GIURISPRUDENZA PENALE

L'acquisizione delle comunicazioni criptate tramite Ordine Europeo di Indagine: la giurisprudenza delle Sezioni Unite tra diritti fondamentali e procedura penale.

di ***Caterina Fatta*** e ***Emanuele Dodero***

CASSAZIONE PENALE, SEZIONI UNITE, 14 GIUGNO 2024, N. 23755 - 23756
PRESIDENTE CASSANO, RELATORE CORBO

Sommario: 1. I casi oggetto delle pronunce n. 23755 e 23756 del 2024. - **2.** I precedenti giurisprudenziali **- 2.1** L'orientamento estensivo. **– 2.2** L'orientamento restrittivo. **- 2.3**. L'orientamento intermedio. **- 3.** La decisione delle Sezioni Unite: la normativa applicabile e l'utilizzabilità di quanto acquisto. **- 3.1** I principi di diritto espressi dalla Suprema Corte. **- 3.2** La normativa applicabile in materia di acquisizione tramite OEI e il controllo del Giudice endogeno. **- 3.3** L'utilizzabilità di quanto acquisito. Il vaglio del Giudice. - **4.** Le Garanzie difensive alla luce dei principi di diritto espressi dalle Sezioni Unite. La differenza procedurale rispetto al Diritto interno. Criticità.

1. I casi oggetto delle pronunce n. 23755 e 23756 del 2024

Il 14 giugno 2024, sono state depositate le motivazioni delle sentenze n. 23755 e 23756 con le quali le Sezioni Unite hanno statuito i principi di diritto che presiedono all'acquisizione, tramite Ordine Europeo di Indagine (in seguito anche "**OEI**"), delle comunicazioni intercorse mediante messaggistica criptata sulla piattaforma *Sky-Ecc*.

Sebbene si tratti di concetti sempre più comuni nella prassi giudiziaria, pare utile ricordare brevemente cosa si intenda precisamente per "criptofonini" e cosa sia la piattaforma *Sky-Ecc*.

Con il termine criptofonini, si è soliti riferirsi a determinati telefoni/cellulari/*smartphone*, modificati, sia a livello *hardware* che *software*, in modo da disabilitare qualsiasi impostazione o applicazione che ne renda agevole l'intercettazione e la localizzazione, quali ad esempio il sistema di localizzazione GPS, il *Bluetooth* e la fotocamera.

I criptofonini comunicano solo attraverso un ambiente protetto, nel senso che tutte le comunicazioni, sia di messagistica che di chiamata, vengono

crittografate[1] grazie ad apposite applicazioni installate sui dispositivi, quali la nota *Sky-Ecc*, che non permettono di intercettarle, né ne consentono il salvataggio automatico su un *server* pubblico, in quanto i *backup* delle conversazioni criptate vengono archiviati su un apposito *server* accessibile solo alla società che fornisce il servizio.
Si tratta, dunque, di sistemi che dovrebbero fungere da schermo totale del criptofonino nei confronti dei terzi, impedendone l'accesso e la captazione dei dati. Quantomeno, così è stato fino al 2021, quando le forze di polizia mitteleuropee hanno decifrato la piattaforma *Sky-Ecc* e sono entrate in possesso di numerose conversazioni aventi ad oggetto attività illecite.
È stata proprio la disponibilità di queste conversazioni da parte delle menzionate Autorità ad indurre, comprensibilmente, l'Autorità Giudiziaria italiana a chiederne l'acquisizione mediante OEI, dando così origine ai casi oggetto delle sentenze in commento.
Entrambi i casi esaminati dalle Sezioni Unite concernevano, infatti, la trasmissione delle comunicazioni presenti nei *server* della piattaforma *Sky-Ecc* di cui l'Autorità giudiziaria francese era entrata in possesso tramite intercettazione delle comunicazioni criptate, acquisizione dei relativi tabulati, nonché in esecuzione di perquisizioni e sequestri ed acquisizione dei dati conservati nei *server* della società[2].
A fronte di tale acquisizione, le difese degli imputati avevano sollevato molteplici questioni relative all'utilizzabilità di tali dati, poi confluite nei ricorsi esaminati dalle Sezioni Unite.
Il punto di partenza di tutte le doglianze esaminate dalla Suprema Corte era la necessità di definire, alla stregua delle norme procedurali italiane, gli elementi probatori acquisiti dall'Autorità Giudiziaria francese, così da poterne definire il conseguente regime di utilizzabilità processuale.
In questo senso, le difese avevano ritenuto che parte del materiale investigativo trasmesso alla Procura italiana fosse assoggettabile alla disciplina dell'art. 234 *bis* c.p.p., essendo stati acquisiti dall'Autorità Giudiziaria francese dei dati informatici conservati all'estero dalla Società *Sky Global*, mentre l'altra parte dovesse essere assoggettata alla disciplina delle intercettazioni ai sensi degli artt. 266 e ss c.p.p., trattandosi degli elementi probatori frutto delle attività di intercettazione svolte dall'Autorità francese mediante captatore informatico.

