

**Penale Sent. Sez. 1 Num. 6363 Anno 2023**

**Presidente: SIANI VINCENZO**

**Relatore: TOSCANI EVA**

**Data Udiienza: 13/10/2022**

### **SENTENZA**

sul ricorso proposto da:

██████████ nato a ██████████

avverso l'ordinanza del 17/05/2022 del TRIB. LIBERTA' di ROMA

udita la relazione svolta dal Consigliere EVA TOSCANI;

lette le conclusioni del PG FRANCA ZACCO

Il PG conclude chiedendo il rigetto del ricorso.

udito il difensore

L'avv. ██████████ conclude riportandosi ai motivi di ricorso e chiede l'annullamento con rinvio dell'ordinanza impugnata.

Alle ore 12.28 l'udienza viene sospesa.

Alle ore 12.43 l'udienza riprende.

## RITENUTO IN FATTO

1. Con la decisione indicata nel preambolo, il Tribunale di Roma, in funzione di giudice del riesame, ha confermato l'ordinanza con cui il Giudice per le indagini preliminari dello stesso Tribunale aveva applicato la misura cautelare della custodia in carcere a ██████████ gravemente indiziato del tentato omicidio premeditato ai danni di ██████████ dei connessi reati di porto e detenzione illegali della pistola utilizzata per realizzarlo.

Nell'esaminare i motivi di gravame, il Tribunale è pervenuto alle conclusioni che seguono:

- è pienamente utilizzabile la messaggistica o chat Sky Ecc riconducibile all'ID SQHH3Q in uso all'indagato, acquisita in diverso procedimento penale presso l'autorità giudiziaria francese tramite ordine europeo d'indagine; si tratta di dati non captati in concomitanza con il flusso di comunicazioni, attività quest'ultima che deve essere necessariamente preceduta da un provvedimento di autorizzazione preventiva secondo la disciplina in materia d'intercettazioni telefoniche o telematiche e, pertanto, assimilabili ai documenti, perché fisicamente conservati nel *server* del gestore;
- l'acquisizione delle *chat* da parte della polizia francese è avvenuta con modalità conformi all'ordine di indagine europeo che aveva richiesto l'estrazione dei dati relativi allo specifico ID, strettamente inerente alla vicenda omicidiaria. Vige peraltro in materia la presunzione di legittimità dell'attività svolta dall'autorità giudiziaria straniera; la richiesta ha, infatti, a oggetto l'acquisizione degli esiti di attività d'indagine disposta dall'autorità francese nel corso di autonome investigazioni disciplinate dalla legislazione interna;
- l'individuazione di ██████████ quale reale utilizzatore dell'ID SQHH3Q, nell'agosto 2020, al di là dei dubbi espressi dalla difesa sulla base di ricostruzioni meramente ipotetiche, si evince dal contenuto della messaggistica contenente ripetuti e univoci riferimenti diretti alla persona dell'indagato, attraverso il riferimento di informazioni strettamente personali;
- segnatamente, dall'analisi del susseguirsi dei messaggi Sky Ecc, emerge che a sparare sia stato ██████████ e, comunque, che egli si era appositamente armato per recarsi all'incontro con ██████████ con il quale aveva motivi di contrasto. La consulenza medico-legale ha evidenziato che le lesioni prodotte dai due proiettili che attinsero la vittima, al capo e allo stomaco, erano idonee entrambe a cagionarne la morte e che è residuo l'indebolimento permanente di più organi.

2. Ricorre ██████████ per messo del difensore di fiducia, sviluppando cinque motivi.

2.1. Con il primo denuncia vizio della motivazione con riferimento all'acquisizione, mediante ordine europeo d'indagine richiesto alle autorità francesi, dei messaggi che si assumono scambiati dall'indagato sulla piattaforma di comunicazione Sky Ecc.

Il Tribunale – secondo il ricorrente – ha negato validità delle eccezioni difensive circa l'avvenuta acquisizione dei dati informatici in assenza di garanzie in ordine alla loro genuinità, avendo l'autorità giudiziaria francese disatteso le formalità di esecuzione dell'ordine di investigazioni europeo trasmesso dalla procura italiana e, tra queste, quella dell'indicazione del protocollo di informatica forense utilizzato per garantire la corrispondenza del dato originale con quello trasmesso.

In assenza del sequestro del telefono o della banca dati non vi è alcuna possibilità di verificare la genuinità del contenuto dei messaggi, peraltro estrapolati dalla polizia giudiziaria italiana nonostante l'ordine europeo di indagine. L'autorità francese ha, infatti, trasmesso l'intero *data set* delle utenze interessate, dal quale la polizia giudiziaria ha estrapolato i dati grazie alle informazioni fornite dalla polizia giudiziaria francese sulla chiave di decifrazione.

