

LE SEZIONI UNITE SULL'UTILIZZABILITÀ DELLA MESSAGGISTICA CRIPTATA ACQUISITA MEDIANTE ORDINE EUROPEO DI INDAGINE

Salvatore Pignata



Nota a Cassazione penale, sezioni Unite,

5 ottobre 2024 (dep. 14 giugno 2024), n. 23755 – Presidente Cassano, Estensore Corbo

1. Il fatto

Il procedimento in esame ha per oggetto il ricorso per cassazione avverso l'ordinanza del 29 giugno 2023, con la quale il Tribunale di Potenza ha rigettato l'istanza di riesame proposta nell'interesse di un indagato

avverso l'ordinanza del giudice per le indagini preliminari del Tribunale di Potenza che aveva applicato nei suoi confronti la misura cautelare della custodia in carcere per il reato di cui all'art. 74 d.P.R. n. 309 del 1990, ritenendo sussistenti gravi indizi di colpevolezza a carico dello stesso con riferimento alla sua partecipazione ad un'associazione per delinquere finalizzata alla traffico di stupefacenti, anche sulla base di elementi indiziari costituiti da comunicazioni intercorse sulla rete criptata Sky-Ecc, acquisiti mediante ordine europeo di indagine (di seguito "o.e.i.") eseguito dall'autorità giudiziaria francese.

In particolare, il ricorrente ha posto all'attenzione del giudice di legittimità la questione della inutilizzabilità della disciplina di cui all'art. 234 bis c.p.p., la mancata acquisizione dei file rappresentativi delle comunicazioni e delle chiavi di decifrazione, l'illegittimità dell'o.e.i. in quanto adottato senza la preventiva autorizzazione del giudice italiano e la violazione di diritti fondamentali.

Con ordinanza del 3 novembre 2023, la terza Sezione della Corte di cassazione, cui era stato assegnato il ricorso, rilevando l'esistenza di questioni di diritto idonee controverse, per le quali si assiste ad una disputa giurisprudenziale, ha rimesso le stesse alle Sezioni unite ai sensi dell'art. 618, comma primo, c.p.p.; in particolare si chiede al supremo consesso riunito:

- a) se l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato attraverso un ordine europeo di indagine rivolto all'autorità giudiziaria straniera che ne abbia eseguito la decrittazione costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234 *bis* c.p.p., di documenti *ex art.* 234 c.p.p., o sia riconducibile ad altra disciplina pure relativa all'acquisizione di prove;
- b) se l'acquisizione sopra indicata debba essere preventivamente autorizzata o successivamente valutata dall'autorità giurisdizionale italiana, ai fini dell'utilizzabilità dei relativi dati.

2. La ricostruzione dei diversi orientamenti da parte delle Sezioni unite.

Prima di addentrarsi nella disamina della Sentenza in oggetto, giova effettuare alcune considerazioni di carattere generale con riferimento all'ordine europeo di indagine.

L'ordine europeo di indagine (o.e.i.), previsto dalla Direttiva 2014/41/UE, attuata in Italia con la Legge n. 108 del 2017, è uno strumento di cooperazione giudiziaria in materia penale tra gli Stati membri, volto

all'acquisizione transazionale di prove, anche già formate dallo Stato estero di esecuzione, e di atti investigativi.

L'o.e.i. è basato sul principio del riconoscimento reciproco, ovverosia sulla circostanza che l'autorità estera è tenuta a riconoscere e a garantire l'esecuzione della richiesta avanzata dallo Stato richiedente, con le stesse modalità previste dalla disciplina dettata nello Stato di esecuzione.

I presupposti necessari per poter adottare un ordine europeo di indagine sono che l'atto investigativo richiesto all'autorità giudiziaria estera sia necessario, proporzionato e infine consentito in casi analoghi nello Stato richiedente.

Ciò premesso, si passeranno in rassegna gli orientamenti contrastanti in seno alla giurisprudenza di legittimità sulle questioni sopra esposte.

2.1. L'orientamento che ritiene che la disciplina applicabile sia quella relativa all'acquisizione di documenti e dati informatici di cui all'art. 234 *bis* c.p.

Secondo l'orientamento più risalente, quando l'autorità giudiziaria straniera trasmette, in accoglimento dell'o.e.i., comunicazioni su chat di gruppo scambiate con sistema cifrato, le quali siano già in suo possesso nell'ambito di un procedimento penale estero, si verte nell'ipotesi prevista dall'art. 234 *bis* c.p.p.

In tal senso, alcune pronunce affermano che occorre distinguere tra due diversi tipi di possibili operazioni^[1].

Nello specifico, quando l'attività di captazione e registrazione riguarda messaggi in fase di transito dall'apparecchio del mittente a quello del destinatario, la disciplina applicabile è quella dettata dall'art. 266 *bis* c.p.p., ovverosia quella relativa alla intercettazioni di comunicazioni o conversazioni.

Se, invece, l'attività di acquisizione e decifrazione si riferisce a comunicazioni già effettuate o comunque già acquisite dall'autorità giudiziaria estera, la disposizione applicabile sarà quella di cui all'art. 234 *bis* c.p.p., la quale consente l'acquisizione di documenti informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, «*previo consenso, in quest'ultimo caso, del legittimo titolare*».