[1] Quindi oscurate o comunque rese inaccessibili a persone diverse dai destinatari, grazie all'utilizzo di algoritmi, anche con cifratura a più livelli, quali crittografia Diffie-Hellman, a curve ellittiche (ECC), PGP (Pretty Good Privacy) per le email, OTR (Off-the-Record Messaging) per la chat e ZRTP per le chiamate.
[2] Sul tema della c.d. *data retention*, intesa come consultazione dei dati conservati dal gestore di rete o dal provider, CUOMO, *La prova digitale*, in Prova scientifica e processo penale, a cura di Canzio, Luparia, Milano, 2022, 663 ss.

Per ognuna delle due categorie di elementi probatori trasmessi in esecuzione dell'OEI erano state sollevate diverse questioni di inutilizzabilità.
Con riferimento all'acquisizione dati conservati presso i server di Sky Global, dal momento che l'art. 234 *bis* c.p.p. richiede il previo consenso del legittimo titolare dei dati informatici custoditi all'estero, le difese avevano sostenuto che non fosse stato correttamente individuato il legittimo titolare.
Ed infatti, l'Autorità giudiziaria italiana aveva operato come se l'Autorità giudiziaria francese il *legittimo titolare* di tali dati, sennonché, secondo la Convenzione di Budapest in materia di *cybercrime* del 23 novembre 2001, il *legittimo titolare* dei dati è il proprietario dell'*accoun*t, ossia – nel caso concreto – la Sky Global, e non l'autorità giudiziaria che li abbia legittimamente acquisiti (cfr. art. 32, lett. b della Convenzione[3]).
Pertanto, non essendo l'Autorità francese il legittimo titolare dei dati informatici, quanto acquisto avrebbe dovuto essere considerato inutilizzabile nel procedimento italiano.
Ma questa non sarebbe stata l'unica ragione che avrebbe impedito l'utilizzabilità di tali dati. Ed infatti, l'acquisizione di dati informatici conservati all'estero dalla Società *Sky Global* sarebbe avvenuta anche in violazione della disciplina di cui all'art. 132 del Dlgs. n. 196/2003[4] (c.d. Codice della Privacy), in quanto l'OEI era stato inoltrato in assenza della previa autorizzazione all'acquisizione dei dati da

[3] Secondo la disposizione citata dal ricorrente, ovvero l'art. 32, rubricata Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili, "*Una Parte può, senza l'autorizzazione di un'altra Parte:*
a. accedere ai dati informatici immagazzinati disponibili al pubblico (fonti aperte), senza avere riguardo al luogo geografico in cui si trovano tali dati; o
b. accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati situati in un altro Stato, se la Parte ottiene il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati allo Stato attraverso tale sistema informatico".

[4] L'art. 132 del Dlgs. 196 del 30 giugno 2003, rubricato: Conservazione di dati di traffico per altre finalità, stabilisce, per quanto qui rileva, che: *"(…) se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private. 3-bis. Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato (…)".*

parte del Giudice[5]. Del resto, in linea con quanto statuito della giurisprudenza dalla Corte di Giustizia UE[6], l'accesso ai dati relativi al traffico telefonico/telematico ed all'oggetto delle comunicazioni è consentito solo in caso di un preventivo controllo del giudice non essendo sufficiente il solo provvedimento del Pubblico Ministero[7].