L'acquisizione dei dati non risulta con certezza essere stata compiuta autonomamente ed esclusivamente dall'autorità straniera. Al contrario residua il fondato dubbio che l'acquisizione sia il frutto di attività compiuta da più forze di polizia.

L'impossibilità di utilizzare le conversazioni avvenute per il tramite della messaggistica riportata vuota di contenuto la valutazione dell'ordinanza in tema di gravità indiziaria non superando gli indizi raccolti, depurati dal contenuto della messaggistica suddetta, la cosiddetta prova di resistenza.

La difesa è tornata su tale primo motivo di censura, approfondendolo, con i motivi nuovi ritualmente depositati.

Nel ribadire l'inutilizzabilità dei messaggi che sono transitati sul cripto cellulare in uso all'indagato, ha posto in risalto come le censure difensive abbiano trovato recente, autorevole riscontro in una pronuncia in sede di legittimità che, in una situazione analoga a quella in esame ha determinato l'annullamento con rinvio di un'ordinanza cautelare, riconoscendo alla difesa «il diritto di conoscere le modalità di svolgimento dell'attività investigativa svolta il procedimento di acquisizione di una messaggistica criptata» (Sez. 4, n. 32915 del 15/07/2022).

2.2. Con il secondo motivo deduce vizio di motivazione con riferimento alla richiesta di esclusione dell'aggravante della premeditazione.

Nonostante l'espressa richiesta di una concreta verifica della sussistenza di detta circostanza aggravante, l'ordinanza impugnata ha eluso ogni risposta con un'affermazione meramente assertiva imperniata sulla carenza di interesse.

2.3. Con il terzo motivo deduce vizio di motivazione con riferimento alla sussistenza dell'aggravante della premeditazione alla luce dei criteri individuati dalla giurisprudenza di legittimità.

Nel confermare integralmente l'ordinanza applicativa della misura cautelare, il Tribunale del riesame ha fatto propria la qualificazione giuridica indicata nell'imputazione provvisoria che ascrive all'indagato una condotta premeditata.

Nel giustificare l'adesione a tale qualificazione giuridica, il giudice della cautela si è soffermato unicamente sull'elemento cronologico, sottolineando la circostanza che l'indagato, il giorno prima dell'agguato occorso il 4 agosto 2020, si era recato a Salerno, per procurarsi sia l'arma impiegata per l'esecuzione del grave fatto di sangue, sia per reclutare i complici che l'avevano effettivamente accompagnato all'incontro.

L'ordinanza di custodia cautelare non solo trascura l'ulteriore elemento che deve necessariamente sussistere, ovvero quello ideologico, ma addirittura lo contraddice allorquando (a p. 8) individua quale fattore scatenante della violenta reazione di ██████████ nell'insistenza da parte della vittima nelle sue pretese creditorie, "allargandosi eccessivamente", spingendosi fino a suonare a casa del suo debitore e a minacciarne la compagna di mandarli via di casa.

2.4. Con il quarto motivo prospetta la contraddittorietà della motivazione in punto di esigenze cautelari.

Il pericolo di recidiva è stato desunto esclusivamente dalla gravità del fatto, oltre che per la condotta susseguente, che si assume essere stata caratterizzata da protratta irreperibilità e dall'assenza di ogni resipiscenza. Si tratta di una motivazione in contrasto con la ricostruzione dei fatti, avallata dal giudice della cautela, che ha individuato il movente nelle condotte provocatorie della vittima e nella paura di perdere la casa.

Ugualmente insussistente è il pericolo di fuga, del tutto ipotetico, poiché l'indagato non è mai stato latitante, bensì si è trasferito legittimamente in Spagna, dove ha vissuto con la propria compagna dove ha svolto attività lavorativa, utilizzando le proprie generalità, senza mai sfuggire alle proprie eventuali responsabilità.

3. Il Sostituto Procuratore generale, ██████████ ha prospettato il rigetto del ricorso.

### **CONSIDERATO IN DIRITTO**

Il Collegio ritiene che il ricorso vada accolto limitatamente alla declaratoria d'inammissibilità della richiesta di riesame sull'aggravante della premeditazione.

1. Infondato è il primo motivo di ricorso, concernente l'eccezione inutilizzabilità delle *chat* relative alle comunicazioni intrattenute dall'indagato, utilizzando la rete Sky ECC tramite un apposito *smartphone*.