Le richiamate pronunce specificano che, quando l'autorità giudiziaria italiana riceve dall'autorità giudiziaria straniera un dato informatico (ovverosia una «*rappresentazione comunicativa incorporata in una base materiale con metodo digitale*»), si versa nell'ambito dell'acquisizione di un documento informatico, aggiungendo che, in tali ipotesi, sussiste anche l'ulteriore requisito per l'applicabilità della disciplina dettata dall'art. 234 *bis* c.p.p., ovverosia il consenso all'acquisizione da parte del legittimo titolare, per esso intendendosi anche la persona giuridica che di quei dati può disporre in forza di un titolo legittimo (pertanto, anche la polizia giudiziaria o l'autorità giudiziaria dello Stato estero).

Peraltro, le tre pronunce più recenti che aderiscono a tale scuola di pensiero^[2], riconnettono la legittimità del procedimento di acquisizione dei dati da parte dell'autorità giudiziaria italiana alla procedura di esperimento dell'ordine europeo di indagine.

Infatti, precisano che l'o.e.i.: a) deve avere a oggetto prove acquisibili dello Stato di emissione; b) deve essere eseguito in conformità della disciplina prevista nello Stato di esecuzione in relazione a un atto analogo; c) deve presumersi adempiuto, secondo quanto previsto dal consolidato orientamento della suprema Corte in tema di rogatoria, nel rispetto di tale disciplina e dei diritti fondamentali, salvo concreta verifica di segno opposto.

Le Sezioni unite evidenziano che – come statuito nelle sentenze nn. 6363 e 6364 del 2022 - la disciplina dell'o.e.i. non impedisce, sulla base sia della Direttiva n. 2014/41/UE che del D.lgs. n. 108/2017, di acquisire i risultati di attività investigative già compiute; è irrilevante se la richiesta di o.e.i. sia avanzata dal p.m. anche quando attiene ad atti acquisibili in Italia solo sulla base di un provvedimento giurisdizionale ai sensi dell'art. 132 D.lgs. n. 196/2003, in quanto, in tale caso, l'attività di acquisizione dei dati è stata disposta dal giudice dello Stato estero; non si pone alcun problema di genuinità del dato informatico derivante dalla mancata ostensione dell'algoritmo necessario alla decriptazione dei messaggi, in quanto, secondo la scienza informatica, solo l'algoritmo corretto consente di ottenere un testo dotato di significato, per cui è onere della difesa allegare specifici e concreti elementi, dai quali desumere, nel singolo caso, rischi di alterazioni.

Numerose altre pronunce stabiliscono che: a) è irrilevante accertare se l'autorità giudiziaria straniera abbia acquisito i dati *ex post* o in tempo reale, in quanto l'aspetto fondamentale è essere stata la richiesta italiana di o.e.i. avanzata quando i flussi di comunicazione non erano più in corso; b) l'onere di provare che gli atti compiuti dall'autorità giudiziaria straniera abbiano violato i principi fondamentali e inderogabili dell'ordinamento giuridico italiano grava su chi formula la relativa eccezione, anche tenuto conto che il diritto

straniero è un “fatto”^[3].

2.2. L'impostazione che ritiene che la disciplina applicabile sia quella di cui all'art. 254 *bis* c.p., dettata in materia di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.

Secondo una diversa opzione ermeneutica, espressa da due pronunce (Cass. pen., sez. VI, 26 ottobre 2023, n. 44155; Cass. pen., sez. VI, 26 ottobre 2023, n. 44154), l'acquisizione svolta mediante un ordine europeo di indagine di messaggi su chat di gruppo scambiati con sistema cifrato, quando riguarda i risultati di un'attività di acquisizione di comunicazioni non in corso o al sequestro di dati archiviati in un server o in altri supporti informatici, è disciplinata dall'art. 254 *bis* c.p.p. e non dalla disposizione di cui all'art. 234 *bis* c.p.p.

In tal senso, si osserva che, per un verso, l'art. 234 *bis* c.p.p., riguarda soltanto i dati preesistenti rispetto al momento dell'inizio delle indagini da parte dell'autorità giudiziaria straniera o comunque formati al di fuori di tali investigazioni e che, sotto altro profilo, non può discorrersi di acquisizione avvenuta con il consenso del legittimo titolare, in quanto questi si identifica con il mittente e con il destinatario del messaggio, oltre che con la società di gestione della piattaforma di transito della comunicazione e non già con l'autorità giudiziaria straniera (come sostenuto, invece, dal primo orientamento), la quale, infatti, sarebbe soltanto un mero detentore di dati a fini di giustizia.

Pertanto, secondo queste decisioni, l'attività sopra indicata, se non riferita a comunicazioni in corso, deve essere regolata dall'art. 254 *bis* c.p.p. che si occupa di definire la disciplina in tema di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di comunicazioni.

In tal senso, si specifica che se l'attività di apprensione è relativa a dati esterni al traffico telefonico o telematico, la disciplina applicabile è quella dettata dall'art. 132 d.lgs. n. 196 del 2003; diversamente, se si è verificata una captazione di comunicazioni o di flussi comunicativi in corso, la disciplina da applicare è quella dettata in materia di intercettazioni dagli artt. 266 ss. c.p.p.

Si richiama, sul punto, la sentenza CGUE, Grande Sezione, 2 marzo 2021, H.K./ Prokurator, causa C-746/18, la quale ha stabilito, in primo luogo, che, in forza del principio di proporzionalità, occorre che le categorie di soggetti interessati e la durata per la quale è richiesto l'accesso agli atti siano limitati a quanto strettamente necessario ai fini dell'indagine; in secondo luogo, che è richiesta, in tali ipotesi, un'autorizzazione di un giudice.