Più in generale, poi, l'impossibilità per la difesa di conoscere le modalità di acquisizione e decriptazione delle comunicazioni presenti sul sistema *Sky-Ecc* avrebbe integrato una nullità di ordine generale *ex* art. 178 c.p.p. con violazione del diritto di difesa.

Con riguardo all'acquisizione, in esecuzione dell'OEI, degli elementi probatori frutto delle attività di intercettazione svolte dall'Autorità francese mediante captatore informatico, le difese avevano invece dedotto l'illegittimità dell'acquisizione di tali elementi ai sensi dell'art. 234 *bis* c.p.p., dal momento che avrebbe dovuto invece essere applicata la disciplina propria dell'acquisizione delle risultanze di attività di intercettazione, ovvero quella disciplinata dagli art. 266 e ss c.p.p..

Si deduceva, altresì, l'inutilizzabilità delle comunicazioni intercorse sul sistema *Sky-Ecc*, per violazione dell'art. 6, paragrafo 1, lett. a) e lett. b), della Direttiva

---

[5] In tema di *data retention* e tutela del diritto alla *privacy* a livello sovranazionale e sui principi di diritto espressi sulla tematica dalla Corte di Giustizia dell'Unione Europea cfr. LANDOLFINI, *data retention tra continui sviluppi e nodi irrisolti,* in la Legislazione Penale, 2024.

[6] In particolare, il ricorrente evidenzia la sentenza Corte di giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C- 746/18.

[7] Il ricorrente, pertanto, ha richiesto alla Corte di Cassazione, oltre all'annullamento dell'ordinanza impugnata, di formulare alla Corte di Giustizia dell'Unione Europea i seguenti quesiti: "*a) se l'art. 6, paragrafo 1, della Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale, letto alla luce degli artt. 7,8 e 11 nonché 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea, debba essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'acquisizione di dati elettronici relativi al traffico, all'ubicazione o al contenuto di comunicazioni già in possesso dell'autorità di esecuzione, o comunque contenuti in basi di dati di polizia o delle autorità giudiziarie, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica;*

b) se l'art. 6, paragrafo 1, della Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale, letto alla luce degli artt. 7,8 e 11 nonché 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea, debba essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'acquisizione di dati elettronici relativi al traffico, all'ubicazione o al contenuto di comunicazioni già in possesso dell'autorità di esecuzione, o comunque contenuti in basi di dati di polizia o delle autorità giudiziarie, senza che tale accesso sia preventivamente autorizzato da un giudice o da altra entità incaricata"

20114/41/UE[8], trattandosi di atti che non avrebbero potuto essere compiuti in Italia considerata l'indiscriminata e generalizzata intercettazione di tutte le comunicazioni presenti sulla piattaforma *Sky-Ecc*.
Ebbene, alla luce di quanto dedotto con i ricorsi, la Terza sezione penale della Corte di cassazione con ordinanza del 3 novembre 2023 e la Sesta Sezione con ordinanza del 15 gennaio 2024 hanno ritenuto che sulle questioni sollevate dalle difese degli imputati vi fosse un contrasto giurisprudenziale che avrebbe dovuto essere risolto dalle Sezioni Unite.

2. I precedenti giurisprudenziali

Prima di esaminare la soluzione offerta dalle Sezioni Unite in ordine alle questioni sollevate dalle difese, pare utile richiamare brevemente i diversi orientamenti giurisprudenziali formatisi in relazione alla corretta qualificazione giuridica (e conseguente disciplina applicabile) degli elementi probatori frutto dell'attività di indagine estera.
Come noto, emerge che la giurisprudenza, nel tempo, abbia intrapreso un percorso evolutivo, muovendosi gradualmente da un approccio che favoriva principalmente la rapidità e l'efficacia dell'indagine a un modello più equilibrato che tenga conto delle implicazioni in termini di diritti fondamentali, come deducibile dall'interpretazioni giurisprudenziali più recenti della normativa.
Dovendo, comunque, rilevare che, al di là dei tre diversi orientamenti che verranno esaminati, un approdo comune riguarda la classificazione dell'acquisizione di comunicazioni in corso di esecuzione: qualora l'OEI abbia ad oggetto l'acquisizione di attività captativa afferente a comunicazioni in transito da un dispositivo ad un altro e non di dati "statici", già in possesso dello Stato di esecuzione, devono trovare applicazione le disposizioni di cui agli artt.266 e ss c.p.p. e, dunque, i presupposti per cui è consentita l'attività di intercettazione, nonché le garanzie a presidio dell'utilizzabilità/inutilizzabilità dei risultati.
Del resto, quanto appena rilevato trova corrispondenza nella normativa europea, laddove l'art. 6 par. 1, lett. b. Direttiva 2014/41/UE prevede che