1.1. Al fine di inquadrare correttamente le questioni giuridiche poste all'attenzione del Collegio, non è superfluo evidenziare come il sistema SKY Ecc sia una piattaforma di comunicazione criptata che consente lo scambio di comunicazioni utilizzando i cc.dd. criptofonini, ovverosia *smartphone* opportunamente modificati nel *software* (prevalentemente con il sistema Android o Blackberry) con l'unico scopo di garantirne l'inviolabilità, poiché il relativo sistema operativo è caratterizzato da particolari requisiti di sicurezza che si possono riassumere nella cifratura dei dati trasmessi e di quelli memorizzati, nella possibilità per l'utilizzatore di cancellare, quasi in tempo reale e anche da remoto l'intera memoria del telefono inserendo un cd. *panic code*, o nella possibilità di segnalare la presenza di sistemi di individuazione (cd. Imsi Catcher) o di tentativi di aggressione informatica da parte di agenti esterni.

Il sistema di comunicazione di Sky-ECC non è basato sulla tecnologia Pin to Pin (tipo Blackberry, vale a dire su un sistema crittografico dove le chiavi di cifratura sono collocate in un server), bensì sul sistema *end to end* che prevede la cifratura delle conversazioni mediante l'utilizzo di chiavi depositate esclusivamente sui dispositivi che colloquiano, sicché, in questa modalità, neanche il gestore del servizio è in grado di conoscere le chiavi utilizzate e di conseguenza il contenuto delle comunicazioni.

1.2. Si apprende dal provvedimento impugnato e dalla documentazione in atti dallo stesso richiamata che la messaggistica è stata acquisita (cfr. nota Ros in data 11 agosto 2021, richiamata) in esito a un'operazione conclusasi a marzo 2021 (operazione ~~XXXX~~), svolta da una squadra investigativa comune costituita tra autorità francesi, olandesi e belghe, in esito alla quale gli investigatori stranieri hanno avuto accesso a centinaia di milioni di messaggi degli utenti di SKY ECC.

Il dato probatorio nel presente processo è stato ottenuto in esecuzione di un ordine europeo d'indagine (O.I.E.), rivolto alla competente autorità francese che, in persona del Vice-president Chargé de l'instruction del Tribunal Judiciaire de Paris, ha poi provveduto, trasmettendo i dati ufficiali riversati su un CD con allegato verbale delle operazioni svolte, autorizzando la Procura di Roma ad utilizzare i dati così trasmessi.

Il Tribunale ha dato conto del fatto che l'O.I.E. si basava sul codice IMEI dello *smartphone* rinvenuto nella disponibilità dell'indagato e nell'ordinanza cautelare si precisa che l'utenza criptata era stata previamente materia di scambio informativo

spontaneo da parte di Europol ex art. 7 della decisione Quadro 2006/960/GAI del 18/12/02, segnalando l'effettiva presenza di quel codice identificativo nel *database* di cui poteva disporre.

1.3. Di conseguenza, rileva il Collegio, il materiale che è stato posto a disposizione dell'Autorità giudiziaria italiana è costituito dai dati informatici relativi alle conversazioni e alle comunicazioni trasmesse mediante il criptofonino che utilizzava l'indagato, così come è altrettanto pacifico che i *files* oggetto di esame siano la copia di quelli che sono stati trasmessi dall'Autorità giudiziaria francese già decriptati; l'operazione di decriptazione è stata eseguita dalle polizie straniere mediante l'individuazione del necessario algoritmo di criptazione utilizzato dalla società proprietaria del sistema di cifratura SKY ECC.

Riguardo alla questione della natura delle *chat* oggetto di doglianza è già stato chiarito (Sez. 1, n. 34059 del 01/07/2022, Molisso, non mass.; Sez. 6 n. 18907 del 20/04/2021, Civale, Rv. 281819 - 01) che occorre distinguere due diversi tipi di operazione che gli inquirenti possono effettuare nello svolgimento delle indagini, segnatamente: le operazioni di captazione e di registrazione del messaggio cifrato nel mentre lo stesso è in transito dall'apparecchio del mittente a quello del destinatario, che viaggia attraverso reti *internet* messe a disposizione in ogni paese da gestori di servizi telematici e che, lungo tale 'tragitto' transita di regola da un server che non è necessariamente collocato nel paese o in uno dei paesi nei quali si trovano fisicamente i soggetti che stanno comunicando tra loro, e le diverse operazioni di decrittazione del contenuto del messaggio, necessarie per trasformare mere stringhe informatiche in dati comunicativi intellegibili.