Pertanto, questo orientamento evidenzia che l'acquisizione all'estero di documenti e di dati informatici relativi alla corrispondenza o ad altre forme di comunicazione deve essere sempre autorizzata da un giudice, altrimenti concretizzandosi il paradosso secondo il quale, per l'acquisizione dei dati relativi al traffico telefonico e telematico occorrerebbe la preventiva autorizzazione del giudice, mentre per eseguire il sequestro di dati informatici relativi al contenuto di comunicazioni oggetto di quel traffico sarebbe sufficiente un provvedimento emesso dal pubblico ministero.

Tale impostazione, peraltro, è conforme alla più recente giurisprudenza della Corte costituzionale in tema di tutela della libertà e della segretezza della corrispondenza ex art. 15 Cost.; in particolare, si fa riferimento alla sentenza n. 170/2023, con la quale il giudice delle leggi ha statuito che l'art. 15 Cost. tutela la corrispondenza, inclusa quella "elettronica", anche dopo la sua ricezione da parte del destinatario, almeno fino a quando non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza; e alla sentenza n. 2/2023, con la quale è stato invece precisato che tale tutela si connota anche per la «riserva di giurisdizione», intesa come vaglio dell'autorità giurisdizionale.

In tal senso, si aggiunge che questa giurisprudenza costituzionale si armonizza con quella della Corte EDU, che ha ricondotto nell'alveo operativo dell'art. 8 CEDU i messaggi di posta elettronica e la messaggistica istantanea inviata e ricevuta tramite internet.

Pertanto, l'orientamento in parola ritiene che l'autorità giudiziaria italiana competente a emettere l'o.e.i. diretto ad acquisire quegli elementi è il pubblico ministero, ma potrebbe essere necessaria la previa autorizzazione del giudice. In tale ottica, si sottolinea come l'illegittimità dell'o.e.i. emesso senza la preventiva autorizzazione del giudice, quando necessaria, può essere eccepita dalla difesa, ma con conseguenze diverse: se con l'o.e.i. è stata svolta un'attività investigativa illegittima, saranno inutilizzabili le prove acquisite; se, invece, l'o.e.i. è stato emesso ai fini di acquisire una prova «già disponibile» nello Stato di esecuzione e non è stata eccepita l'inosservanza della relativa disciplina davanti all'autorità giudiziaria straniera, la verifica circa la sussistenza delle condizioni di ammissibilità può essere demandata al giudice italiano.

2.3. L'orientamento che ritiene che l'acquisizione dei dati possa essere disposta direttamente dal pubblico ministero.

Secondo una diversa impostazione teorica, sostenuta da tre pronunce^[4] l'acquisizione, mediante ordine europeo di indagine, di messaggi su chat di gruppo scambiati con sistema cifrato, quando è relativa a elementi già raccolti nell'ambito di un procedimento penale estero, ha ad oggetto, se riguarda

corrispondenza, una prova documentale, mentre, nel caso in cui si riferisca ai risultati di intercettazioni, il relativo trasferimento nel procedimento penale nazionale può essere disposto direttamente dal pubblico ministero senza preventiva autorizzazione del giudice.

Siffatta impostazione afferma che l'acquisizione di comunicazioni conservate nei dispositivi informatici, anche quando riguarda corrispondenza, è regolata dalla disciplina in materia di perquisizione e sequestro ai sensi degli artt. 244, 247, co. 1 *bis*, 264 *bis* e 352, co. 1 *bis*, c.p.p. e, pertanto, non occorre un provvedimento abilitativo del giudice.

Tali decisioni osservano come l'indirizzo espresso non si pone in contrasto con l'insegnamento della Corte costituzionale (sentenza n. 170/2023 citata) – 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 –, atteso che il richiamato principio richiede l'applicazione delle garanzie previste dall'art. 15 Cost. e, dunque, l'intervento del pubblico ministero e non anche la preventiva autorizzazione del giudice.

Rileva, altresì, che la corrispondenza, anche informatica, costituisce prova documentale *ex art.* 234 c.p.p., senza che possa applicarsi l'art. 234 *bis* c.p.p., in quanto attiene a materiale disponibile in rete ovvero sia che, se non liberamente accessibile al pubblico, può essere acquisito mediante il consenso del «*legittimo titolare*».

A sostegno di tale argomentazione, si richiama, con riferimento all'acquisizione di prove già raccolte nello stato di esecuzione dell'o.e.i., l'art. 270 c.p.p. al fine di evidenziare come il trasferimento di prove tra procedimenti possa essere richiesto con provvedimento del pubblico ministero anche con riguardo ai risultati dell'attività di intercettazione, senza alcun provvedimento autorizzatorio del giudice, aggiungendo che la preventiva autorizzazione del giudice italiano per l'acquisizione di dati già nella disponibilità dell'autorità giudiziaria estera non è imposta dal diritto sovranazionale, atteso che la Direttiva 2002/58/UE riguarda il divieto per gli operatori telefonici di conservare i dati relativi al traffico e di ubicazione degli utenti, ma non vieta le intercettazioni o l'acquisizione di documentazione elettronica conservata nei dispositivi personali dell'utente o negli spazi virtuali su *server* in suo accesso esclusivo.