[8] L' Articolo 6, rubricato Condizioni di emissione e trasmissione di un OEI, statuisce che: "*1. L'autorità di emissione può emettere un OEI solamente quando ritiene soddisfatte le seguenti condizioni:*
a) l'emissione dell'OEI è necessaria e proporzionata ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata;
b) l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo.
2. Le condizioni di cui al paragrafo 1 sono valutate dall'autorità di emissione per ogni caso.
3. Se ha motivo di ritenere che le condizioni di cui al paragrafo 1 non siano state rispettate, l'autorità di esecuzione può consultare l'autorità di emissione in merito all'importanza di eseguire l'OEI. Dopo tale consultazione, l'autorità di emissione può decidere di ritirare l'OEI".

l'Autorità dello Stato di emissione dell'OEI valuti che: "*l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alla stesse condizioni in un caso interno analogo*".
Diversamente, qualora oggetto dell'acquisizione siano dati informatici "statici", ovvero trascrizioni di intercettazioni già disposte dall'Autorità estera in un autonomo procedimento, come vedremo, l'interpretazione giurisprudenziale non appare univoca.

2.1 L'orientamento estensivo.
Secondo l'orientamento più risalente, quando l'autorità italiana emette un OEI avente ad oggetto la richiesta rivolta ad un'autorità straniera di acquisizione di *chat* di gruppo scambiate con sistema criptato, dovrebbe trovare applicazione la disposizione di cui all'art. 234 *bis* c.p.p. "*Acquisizione di documenti e dati informatici*"[9].
In particolare, sul presupposto che quanto oggetto di acquisizione tramite OEI consiste in un mero dato informatico, tale orientamento afferma che, non venendo in rilievo un'attività intercettiva "in atto" poiché già stata svolta dall'Autorità giudiziaria dello Stato di esecuzione, i risultati delle intercettazioni effettuate siano classificabili quale documentazione.
Vediamo le ragioni di tali asserzioni.
Le ultime pronunce in linea con tale orientamento[10], mantenendo la distinzione tra i c.d. dati statici o freddi e attività intercettiva pura, comune a tutti gli orientamenti, hanno chiarito alcuni nodi focali e principi espressi nel tempo dalla giurisprudenza conforme a tale interpretazione.
In particolare, è stato precisato che nella nozione di "*legittimo titolare*" di cui all'art. 234 *bis* c.p.p., rientra anche la persona giuridica che dispone liberamente

[9] Per una disamina più approfondita dell'istituto cfr. P. TONINI e C. CONTI, *Manuale di Procedura Penale*, venticinquesima edizione, Giuffrè pp. 390 e ss. La dottrina appena menzionata annovera la disposizione in esame quale nuovo mezzo di ricerca della prova e non quale mezzo di prova. Affermando che per l'acquisizione transfrontaliera dei documenti informatici è necessario adottare le cautele previste con riferimento ai *nuovi mezzi di ricerca della prova informatica*. Secondo gli Autori, nel dettaglio, tale acquisizione potrà compiersi solo ove lo Stato sul cui territorio sono allocati i *server* abbia aderito alla convenzione di Budapest sul *cybercrime*. Questo poiché unva volta avvenuta la ratifica della stessa e, di conseguenza, in applicazione del principio di reciprocità ivi contenuto non sarà necessario richiedere il consenso all'acquisizione dello Stato. Diversamente, qualora i server siano allocati sul territorio di uno Stato che non abbia ratificato la predetta Convenzione, non potrà essere acquisito alcun dato o documentazione informatica per difetto del necessario consenso, che non sarebbe comunque surrogabile da parte di un privato.
[10] Cfr. sul punto *ex multis*: Cass. Pen. Sez. I, Sent. del 13 gennaio 2023 n. 19082; Cass. Pen. Sez. I, Sent. del 13 ottobre 2022 n. 6363; Cass. Pen. Sez. I, Sent. del 13 ottobre 2022 n. 6364; Cass. Pen. Sez. I, Sent. del 1 luglio 2022 n. 34059.

dei dati e documenti informatici in forza di un legittimo titolo, ritenendo tali anche la polizia giudiziaria o l'Autorità giudiziaria dello Stato estero di esecuzione dell'O.E.I.[11].