E' chiaro che solo alla prima delle due appena indicate tipologie di operazioni fa riferimento l'art. 266-*bis* cod. proc. pen., che estende l'applicabilità delle norme del codice di rito relative alle 'normali' intercettazioni di conversazioni o comunicazioni tra soggetti a distanza, alle intercettazioni di flussi di comunicazioni relativi a sistemi telematici ovvero intercorrenti tra più sistemi telematici: flussi che non avvengono in via diretta tra apparecchi informatici, ma che sfruttano la trasmissione dei dati in via telematica, dunque via cavo o ponti radio, ovvero per mezzo di altra analoga strumentazione tecnica (nel senso della qualificazione come intercettazione ai sensi dell'art. 266-*bis* cod. proc. pen. dell'acquisizione dei contenuti di messaggistica in atto effettuata con sistema Blackberry, cfr. Sez. 4, n. 49896 del 15/10/2019, Brandimarte, Rv. 277949-01; Sez. 3, n. 47557 del 26/09/2019, Scognamiglio, Rv. 277990-01/02; Sez. 3, n. 50452 del 10/11/2015, Guarnera, Rv. 265615-01).

Laddove il messaggio telematico sia "in chiaro", cioè non criptato la sua captazione e la sua registrazione ne rendono immediatamente intellegibile il

contenuto e, perciò, direttamente utilizzabile a fini di prova il relativo risultato conoscitivo.

Se, invece, il messaggio telematico, come è accaduto nel caso di specie, sia criptato, gli inquirenti ne possono valorizzare il contenuto a fini dimostrativi solo laddove abbiano la disponibilità dell'algoritmo che consente di decriptarne il tenore ovvero se tale 'chiave' venga altrimenti messa a disposizione degli investigatori dalla società che ne è proprietaria (e che la sfrutta dal punto di vista commerciale).

Così delineati i termini della questione, deve escludersi che l'attività di acquisizione e di decifrazione di tali dati comunicativi rientri nel novero delle attività di intercettazione poiché queste ultime postulano la captazione di un flusso di comunicazioni in atto, di tal che non è applicabile la relativa disciplina processuale contenuta negli artt. 266 e ss. del codice di rito, la cui estensione alle intercettazioni dei flussi di comunicazioni relativi a sistemi telematici ovvero intercorrenti tra più sistemi telematici è prescritta dall'art. 266-*bis* cod. proc. pen.

Nel caso in esame trova invece applicazione l'art. 234-*bis* cod. proc. pen. (introdotto dall'art. 2, comma 1-bis, del decreto legge 18 febbraio 2015, n. 7, convertito dalla legge 17 aprile 2015, n. 43), norma secondo cui «È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».

Si tratta di disposizione applicabile anche nel caso *de quo*, nel quale l'acquisizione ha riguardato non un documento cartaceo o analogico, bensì un documento inteso come «rappresentazione comunicativa incorporata in una base materiale con un metodo digitale», ovvero dati informatici che hanno consentito di rendere intellegibile il contenuto di stringhe redatte secondo il sistema binario. Vi è stato, altresì, il consenso all'acquisizione da parte del "legittimo titolare" di quei documenti o dati conservati all'estero, da intendersi come persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del paese estero, identificabile non soltanto nella persona fisica e/o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria, nell'autorità giudiziaria, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'*internet service provider*.

Del resto - come si evince dalla lettura dell'O.I.E. trasmesso al *Tribunal judiciaire* di Parigi - l'autorità italiana non ha mai formulato richiesta a quella francese di procedere ad attività di intercettazione telefonica/telematica (nel questo caso bisognava completare la sezione H7 dell'O.I.E.) ovvero di atti d'indagine implicanti l'acquisizione di prove in tempo reale, in modo

continuo e per un determinato periodo di tempo (nel qual caso sarebbe venuta in rilievo la sezione H5 dell'O.I.E.), ma ha unicamente formulato richiesta di trasmissione di copia dei messaggi riferibili ai PIN di interesse cambiati sulla piattaforma Sky-ECC, messaggi, come detto, già acquisiti.

1.4. Ciò di cui si è dato sin qui conto consente di valutare le deduzioni difensive e rilevarne l'infondatezza.

Priva di pregio è la doglianza secondo la quale l'Autorità giudiziaria francese avrebbe disatteso le formalità di esecuzione dell'ordine d'investigazione europeo trasmesso dalla Procura italiana e, segnatamente, quella dell'indicazione del protocollo d'informatica forense, necessario per garantire la corrispondenza del dato originale con quello trasmesso.

La difesa si duole del fatto che l'Autorità francese, invece di veicolare il dato informatico attraverso una codifica *hash*, abbia utilizzato comuni *file excel 3* privi della tutela di una *password* di protezione di scrittura, con ogni conseguenza in termini di genuinità dei dati e tutela da rischio di manipolazione durante l'operazione di decrittazione.

La censura non coglie nel segno perché confonde il tema della genuinità del dato decrittato con quello della garanzia di quella che viene definita come catena di custodia.