3. La soluzione delle Sezioni unite.

La suprema Corte nel suo più autorevole consesso ha ritenuto opportuno precisare, in via preliminare, che,

in relazione all'acquisizione mediante o.e.i. di messaggi scambiati su chat di gruppo con un sistema cifrato, già a disposizione dell'autorità giudiziaria estera, non è applicabile la disciplina dettata dall'art. 234 *bis* c.p.p., giacché la stessa si pone quale alternativa a quella prevista in tema di ordine europeo di indagine ed è quindi incompatibile con essa.

Le Sezioni unite spiegano, infatti, che l'art. 234 *bis* c.p.p. regola - come si evince dal tenore letterale della disposizione - non già un mezzo di prova, bensì una modalità di acquisizione di particolari elementi di prova presenti all'estero, attuata direttamente dall'autorità giudiziaria italiana e, prescinde pertanto da qualsiasi forma di collaborazione da parte dello Stato estero di esecuzione.

Lo strumento dell'o.e.i., sebbene regoli anch'esso una modalità di acquisizione di elementi di prova "transfrontalieri", si realizza, tuttavia, nell'ambito di rapporti di collaborazione tra autorità giudiziarie di diversi Stati membri dell'UE.

Pertanto, sottolineano le Sezioni Unite, si tratta di discipline che attengono a ipotesi diverse tra loro, già con riferimento al presupposto applicativo. E infatti, mentre l'art. 234 *bis* c.p.p. riguarda l'acquisizione di elementi conservati all'estero che non richiede forme di collaborazione con l'autorità giudiziaria dell'altro Stato, la disciplina relativa all'o.e.i. attiene all'acquisizione di elementi di prova conservati all'estero, mediante la collaborazione con l'autorità giudiziaria dello Stato straniero di esecuzione.

Tanto chiarito, viene evidenziato come la Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine (attuata in Italia con il d.lgs. n. 108 del 21 giugno 2017), preveda che la disciplina dettata sia preminente, con riferimento all'acquisizione di prove nell'ambito di rapporti di collaborazione tra autorità giudiziarie di Stati diversi dell'Unione Europea.

Dopo aver chiarito che la disciplina relativa all'acquisizione di elementi istruttori da parte dell'autorità giudiziaria italiana mediante ordine europeo di indagine è costituita dalla Direttiva 2014/41/UE e dal D.lgs. n. 108/2017, vengono esaminate le regole generali di questo sistema normativo.

Per quanto attiene alle condizioni di ammissibilità dell'ordine europeo di indagine, viene rimarcato che, soltanto se l'o.e.i. è stato legittimamente emesso, gli elementi acquisiti per suo tramite potranno essere validamente utilizzati nel procedimento penale pendente in Italia.

In tal senso, l'art. 27, co. 1, del d.lgs. n. 108/2017 prevede che «*il pubblico ministero e il giudice che procede possono emettere, nell'ambito delle relative attribuzioni, un ordine di indagine e trasmetterlo direttamente all'autorità di esecuzione*».

Sotto questo versante, secondo le Sezioni unite, la previsione di carattere generale di cui all'art. 1 del citato decreto legislativo induce a ritenere applicabili anche agli o.e.i. emessi dall'autorità giudiziaria italiana le condizioni di ammissibilità previste dall'art. 6, par. 1, della richiamata Direttiva 2014/41/UE, il quale consente all'autorità richiedente di emettere un o.e.i. soltanto quando essa ritenga soddisfatte le seguenti condizioni: a) l'emissione dell'o.e.i. è necessaria e proporzionata rispetto ai fini del procedimento, tenuto conto dei diritti della persona sottoposta a indagine o imputata; b) l'atto o gli atti di indagine richiesti mediante o.e.i. avrebbero potuto essere emessi alle stesse condizioni in un analogo caso interno.

Chiariscono le Sezioni unite che, sulla base del coordinamento normativo tra il d.lgs. n. 108/2017 e la Direttiva 2014/41/UE, è ragionevole sostenere che, ai fini dell'utilizzabilità degli atti acquisiti mediante o.e.i. dall'autorità giudiziaria italiana, è necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea (tra i quali il diritto alla difesa e al giusto processo), ma non anche l'osservanza, da parte dello Stato estero, di tutte le disposizioni previste dall'ordinamento giuridico italiano in materia di formazione e di acquisizione degli atti corrispondenti formati sul territorio italiano, tenuto conto che, da un lato, gli artt. 1 e 14 della Direttiva e il d.lgs. 108/2017 richiedono il rispetto dei richiamati principi; e, dall'altro, che l'art. 36 dello stesso decreto legislativo del 2017 non prevede ai fini dell'utilizzabilità degli atti formati all'estero la puntuale applicazione delle regole che sovrintendono la formazione dello stesso atto in Italia.

In tal senso, ai fini dell'accertamento del rispetto dei diritti fondamentali, vengono in rilievo i principi della presunzione relativa di conformità ai diritti fondamentali dell'attività svolta dall'autorità giudiziaria estera nell'ambito di rapporti di collaborazione ai fini dell'acquisizione di prove e dell'onere per la difesa di allegare e provare il fatto dal quale dipende la asserita trasgressione.

Infatti, come sancito dalla giurisprudenza nazionale ed europea con molte pronunce sul tema, nel caso in un una parte deduca il verificarsi di causa di nullità o di inutilizzabilità collegate ad atti non rinvenibili nel fascicolo del dibattimento, la stessa ha l'onere di precisa indicazione e di formale produzione delle risultanze documentali addotte a fondamento dell'eccezione formulata, anche sulla scorta della regola generale scolpita nell'art. 187, co. 2, c.p.p., secondo cui i fatti dai quali dipende l'applicazione di norme processuali

sono oggetto di prova^[5]. Pertanto, argomentano le Sezioni unite, l'onere di allegare e provare i fatti da cui dipende la violazione di diritti fondamentali, cui è collegata l'eccezione di inutilizzabilità o invalidità di atti istruttori acquisiti dall'autorità giudiziaria italiana mediante o.e.i., grava sulla parte che ha sollevato la relativa eccezione.