Pertanto, non è necessario che la Società titolare della piattaforma, quali ad esempio *Sky-ecc*, esprima il proprio consenso all'acquisizione da parte dell'Autorità Giudiziaria, essendo già quest'ultima, secondo tale orientamento, il legittimo titolare di cui il consenso costituisce prerequisito all'attività di indagine.

Inoltre, secondo tale orientamento[12] è esclusa altresì la necessità che l'Autorità Giudiziaria richieda una preventiva autorizzazione del Giudice prima di procedere con l'acquisizione tramite OEI. Ciò sarebbe una diretta conseguenza dell'applicazione della disciplina di cui all'art. 234 *bis* c.p.p.

Ma non solo.

l'indirizzo in esame esclude che per l'acquisizione di dati crittografati l'OEI debba essere preceduto dall'autorizzazione del giudice nazionale anche quale conseguenza del considerare l'OEI come uno strumento volto a facilitare l'acquisizione delle prove in modo rapido e senza eccessivi formalismi tra gli Stati membri dell'Unione Europea e coerentemente con il principio del mutuo riconoscimento delle decisioni giudiziarie.

Ed infatti, in coerenza con l'art. 9 della Direttiva 2014/41/UE, i sostenitori del presente orientamento ritengono che lo Stato di esecuzione debba rispettare l'ordine investigativo a meno che non vi siano gravi ragioni di rifiuto, come la violazione di diritti fondamentali.

Infine, è opportuno rilevare come, più sentenze di legittimità[13], afferenti all'orientamento giurisprudenziale in analisi, hanno individuato alcune condizioni che devono necessariamente sussistere affinché il procedimento di acquisizione possa considerarsi legittimo.

Segnatamente, l'OEI deve avere ad oggetto solo prove acquisibili nello Stato di emissione, conformemente alla normativa in esso vigente, deve essere eseguito in conformità delle procedure legislative vigenti nello Stato di esecuzione e, infine, l'attività richiesta deve presumersi eseguita nel rispetto dei diritti

---

[11] Cfr. Cass. Pen. Sez. I, Sent. del 13 ottobre 2022 n. 6363, nella quale viene statuito che il legittimo titolare di cui all'art. 234 *bis* c.p.p. è *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*".

[12] In particolare, cfr. Cass. Pen. Sez. 4 del 11 maggio 2023 n. 27775.

[13] Cfr. Cass. Pen. Sez. I, Sent. del 13 gennaio 2023 n. 19082; Cass. Pen. Sez. I, Sent. del 13 ottobre 2022 n. 6363; Cass. Pen. Sez. I, Sent. del 13 ottobre 2022 n. 6364.

fondamentali, salvo prova contraria, il cui onere comunque grava esclusivamente sulla parte che formula l'eccezione[14].

2.2 L'orientamento restrittivo

Un secondo orientamento della giurisprudenza di legittimità, più restrittivo, rileva che l'acquisizione di *chat* criptate tramite l'emissione di un OEI, rientrerebbe nella sfera applicativa di cui all'art. 254 *bis* c.p.p. in tema di "*Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni*"[15].

Pertanto, l'acquisizione dei dati tramite OEI potrebbe avvenire solo previo controllo giurisdizionale, essendo necessario effettuare un bilanciamento tra l'efficacia delle indagini e la tutela della riservatezza delle comunicazioni[16] e dei diritti garantiti dall'art. 8 della CEDU[17].

Le pronunce in questione[18] hanno anche espresso preoccupazioni sul fatto che il ricorso all'OEI senza rispettare la disciplina di cui all' art. 254 *bis* c.p.p. ed in assenza di una chiara regolamentazione, nonché di un controllo preventivo da parte delle Autorità giurisdizionali nazionali, potrebbe risolversi sia in violazioni del diritto di difesa sia in acquisizioni di prove in contrasto con i principi di legalità e proporzionalità.

