. 90/2024), che opera il rafforzamento della cybersicurezza nazionale, allineandosi agli standard europei e definendo nuovi doveri per le Pubbliche Amministrazioni e le aziende private. Il Perimetro di Sicurezza Nazionale Cibernetica (Decreto Legge n. 105/2019), il quale impone rigorose misure di sicurezza alle reti e ai sistemi informativi di soggetti pubblici e privati che svolgono una funzione essenziale per gli interessi dello Stato.