La suprema Corte chiarisce, poi, che la valutazione circa la sussistenza delle condizioni di ammissibilità dell'o.e.i. deve essere effettuata in base al tipo di atto specificamente richiesto e trasmesso, atteso che soltanto in tal modo è possibile verificare l'eventuale violazione dei diritti fondamentali della Costituzione e della Carta dei diritti fondamentali dell'Unione Europea, tra i quali, appunto, il diritto di difesa e il diritto ad avere un giusto processo.

Ebbene, nella vicenda sottoposta all'attenzione delle Sezioni unite, l'o.e.i. ha ad oggetto, come visto, l'acquisizione, da parte dell'autorità giudiziaria italiana, di messaggi scambiati su chat di gruppo mediante un sistema cifrato, già a disposizione dell'autorità giudiziaria francese.

Pertanto, si tratta di prove già in possesso dell'autorità giudiziaria estera e tale circostanza comporta diverse deroghe alla disciplina generale, al fine di renderne più agevole la circolazione dei dati probatori.

E infatti, in primo luogo, l'art. 10 della Direttiva 2014/41/UE prevede che, nel caso di prove già in possesso dell'autorità giudiziaria estera, quando, in base al diritto dello Stato di esecuzione, tali informazioni o prove avrebbero potuto essere acquisite nell'ambito di un procedimento penale o ai fini dell'o.e.i., è esclusa la possibilità, per l'autorità giudiziaria estera, di disporre un atto di indagine alternativo a quello richiesto.

In secondo luogo, dal combinato disposto degli artt. 12, par. 4, e 13, par. 1, della Direttiva citata, emerge che, quando le prove richieste mediante o.e.i. siano già in possesso dello Stato di esecuzione, la loro trasmissione allo Stato di emissione debba avvenire con immediatezza, in quanto non vi è alcun atto di indagine da compiere.

Del resto, nel nostro sistema processuale, la circolazione di prove già formate gode di una disciplina diversa e specifica rispetto a quella prevista per la formazione di prove di identica tipologia.

E invero, il codice di procedura penale (in particolare, il combinato disposto degli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p., relativi, rispettivamente, all'acquisizione di verbali di altri procedimenti, all'utilizzazione dei

risultati delle intercettazioni acquisite in procedimenti diversi e all'acquisizione di atti di un procedimento penale straniero) prevede che il pubblico ministero o la parte che vi ha interesse possano chiedere e ottenere la disponibilità di prove già formate in un procedimento penale, al fine di produrle in un altro procedimento penale, senza necessità di autorizzazione preventiva da parte del giudice competente per quest'ultimo, finanche nelle ipotesi in cui si tratti di prove (come le intercettazioni di comunicazioni o conversazioni), per la cui acquisizione sia necessaria la preventiva autorizzazione del giudice, fermo restando il potere del giudice stesso di valutare se ammettere e utilizzare tali prove acquisite *aliunde* ai fini della decisione.

Pertanto, sulla base dei rilievi svolti, le Sezioni unite stabiliscono che gli atti oggetto dell'o.e.i. relativi a prove già in possesso delle autorità competenti dello Stato di esecuzione, possono essere legittimamente richiesti e acquisiti dal pubblico ministero italiano senza la preventiva autorizzazione del giudice del procedimento nel quale si vorrebbe utilizzarli, in quanto tale condizione non è prevista nel nostro ordinamento, salvo il potere del giudice di valutare l'esistenza dei presupposti per ammettere tali prove e per utilizzarle ai fini della decisione, così garantendo il diritto di impugnazione nello Stato di emissione previsto dall'art. 14, par. 2, Direttiva 2014/41/UE e la verifica del rispetto dei principi riconosciuti dalla Costituzione e dalla Carta dei diritti fondamentali dell'UE e, in particolare, del diritto di difesa e del giusto processo, il cui onere di allegazione e di prova, grava, come visto, sulla parte che eccepisce l'inutilizzabilità o l'invalidità di tali prove per il mancato rispetto dei richiamati principi.

La Suprema Corte sottolinea, poi, che, ai fini della verifica della sussistenza delle condizioni di ammissibilità dell'o.e.i. (in particolare, di quelle previste dall'art. 6, par. 1, della citata Direttiva), e di eventuali violazioni dei diritti fondamentali, occorre individuare il tipo di atto trasmesso, atteso che, per alcuni di essi, è prevista una specifica disciplina da parte della normativa nazionale e sovranazionale.

Nel procedimento *de quo*, sono state attribuite a tali atti due qualificazioni: secondo l'ordinanza impugnata, trattasi di documenti informatici; secondo il ricorrente, invece, si tratterebbe di dati concernenti il traffico telefonico e telematico. Entrambe le prospettazioni escludono, dunque, che si tratti di risultati di intercettazioni di conversazioni o comunicazioni.