Ed infatti, contrariamente all'orientamento "estensivo" di cui al paragrafo precedente, si è sostenuto che, nei casi di specie, non troverebbe applicazione l'art. 234 *bis* c.p.p., poiché l'Autorità giudiziaria straniera non potrebbe definirsi il legittimo titolare di cui è richiesto il consenso *ex* art. 234 *bis* c.p.p., essendo mero detentore dei dati acquisiti.

Per converso, secondo i sostenitori di tale tesi legittimo titolare è esclusivamente chi trasmette o chi riceve i messaggi e le comunicazioni o nella la società che gestisce la piattaforma.

---

[14] Cfr. *ex multis*: Cass. Pen. Sez. 3 del 19 ottobre 2023 n. 47201; Cass. Pen. Sez. 4 del 30 maggio 2023 n. 37503; Cass. Pen. Sez. 4 del 5 aprile 2023 n. 16347.

[15] cfr. P. TONINI e C. CONTI, *op. cit.* p 418.

[16] Sulla tematica del bilanciamento e in generale del principio di proporzionalità cfr. F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in DPenCont 2018, 176 ss.

[17]Art. 8 CEDU: Diritto al rispetto della vita privata e familiare: 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

[18] Cfr. Cass. Pen. Sez. 6 del 26 ottobre 2023 n. 44155; Cass. Pen. Sez. 6 del 26 ottobre 2023 n. 44154.

Inoltre, l'orientamento in esame ritiene che l'art. 234 *bis* c.p.p. possa trovare applicazione esclusivamente con riferimento alla trasmissione di documentazioni o dati formatisi "fuori" da un procedimento penale, sia esso nazionale o estero, escludendo, pertanto, la possibilità di acquisirli se i messaggi e le comunicazioni criptate siano avvenuti mentre era già in corso un'investigazione.

Infine, la corretta interpretazione del dettato normativo di cui all'art. 43 comma IV del D.lgs. n. 108 del 2017[19], anche nel rispetto dei limiti fissati dalla Corte di Giustizia UE in tema di acquisizione dei dati esterni[20], comporterebbe che l'attività di decrittazione delle comunicazioni intercettate, se richiesta dall'Autorità giudiziaria italiana a quella estera, dovrebbe essere preventivamente autorizzata dal Giudice italiano, non essendo sufficiente il solo provvedimento del Pubblico Ministero per l'acquisizione di documenti e dati informatici inerenti a qualsiasi forma di comunicazione, compresa, dunque, la messaggistica criptata.

Dunque, senza la preventiva autorizzazione del Giudice l'OEI sarebbe illegittimo[21] e ciò comporterebbe due conseguenze: se l'OEI ha determinato lo svolgimento di attività di indagine intercettiva, quanto acquisito sarebbe inutilizzabile; se quanto richiesto con OEI è afferente all'acquisizione di quanto già in possesso dell'Autorità giudiziaria dello Stato di esecuzione, la verifica sull'ammissibilità della prova potrà essere posta innanzi al Giudice italiano.

Ed infatti, a sostegno di questo orientamento vi è quanto statuito dalla stessa Direttiva sull'OEI 2014/41/UE, la quale richiede, oltre all'autorizzazione del Giudice dello Stato di esecuzione, il controllo sull'ammissibilità e sull'utilizzabilità della prova acquisita da parte del Giudice dello Stato di emissione.

Del resto, a conferma di quanto appena evidenziato e in linea con i principi già espressi in tema di rogatorie, quanto acquisito con l'OEI potrà essere utilizzato in Italia solo se non in contrasto con i principi fondamentali dell'ordinamento, anche se ottenuto applicando la legge dello Stato di esecuzione[22].

---

[19] Il comma IV dell'art. 43 statuisce che: "*la richiesta può avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate*". In generale, sulla relativamente alla disciplina del D.lgs. del 21 giungo 2017 n. 108, si vedano DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017*, in Dir. Pen. Cont., 7-8, 2017, 208 ss. e MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in Dir. Pen. Proc., 2, 2018, 158 ss..