Sotto il primo profilo, si osserva che l'attività di acquisizione di dati in giacenza (definiti freddi) o l'intercettazione di dati telematici in transito permette l'acquisizione, qualora il messaggio telematica sia criptato mediante un impiego di un algoritmo o di una chiave di cifratura e trasformato in un mero dato informatico, di una stringa informatica composta da un codice binario. In questo caso - come si è già detto - l'intelligibilità del messaggio è subordinata all'attività di decriptazione che presuppone la disponibilità dell'algoritmo che consente di trasformare il codice binario in un contenuto dimostrativo, ma ogni messaggio cifrato è inscindibilmente accoppiato alla sua chiave di cifratura, sicché la sola chiave esatta produrrà una decifrazione corretta, dovendosi escludere che possa decifrarne una parte corretta e uno non corretta; né vi sono possibilità che una chiave errata possa decrittare il contenuto, anche parziale, del codice umano contenuto.

Si richiama in proposito quanto chiarito da questa Corte (Sez. 2, n. 30395 del 21/04/2022, Chianchiano, Rv. 283454 - 01; Sez. 6, n. 14395 del 27/11/2019, Testa, Rv. 275534 - 01) secondo cui, in assenza dell'algoritmo necessario alla decrittazione, secondo la scienza informatica, risulta impossibile ottenere un testo difforme dal reale, potendosi al più imbattersi in una sequenza alfanumerica o simbolica (detta stringa) priva di senso alcuno.



Pertanto, salva l'allegazione di specifici e concreti elementi di segno contrario, nel presente caso non prospettati, deve escludersi la ricorrenza di alterazioni ovvero manipolazione dei testi captati.

Sotto il secondo profilo, quella dell'algoritmo di Hash non è l'unica, sebbene sia la più diffusa, metodica idonea a garantire una corretta catena di custodia, ben potendosi la stessa ottenere legandola al contenitore, invece che al contenuto (come nel caso della stringa di HASH, progettata in modo da poter fungere da *sigillo digitale*), attraverso l'uso di contenitori non modificabili, ovvero sia l'uso di supporti di memoria a tecnologia ottica non riscrivibile (CD e DVD).

Ciò è stato fatto dalle autorità francesi, risultando inoltre dal verbale di trasmissione in data 22 ottobre 2021, in atti, che i dati richiesti sono stati riversati in supporti ottici non riscrivibili (cd-rom) e trasmessi all'interno di buste sigilliate antieffrazione.

Sotto altro profilo, osserva il Collegio come l'attestazione da parte dell'Autorità giudiziaria francese secondo la quale i dati trasmessi in esecuzione dell'O.I.E. corrispondano a quelli acquisiti nei procedimenti francesi risulti attestata nello stesso verbale di esecuzione (*Commission rogatoire*) in data 16 settembre 2021, in atti, nel quale il giudice istruttore francese, nel delegare la polizia giudiziaria al compimento dell'attività materiale di "copia", espressamente dichiara che «*Disons que les procès-verbaux dressés nous seront transmis, avec une copie certifiée dans le meilleur délai*» («i verbali saranno trasmessi con copia certificata al più presto»).

Si è, dunque, in presenza di un'attestazione di conformità da parte sia del giudice francese che dell'autorità investigativa che ha eseguito l'estrazione, attestazione che sulla base del già richiamato principio della reciproca fiducia in forza delle relazioni intercorrenti dagli stati, consente di realizzare la presunzione di legittimità degli atti compiuti dalle autorità straniere secondo la legislazione dello specifico stato straniero.

1.5. Del pari infondata la censura compendiata nella seconda parte del primo motivo di ricorso.

La difesa dubita, peraltro esprimendo tale dubbio in termini meramente ipotetici e aspecifici, che l'attività d'intercettazione/acquisizione della messaggistica sulla piattaforma Sky Ecc sia avvenuta sotto la direzione e il controllo dell'Autorità giudiziaria, ipotizzando che la stessa sia il frutto di attività di polizia giudiziaria.

La censura trascura di considerare come l'acquisizione delle *chat* sia avvenuta con ordine europeo d'indagine, disciplinato dal d.lgs. 27 giugno 2017, n. 108, emanato per dare attuazione alla direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014.

L'art. 2 della direttiva stabilisce che «Gli Stati membri eseguono un OEI in base al principio del riconoscimento reciproco e conformemente alla presente direttiva» e l'art. 9 che «L'autorità di esecuzione riconosce un OEI, trasmesso conformemente alle disposizioni della presente direttiva, senza imporre ulteriori formalità e ne assicura l'esecuzione nello stesso modo e secondo le stesse modalità con cui procederebbe se l'atto d'indagine in questione fosse stato disposto da un'autorità dello Stato di esecuzione, a meno che non decida di addurre uno dei motivi di non riconoscimento o di non esecuzione ovvero uno dei motivi di rinvio previsti dalla presente direttiva».