Ebbene, la qualificazione giuridica di tali atti quali documenti – che comprende anche quelli rappresentativi di comunicazioni elettroniche, quali i messaggi di posta elettronica già trasmessi e allocati nella memoria del dispositivo del destinatario o del mittente o nel server del gestore del servizio^[6] e i messaggi inviati tramite

l'applicativo WhatsApp o sms già trasmessi o conservati nella memoria di un'utenza cellulare^[7] comporta l'applicazione della disciplina dettata dall'art. 234 c.p.p., il quale consente l'acquisizione degli stessi.

Giova precisare, tuttavia, che, nelle ipotesi in cui tale prova documentale abbia ad oggetto comunicazioni scambiate in modo riservato tra un numero determinato di persone, indipendentemente dal mezzo tecnico impiegato, occorre assicurare la tutela prevista dall'art. 15 Cost. in materia di corrispondenza, come precisato dalla Corte costituzionale.

Il Giudice delle leggi, infatti, con le sentenze nn. 170/2023, 227/2023 e 2/2023, ha specificato che il concetto di corrispondenza comprende qualsiasi comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate, realizzata in modo diverso dalla conversazione in presenza e che prescinde dal mezzo tecnico utilizzato e, pertanto, si estende anche alla posta elettronica e ai messaggi inviati tramite l'applicativo WhatsApp o sms o sistemi simili, in quanto «*del tutto assimilabili a lettere o a biglietti chiusi*», perché accessibili soltanto mediante codici di accesso o altri meccanismi di identificazione.

Di conseguenza, in tali ipotesi, trova applicazione la tutela prevista dall'art. 15 Cost., che assicura la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, consentendone la limitazione sulla base delle riserve di legge e di giurisdizione, ovvero sia con le garanzie previste dalla legge e soltanto con atto motivato dell'autorità giudiziaria.

Il riferimento all'autorità giudiziaria, spiegano le Sezioni unite, non richiede, per la limitazione della libertà e della segretezza della corrispondenza e, quindi, per la relativa acquisizione in un procedimento penale, la necessità di un provvedimento di un giudice, in quanto tale espressione comprende sia la figura del giudice che quella del pubblico ministero (che, infatti, rientra nella categoria di autorità giudiziaria anche secondo il diritto euro-unitario, come affermato dalla Corte di Giustizia con la richiamata sentenza dell'8 dicembre 2020).

Del resto, precisano le Sezioni unite, tale osservazione è confermata dalla disciplina dettata dall'art. 254 c.p.p., il quale stabilisce che il sequestro di corrispondenza è disposto dall'autorità giudiziaria, senza richiamare la necessità dell'intervento del giudice, previsto espressamente, invece, per il sequestro da eseguire presso gli studi dei difensori dall'art. 103 c.p.p.; e dall'art. 353 c.p.p., il quale stabilisce che l'acquisizione di plichi chiusi di corrispondenza, anche in forma elettronica o telematica, è autorizzata, nel corso delle indagini preliminari, dal pubblico ministero che, quindi, è inteso quale titolare del potere di

disporre il sequestro.

Con riferimento alla verifica dei presupposti di ammissibilità della loro acquisizione di cui all'art. 6, paragrafo 1, Direttiva 2014/41/UE, relativo alla c.d. *"valutazione in astratto"*, l'acquisizione originaria della prova documentale nel sistema processuale italiano può essere disposta dal pubblico ministero, con atto motivato, senza alcuna necessità della preventiva autorizzazione del giudice, fatta eccezione per l'ipotesi di sequestro da eseguire presso lo studio del difensore di cui all'art. 103 c.p.p.

Pertanto, se l'o.e.i. ha ad oggetto l'acquisizione di documenti e corrispondenza che non costituiscono prove già in possesso dell'autorità competenti dello Stato estero, il rispetto della condizione che subordina il potere dell'autorità di emissione di disporre l'atto di indagine richiesto nell'o.e.i. alle medesime condizioni previste per l'analogo caso interno, è assicurato anche in assenza di un'autorizzazione del giudice, fatta salva l'ipotesi di cui all'art. 103 c.p.p., e, a maggior ragione, se si tratta di acquisizione di documenti, seppur relativi a corrispondenza, già in possesso dell'autorità giudiziaria estera, può essere chiesta mediante o.e.i. dal pubblico ministero senza necessità di autorizzazione del giudice.

Per quanto concerne il rispetto dei diritti fondamentali (la cui eventuale violazione deve essere allegata e provata dalla parte che la eccepisce), ove si versi in tema di corrispondenza, occorre rispettare i principi generali, quale, ad esempio, quello dettato dal richiamato art. 103 c.p.p., che prevede il divieto di sequestro e di ogni altra forma di corrispondenza tra l'imputato e il suo difensore, tranne che si tratti di corpo del reato.

La suprema Corte interpreta la previsione di cui all'art. 103 c.p.p., nel senso che *«le garanzie previste dall'art. 103 cod. proc. pen. si applicano esclusivamente nei confronti di colui che rivesta la qualità di difensore o investigatore in forza di specifico mandato conferitogli nelle forme di legge ed a condizione che i predetti soggetti non siano sottoposti a indagine»*^[8], essendo essenzialmente apprestate in funzione di garanzia del diritto di difesa dell'imputato e, quindi, non possono trovare applicazione nelle ipotesi in cui gli atti di cui all'art. 103 c.p.p. – ispezioni, perquisizioni e sequestri – debbano essere compiuti nei confronti di un avvocato sottoposto a indagine^[9].