[20] Cfr. Corte di Giustizia, Grande Sezione, 2 marzo 2021, H.K./Prokuratur causa C-746/18.

[21] Come nel caso di specie, avendo la Corte statuito come l'acquisizione di documenti e dati informatici all'estero deve sempre essere autorizzata dal Giudice.

[22] Il rispetto dei diritti fondamentali in caso di acquisizione di messaggi crittografati è richiesto anche dalla Corte EDU, la quale considera leso il diritto di difesa quando non viene consentita la verifica del contenuto e dell'integrità di quanto acquisito poiché tale

2.3 Il terzo orientamento giurisprudenziale. L'orientamento intermedio.

Infine, da ultimo, nella giurisprudenza di legittimità si registra un terzo orientamento[23], secondo il quale la corrispondenza acquisita da uno Stato estero mediante l'emissione di un OEI, anche se informatica e relativa ad elementi già raccolti nel procedimento penale pendente innanzi all'Autorità Giudiziaria dello Stato di esecuzione, costituisce una mera prova documentale a norma dell'art. 234 c.p.p.

La Corte di cassazione sottolinea che nell'acquisizione delle comunicazioni personali conservate su dispositivi elettronici, trattandosi di prove documentali, devono trovare applicazione le disposizioni in materia di perquisizione e sequestro, le quali non richiedono l'intervento del Giudice, ma solo l'iniziativa Pubblico Ministero.

Inoltre, in ragione della classificazione di prova documentale delle comunicazioni già in possesso dello Stato di esecuzione, si ritiene inapplicabile la disciplina dell'art. 234 *bis* c.p.p. (anche qui difformemente dal primo orientamento) con la conseguenza che non è richiesto il consenso del legittimo titolare poiché normativamente non annoverato quale presupposto per l'acquisizione.

In particolare, si sostiene che l'art. 234 *bis* c.p.p. si riferisce solo a dati presenti in rete ovvero a materiale, non disponibile al pubblico, che può essere acquisito esclusivamente con il consenso del legittimo titolare.

Diversamente, quanto trasmesso dell'Autorità Giudiziaria straniera avrebbe potuto essere acquisito, a livello nazionale, mediante un mero provvedimento di sequestro probatorio della corrispondenza del Pubblico Ministero, senza richiedere ulteriori garanzie o tutele.

A sostegno dell'inapplicabilità dell'art. 234 *bis* c.p.p., la Corte rileva come l'origine della disposizione in questione sia la Convenzione di Budapest sul *cybercrime*, in particolare l'art. 32, che si riferirebbe esclusivamente all'acquisizione di dati reperibili in rete e non, in generale, ai documenti ottenuti ed acquisiti da altra Autorità.

Pur avvicinandosi al secondo orientamento "restrittivo" (cfr. paragrafo 3.2), tuttavia questo terzo indirizzo sostiene che non ricorra l'obbligo di un preventivo provvedimento autorizzativo del Giudice ai fini dell'acquisizione.

Si rileva, infatti, che tale interpretazione sia conforme con l'art.15 Cost. che, in tema ed a tutela dalla libertà e della segretezza della corrispondenza, richiede esclusivamente il necessario e motivato intervento dell'Autorità giudiziaria,

carenza non consentirebbe all'imputato di preparare un'adeguata difesa a norma dell'art. 6 CEDU. Sul punto cfr. Corte EDU, Gande Camera, 26 settembre 2023, Yuksel Yalcinkaya c. Turchia.

[23] Cfr. Cass. Pen. Sez. 6 del 26 ottobre 2023 n. 4683; Cass. Pen. Sez. 6 del 11 ottobre 2023 n. 48838; Cass. Pen. Sez.6 del 27 settembre 2023 n. 46482.