Tali elementi, che assumono rilievo ai fini dell'interpretazione del decreto attuativo, implicano che l'ordine europeo d'indagine deve aver a oggetto una prova acquisibile nello Stato di emissione e deve essere eseguito in conformità di quanto previsto nello Stato di esecuzione per il compimento di un analogo atto di acquisizione probatoria, potendosi peraltro presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo concreta verifica di segno contrario.

Va, infatti, ricordato a tale ultimo proposito che, secondo un consolidato orientamento della giurisprudenza di legittimità, l'utilizzazione degli atti trasmessi a seguito di attività di cooperazione internazionale (si vedano le plurime decisioni in tema di rogatoria attiva) non è condizionata a un accertamento da parte del giudice italiano concernente la regolarità delle modalità di acquisizione esperite dall'autorità straniera, in quanto vige la presunzione di legittimità dell'attività svolta e spetta al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate nella fase delle indagini preliminari (in tal senso, Sez. 5, n. 1405 del 16/11/2016, dep. 2017, Ruso, Rv. 269015 - 01; Sez. 2, n. 24776 del 18/05/2010, Mutari, Rv. 247750 - 01; Sez. 1, n. 21673 del 22/01/2009, Pizzata, Rv. 243796 - 01).

In particolare, proprio in tema di valutazione della sussistenza dei gravi indizi di colpevolezza richiesti per l'adozione di provvedimenti di cautela personale nella fase delle indagini preliminari, è stata condivisibilmente affermata l'utilizzabilità della documentazione di atti compiuti autonomamente da autorità straniere in un diverso procedimento penale all'estero, anche al di fuori dei limiti stabiliti per la loro utilizzabilità dagli artt. 238 cod. proc. pen. e 78 disp. att. cod. proc. pen., con il solo limite che tale attività non sia in contrasto con norme inderogabili e principi fondamentali, i quali, però, non si identificano necessariamente con il complesso delle regole dettate dal nostro codice di rito, spettando inoltre a chi eccepisca tale incompatibilità l'onere di dare la prova di tale incompatibilità (cfr. Sez. 5, n. 45002 del 13/07/2016, Crupi, Rv. 268457 - 01).

E - aggiunge il Collegio - questo limite appare difficilmente rinvenibile in attività giudiziarie di uno Stato membro dell'Unione Europea, tenuto a

condividere i principi fondamentali dell'ordinamento europeo, come la Francia, nel cui ordinamento le garanzie della libertà individuale e della riservatezza delle comunicazioni rappresentano un baluardo costituzionale e le cui attività investigative relative a queste piattaforme sono state ritenute correttamente svolte sia dalla Corte di cassazione (sentenza del 2.4.2022) e dalla Corte costituzionale francese (decisione n. 2022 -987 QPC dell'8.4.2022).

Il giudice italiano, dunque, non può conoscere della regolarità degli atti di esecuzione di un sequestro compiuti dall'autorità giudiziaria o di polizia giudiziaria straniera, giacché l'attività investigativa è eseguita secondo la legislazione dello Stato straniero e a maggior ragione ciò vale ove l'originaria attività investigativa non sia compiuta su richiesta dell'autorità giudiziaria italiana, ma sia stata eseguita, nell'ambito di altro procedimento instaurato nello Stato estero, su iniziativa di quell'autorità giudiziaria i cui esiti sono stati trasmessi, come dati definiti freddi, siccome acquisiti in epoca antecedente alla richiesta di O.I.E.

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

L'Autorità francese in tale quadro si è resa garante, in assenza di specifiche deduzioni di segno diverso, del rispetto delle procedure dello Stato di esecuzione, risultando inoltre dal verbale di trasmissione in data 22 ottobre 2021, le modalità di conservazione e di *download* dei dati informatici su apposito CD a supporto delle conversazioni estratte, cui si è apposto un sigillo. Si tratta, con ogni evidenza, di decisivi e riscontrabili riferimenti attestanti che la competente Autorità dello Stato di esecuzione ha assolto alla funzione di assicurare il trasferimento di dati disponibili, la cui concreta attendibilità risulta dall'insieme delle informazioni acquisite.

Le modalità di estrapolazione sono state specificamente segnalate, fermo restando che nel caso di specie veniva in rilievo, come già sottolineato, l'acquisizione di un dato staticamente presente, riconducibile al *genus* dei documenti, comunque garantito nella sua concreta attendibilità dalla procedura seguita. Né può condurre a diverse conclusioni il generico riferimento fatto dal Tribunale alla circostanza che la rete Sky ECC fosse stata «violata»: esso deve essere necessariamente inteso in rapporto al tipo d'indagini già svolte, necessariamente impicanti, in relazione alla natura dei dati di cui si discute, il superamento dell'ostacolo rappresentato dalle chiavi crittografate.