Se si aderisce alla tesi, indicata nel ricorso, secondo la quale tali atti sono da considerarsi relativi al traffico telefonico e telematico, occorre far riferimento ai presupposti necessari per la loro acquisizione, previsti dall'art. 132 del d.lgs. n. 196/2003, ovvero sia che vi sia la preventiva autorizzazione del giudice con decreto motivato, che è adottato se sussistano sufficienti indizi di reati per i quali la legge stabilisce la pena

dell'ergastolo o della reclusione non inferiore nel massimo a tre anni e se siano rilevanti per l'accertamento dei fatti.

Tale disciplina riguarda, però, secondo le Sezioni unite, l'acquisizione dei dati presso il gestore dei servizi telefonici e telematici e non anche l'utilizzazione degli stessi in un procedimento penale diverso rispetto a quello nell'ambito del quale sono stati acquisiti e, pertanto, in tale ipotesi, possono essere acquisiti direttamente dal pubblico ministero, senza dover richiedere la preventiva autorizzazione del giudice competente per il procedimento nel quale intende utilizzarli.

Dunque, sulla base di tali osservazioni, l'organo requirente può avanzare richiesta di o.e.i., senza la preventiva autorizzazione del giudice nazionale, per la trasmissione di dati relativi al traffico telefonico o telematico, già acquisiti dall'autorità giudiziaria straniera, e tale situazione non si pone in contrasto con i diritti fondamentali, in quanto la valutazione circa la sussistenza dei presupposti per l'acquisizione originaria di tali dati è stata già effettuata dal giudice che l'ha autorizzata.

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

Sulla base di tali rilievi, le Sezioni unite hanno enunciato i seguenti principi di diritto:

- *«La trasmissione, richiesta con ordine europeo di indagine, del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, **non rientra nell'ambito di applicazione dell'art. 234-bis cod. proc. pen.**, che opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie, bensì nella disciplina relativa alla **circolazione delle prove tra procedimenti penali**, quale desumibile dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen.».*
- *«In materia di ordine europeo di indagine, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere **legittimamente richieste ed acquisite dal pubblico ministero italiano senza***

la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle».

- «L'emissione, da parte del pubblico ministero, di ordine europeo di indagine diretto ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, **non deve essere preceduta da autorizzazione del giudice italiano**, quale condizione necessaria a norma dell'art. 6 Direttiva 2014/41/UE, perché tale autorizzazione, nella disciplina nazionale relativa alla circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento».
- «La disciplina di cui all'**art. 132 d.lgs. n. 196 del 2003**, relativa all'acquisizione dei dati concernenti il **traffico di comunicazioni elettroniche** e l'ubicazione dei dispositivi utilizzati, si applica alle richieste rivolte ai fornitori del servizio, ma **non anche a quelle dirette ad altra autorità giudiziaria che già detenga tali dati**, sicché, in questo caso, il **pubblico ministero può legittimamente accedere agli stessi senza chiedere preventiva autorizzazione al giudice** davanti al quale intende utilizzarli».
- «L'utilizzabilità del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera, in un procedimento penale pendente davanti ad essa, e trasmesso sulla base di ordine europeo di indagine, deve essere **esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali**, fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione **grava sulla parte interessata**».
- «L'impossibilità per la difesa di **accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo** delle stesse **non determina una violazione dei diritti fondamentali**, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il **pericolo di alterazione** dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente».

Sulla base di tali considerazioni, la Suprema Corte, respinte, in quanto infondate, tutte le eccezioni difensive, ha rigettato il ricorso.

In particolare, i motivi di ricorso relativi alla utilizzabilità delle comunicazioni sono stati ritenuti infondati, in quanto, per le ragioni sopra esposte, la disciplina applicabile non è quella di cui all'art. 234 *bis* c.p.p., essendo la stessa alternativa a (e incompatibile con) quella dettata in tema di o.e.i., ma, in ogni caso, l'ordinanza

impugnata non è annullabile, in quanto sono state rispettate tutte le condizioni di ammissibilità dell'o.e.i.

Inoltre, non vi è stata la prova della lesione dei diritti fondamentali dei soggetti interessati, come sostenuto nel ricorso.

Le Sezioni unite hanno poi sgombrato il campo da qualsiasi dubbio interpretativo rispetto alla Direttiva 2014/41/UE, così respingendo la richiesta di disporre il rinvio pregiudiziale alla Corte di Giustizia e di sollevare la questione di legittimità costituzionale.

4. Osservazioni conclusive.

Le Sezioni unite, come esposto, hanno aderito, tra quelle in premessa enunciate, alla terza scuola di pensiero, secondo la quale la richiesta, da parte dell'autorità giudiziaria italiana, mediante ordine europeo di indagine, volto ad acquisire comunicazioni scambiate in chat di gruppo con sistema cifrato, già ottenute e decifrate dall'autorità giudiziaria estera, è regolata dalla disciplina generale relativa alla circolazione delle prove tra procedimenti penali, come desumibile dal codice di rito.

Si fa riferimento, infatti, alle disposizioni di cui agli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p., le quali consentono al pubblico ministero di disporre l'acquisizione di dati o prove acquisite in un diverso procedimento penale.

Per tali motivi, anche i dati sopra indicati possono essere acquisiti direttamente dal pubblico ministero mediante o.e.i., senza la preventiva autorizzazione del giudice.

Tale soluzione, spiegano, le Sezioni unite, è perfettamente compatibile con l'insegnamento della Corte costituzionale sulla tutela della corrispondenza – essendo rispettata, con il provvedimento del pubblico ministero di acquisizione, la riserva di legge prevista dall'art. 15 Cost. – e non si pone in contrasto con la disciplina dettata dall'art. 132 del d.lgs. n. 196/2003 per l'acquisizione di dati relativi al traffico telefonico e telematico – che richiede la preventiva autorizzazione del Giudice –, giacché tale normativa attiene ai dati da acquisire presso i relativi gestori e non quelli, come nel caso sottoposto al vaglio della suprema Corte, già acquisiti dall'autorità giudiziaria estera.

In ogni caso, si evidenzia nella sentenza in commento, resta salvo il potere del giudice italiano di valutare l'utilizzabilità ai fini della decisione di tali elementi, la quale andrà esclusa soltanto qualora la stessa comporti una violazione dei diritti fondamentali, che deve essere allegata e provata dalla parte che l'ha eccepita.

Pertanto, il giudice nomofilattico fornisce una soluzione al caso che risponde, in primo luogo, all'esigenza di rapida acquisizione dei dati necessari ai fini di indagine – attribuendo il relativo potere al pubblico ministero senza necessità della preventiva autorizzazione giudiziale –, assicurando, in ogni caso, la tutela dei diritti dei soggetti interessati, attraverso il controllo successivo del giudice, che, infatti, dovrà escludere l'utilizzabilità degli stessi se la parte che eccepisce la relativa invalidità adempie all'onere di allegazione e di dimostrazione della lesione dei suoi diritti fondamentali previsti dalla Costituzione e dalla Carta di Nizza (in particolare, del diritto di difesa e del diritto al giusto processo).

Inoltre, aderendo questa volta alla tesi più risalente, la Corte supera anche l'eccezione relativa all'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse, chiarendo che tale circostanza non determina una violazione dei diritti fondamentali, giacché, salvo specifiche allegazioni di segno contrario, non ricorre il pericolo di alterazione dei dati, in considerazione del fatto che il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ragione per cui una chiave errata non ha alcuna possibilità, neppure parziale, di decriptazione.

È di tutta evidenza, quindi, che, con la decisione in commento, le Sezioni unite, nel dirimere i contrasti interpretativi sottoposti alla sua attenzione, realizzano l'equo temperamento tra le necessità di acquisire velocemente gli elementi investigativi – attribuendo il relativo potere direttamente al pubblico ministero, così tutelando anche la riserva di giurisdizione prevista dall'art. 15 Cost., nel caso in cui i dati conservati all'estero costituiscano corrispondenza, nell'accezione fornita dalla Corte costituzionale –, e quella di garantire, in ogni caso, il controllo sul rispetto dei diritti fondamentali della persona interessata, attraverso l'intervento successivo del giudice italiano, che sarà chiamato a valutare l'eventuale inutilizzabilità dei dati richiesti e ottenuti dall'autorità giudiziaria estera, nel caso in cui la loro utilizzazione si ponga in contrasto con i diritti fondamentali della persona, a condizione che il soggetto che la eccepisce dimostri rigorosamente la lesione delle sue garanzie costituzionalmente e convenzionalmente previste.

[1] Cfr. Cass. pen., sez. I, 13 gennaio 2023, n. 19082; Cass. pen., sez. I, 13 ottobre 2022, n. 6363; Cass. pen., sez. I, 13 ottobre 2022, n. 6364; Cass. pen., sez. I, 1° luglio 2022, n. 34059.

[2] Il riferimento è alle richiamate Cass., sent. n. 19082 del 2023; Cass., sent. n. 6363/2022; Cass., sent. n. 6364/2022.

[3] Cass. pen., sez. III, 19 ottobre 2023, n. 47201; Cass. pen., sez. IV, 30 maggio 2023, n. 37503; Cass. pen., sez. IV, 5 aprile 2023, n. 16347; Cass. pen., sez. IV, 5 aprile 2023, n. 16345; Cass. pen., sez. IV, 28 marzo 2023, n. 17647.

[4] Cass. pen., sez. VI, 26 ottobre 2023; Cass. pen., sez. VI, 11 ottobre 2023, n. 48838; Cass. pen., sez. VI, 27 settembre 2023, n. 46482.

[5] Cfr., ex multis, Cass. pen., sez. VI, 4 ottobre 2023, n. 44882; Cass. pen., sez. III, 12 ottobre 2021, n. 1396; Cass. pen., sez. IV, 6 novembre 2019, n. 19216; Cass. pen., sez. un., 16 luglio 2009, n. 39061; conf. Cass. pen., sez. un., 17 novembre 2004, n. 45189; Cass. pen., sez. V, 19 aprile 2023, n. 23015; Cass. pen., sez. VI, 14 dicembre 2017, n. 18187; si veda sul tema anche Corte di Giustizia, sentenza 11 novembre 2021, Gavanozov, C-852/19; conf. Corte di Giustizia, sentenza 8 dicembre 2020, Staatsanwaltschaft Wien, C-584/19.

[6] Cfr., ex multis, Cass. pen., sez. VI, 6 febbraio 2020, n. 12975; Cass. pen., sez. III, 16 aprile 2019, n. 29426.

[7] Cass. pen., sez. VI, 16 marzo 2022, n. 22417; Cass. pen., sez. V, 21 novembre 2017, n. 1822.

[8] In termini, Cass. pen., sez. VI, 9 novembre 2018, n. 8295; conf., ex multis, Cass. pen., sez. II, 16 maggio 2006, n. 31177; Cass. pen., sez. II, 16 maggio 2012, n. 32909.

[9] Cass. pen., sez. V, 5 dicembre 2011, n. 12155.