A fronte di ciò, mentre non è stato prospettato alcun profilo rilevante in merito al rispetto in genere dei diritti fondamentali e del principio di proporzione, si rileva

che le facoltà difensive devono essere correlate alla possibilità di stabilire un diretto confronto con i dati acquisiti, di cui ben può essere contestata sulla base di deduzioni specifiche l'attendibilità e l'effettiva rispondenza a comunicazioni reali, in relazione al codice IMEI preso in considerazione, nonché la riconducibilità di quei dati all'indagato taluno, fermo restando che deve tenersi conto della garanzia riveniente dall'Autorità delegata e che devono inoltre considerarsi tutti gli elementi attestati dalle informative di polizia giudiziaria in merito al rispetto della catena di custodia

1.6. E' ancora il caso di precisare come l'acquisizione delle *chat* sia perfettamente compatibile con il diritto interno, ivi compresa la sopravvenuta disciplina dello Stato italiano in materia di acquisizione di tabulati, introdotta con il d.l. 30 settembre 2021 n. 132 convertito, con modificazioni, dalla legge 23 novembre 2021 n. 178.

Come si legge nel preambolo di tale decreto, l'intervento è stato motivato dalla necessità e urgenza di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale nel rispetto dei principi enunciati dalla Grande sezione della Corte di giustizia dell'Unione europea nella sentenza del 2 marzo 2021, causa C-746/18, e in particolare di circoscrivere le attività di acquisizione ai procedimenti penali aventi ad oggetto forme gravi di criminalità e di garantire che dette attività siano soggette al controllo di un'autorità giurisdizionale. La portata maggiormente innovativa della nuova disciplina, dopo la limitazione dei reati per cui tale attività investigativa è ammissibile, è stata quella di aver attribuito al giudice e non più al pubblico ministero il potere di disporre l'acquisizione dei tabulati sicché nel novellato art. 132 d.lgs. 30 giugno 2003, n. 196, l'acquisizione è prevista con decreto motivato del giudice su richiesta del pubblico ministero.

Nel caso che ci occupa – ribadito che ciò che è stato acquisito rientra nel novero dei documenti informatici e non "dati esteriori" (il riferimento è ai tabulati, dei quali le Sezioni Unite n. 21 del 13/07/1998, Gallieri, Rv. 211196 - 01, hanno offerto una utile definizione precisando che «essi costituiscono la documentazione in forma intellegibile del flusso informatico relativo ai dati esterni al contenuto delle conversazioni; stampa che fa parte peraltro, secondo la tecnica informatica, del "movimento" dei dati gestito dall'ente concessionario del servizio, nell'ambito del flusso costituito appunto dall'ingresso-elaborazione-registrazione e stampa») – in ogni caso la già evidenziata circostanza che la complessiva attività di acquisizione si è svolta sotto la direzione del giudice francese (come attestato dal provvedimento del Vice-président chargé de l'instruction di trasmissione e autorizzazione alla loro utilizzazione) pone al riparo da qualsiasi censura in punto di legittima modalità di acquisizione dei dati esterni relativi alle comunicazioni.

1.7. Deve, inoltre, essere chiarito che la situazione delineata non corrisponde interamente a quella esaminata in altra recente pronuncia della Corte di cassazione (Sez. 4, n. 32915 del 15/07/2022, Lori, non mass.).

Diversamente dal caso che ci occupa, in quella occasione la difesa aveva svolto una specifica richiesta al Pubblico Ministero di messa a disposizione della «documentazione (comprensiva dei file) consegnata da Europol nel mese di marzo 2021, a seguito dell'accesso ai server di Sky ECC, con indicazione delle modalità di acquisizione da parte della stessa Europol dei dati in oggetto dai *server*, con annessi verbali, nonché i verbali delle attività compiute dagli investigatori italiani per fini di polizia di cui alla dichiarata analisi preliminare»; richiesta che era stata respinta con la motivazione che si trattava di atti estranei al fascicolo processuale, trattandosi di «scambi informativi tra forze di polizia di paesi diversi che, in quanto tali non sono processualmente utilizzabili». La necessità di acquisire tale documentazione nella citata sentenza era stata posta dalla Corte alla base di una più ampia valorizzazione del contraddittorio.

Nel caso qui in esame, nessuna richiesta di tale genere è stata prospettata dalla difesa, fermo restando, ad avviso del Collegio, quanto invece all'utilizzabilità degli atti trasmessi a seguito di attività di cooperazione internazionale (rogatoria, O.I.E.), che la stessa non è condizionata a un accertamento da parte del giudice italiano inerente la regolarità delle modalità di acquisizione esperite dall'autorità straniera, ribadendosi il pieno vigore della presunzione della regolarità dell'attività svolta, spettando al giudice straniero a verificare la correttezza della procedura e la competenza a risolvere qualsiasi questione in ordine ad eventuali irregolarità lamentate.

2. Sono, al contrario, fondati il secondo e il terzo motivo di ricorso.

A fronte della richiesta della difesa di verificare la concreta sussistenza della circostanza aggravante della premeditazione, il Tribunale ha ritenuto di omettere qualsiasi valutazione sul punto, evidenziando una carenza d'interesse, per non incidere l'eventuale esclusione di tale aggravante sul punto dei termini di custodia cautelare.

Tale motivazione si pone in contrasto con il principio di diritto, che qui si condivide e ribadisce, secondo cui «In tema di impugnazioni avverso misure cautelari personali, vi è carenza di interesse sia al riesame sia al ricorso per cassazione quando con essi l'indagato tenda ad ottenere l'esclusione di una circostanza aggravante, salvo che da tale esclusione derivi, per lui, una concreta utilità» (Sez. 6 n. 50980 del 21/11/2013, Fabricino, Rv. 258502 - 01); detto principio è stato più volte affermato, relativamente al ricorso per cassazione (Sez. 3, n. 20891 del 18/06/2020, Piccirillo, Rv. 279508 - 01; Sez. 6, n. 5213 del

11/12/2018, dep. 2019, Fucito, Rv. 275028 - 01; Sez. 6, n. 7203 del 08/02/2013, Vuocolo, Rv. 254507 - 01).

Si deve, sul punto, rilevare che la richiesta di riesame, prima, e il ricorso per cassazione, poi, sono stati articolati, non al solo fine di contestare la configurabilità o meno della cennata aggravante, bensi anche in punto di gravità del quadro indiziario e di verifica delle esigenze cautelari, sicché non si profila la ritenuta carenza dell'interesse ad impugnare.

In questa sede, la deduzione in punto di qualificazione giuridica risulta, invero, rivolta a rimuovere l'effettivo pregiudizio che la parte asserisce di aver subito con il provvedimento impugnato. Secondo i principi generali del processo penale, l'interesse all'impugnazione va inteso come pretesa all'eliminazione della lesione attuale di un diritto o di altra situazione soggettiva dell'impugnante tutelata dalla legge non già quale pretesa all'affermazione di un astratto principio giuridico o all'esattezza teorica della decisione, che non realizzano il vantaggio pratico cui deve tendere ogni impugnazione. In particolare, sussiste l'interesse dell'indagato a ricorrere per cassazione avverso l'ordinanza *de libertate* che abbia ritenuto sussistente una circostanza aggravante a effetto speciale, sempre che da questa conseguano immediati riflessi sull'*an* o sul *quomodo* della legittimità della misura.

Nel caso di specie, la definizione della questione giuridica inerente alla configurabilità dell'aggravante in senso favorevole all'impugnante, pur non incidendo sul calcolo del termine di durata massima della custodia cautelare, in ragione del limite edittale massimo della pena detentiva previsto per l'ipotesi base del reato contestato, avrebbe potuto e potrebbe riverberarsi sulla valutazione del fatto concreto e sulla presunzione di adeguatezza della misura cautelare di maggior rigore, tenuto conto che le determinazioni dei giudici *a quibus* hanno avuto come presupposto la valutazione globale della obiettiva gravità della condotte di tentato omicidio premeditato.

3. Non essendo completamente definita, a ragione dell'accoglimento dei motivi in punto di premeditazione, la struttura della gravità del fatto, il quarto motivo di ricorso, che involge il consequenziale e collegato profilo delle esigenze cautelari, deve ritenersi assorbito.

4. L'ordinanza impugnata deve essere, dunque, annullata limitatamente alla declaratoria d'inammissibilità della richiesta di riesame sull'aggravante della premeditazione, con rinvio per nuovo giudizio sul punto e sulle statuizioni consequenziali al Tribunale di Roma, competente ex art. 309 cod. proc. pen.

La cancelleria curerà l'adempimento di cui all'art. 94, comma 1-ter, disp. att. cod. proc. pen.



**P.Q.M.**

Annulla l'ordinanza impugnata, limitatamente alla declaratoria di inammissibilità della richiesta di riesame sull'aggravante della premeditazione, con rinvio per nuovo giudizio sul punto e sulle statuizioni consequenziali al tribunale di Roma, competente ex art. 309 cod. proc. pen.

Rigetta il ricorso nel resto.

Manda alla cancelleria per gli adempimenti di cui all'art. 94, comma 1-ter, disp. att. cod. proc. pen.

Così deciso il 13 ottobre 2022

Il Consigliere estensore

Il Presidente