quale il Pubblico Ministero, ma non alcuna autorizzazione preventiva o postuma del Giudice[24].
Ed infatti, si sottolinea che gli unici presupposti o limiti all'acquisizione dei dati dall'Autorità straniera sono costituiti dal provvedimento del Pubblico Ministero, conformemente alla normativa nazionale in tema di perquisizioni e sequestri, nonché dalla legittimità e conformità delle attività di indagine alla legislazione dello Stato estero, con eventuale provvedimento dell'Autorità giudiziaria, ove la legge lo richieda e dal limite dell'utilizzazione dei dati, così acquisiti, per la tutela della sicurezza pubblica e della prevenzione di gravi reati.
Secondo l'orientamento in esame, se l'OEI può essere considerato come uno strumento efficace per la cooperazione giudiziaria, tuttavia la sua applicazione dovrebbe sempre essere subordinata a una valutazione della proporzionalità e della necessità del provvedimento da parte dell'Autorità Giudiziarie.
Pertanto, essendo anche quanto già acquisito dall'Autorità estera classificabile quale prova documentale, per l'acquisizione sarebbero applicabili l'art. 247 c.p.p., rubricato "*Casi e forme delle perquisizioni*" con particolare riferimento al comma 1 *bis* relativo ai dati informatici[25], l'art. 254 *bis* "*sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni*" e l'art. 352 c.p.p., "*perquisizioni*" ovvero la normativa in tema di perquisizioni e sequestri di prove documentali informatiche.
Ebbene, alla luce dei contrasti giurisprudenziali, delle norme del codice di rito di volta in volta richiamate, nonché dei diversi orientamenti giurisprudenziali appena richiamati, sono state rimesse alle Sezioni Unite, per quanto in questa sede rilevi, le seguenti questioni:
a) *se l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato attraverso un ordine europeo di indagine rivolto ad un'autorità giudiziaria straniera che non abbia eseguito la decrittazione costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234 bis c.p.p. o di documenti ex art. 234 c.p.p. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove*.
b) *se l'acquisizione di cui sopra debba essere oggetto, ai fini dell'utilizzabilità dei relativi dati, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte delle autorità giurisdizionale nazionale*.
c) *se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte da un'autorità giudiziaria straniera su una piattaforma*

[24] Tali considerazioni sono conformi ad una recente pronuncia della Consulta, la n. 170 del 2023, nella quale la Corte ha statuito che i messaggi scambiati tramite *chat* o altre applicazioni debbano essere qualificati quali corrispondenza e, pertanto, debba loro applicarsi la tutela rafforzata, ovvero la riserva di legge e di giurisdizione, annoverata dall'art.15 Cost qualora si procedesse all'acquisizione.
[25] P. TONINI e C. CONTI, *op. cit.* pp. 406 e ss.

informatica criptata integri un'ipotesi disciplinata nell'ordinamento interno dall'art. 270 cod. proc. pen.

3. La decisione delle Sezioni Unite: la normativa applicabile e l'utilizzabilità di quanto acquisto.

3.1 I principi di diritto espressi dalla Suprema Corte

Investita dei quesiti sollevati con la rimessione, le Sezioni Unite, con le sentenze gemelle, rispondono nei seguenti termini[26]:

in merito alla disciplina del codice di rito concretamente applicabile al caso di specie la Suprema Corte ha statuito che

- *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**.*

Ed infine, in merito al tema dell'utilizzabilità il Supremo Consesso ha enunciato che:

- *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 del procedimento nel quale dette risultanze istruttorie vengono acquisite rileva che**, in relazione a esse, **il loro impiego***

[26] Verranno riportati esclusivamente i principi di diritto relativi ai temi trattati nel presente contributo.

***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**.*

3.2 La normativa applicabile in materia di acquisizione tramite OEI e il controllo del Giudice endogeno.

Ebbene, con un tratto di penna, i Giudici della Suprema Corte hanno posto fine ai contrasti giurisprudenziali sorti nel tempo afferenti al tema in esame.

A tal proposito la Corte, in linea con gli orientamenti più recenti, ha statuito che la disciplina di cui all'art. 234 *bis* c.p.p. non sia suscettibile di applicazione nel caso concreto, in quanto avulsa dal tema della circolazione delle prove tra diversi Stati, in ambito di collaborazione giudiziaria.

Secondo la Corte, trattandosi di acquisizioni disposte tramite OEI, devono essere rispettatele garanzie annoverate da questa disciplina e, di conseguenza, non la disciplina alternativa, in tal ipotesi incompatibile, dell'acquisizione dei dati informatici conservati all'estero di cui all'art. 234 *bis* c.p.p., la quale prescinde da qualsivoglia forma di collaborazione con l'Autorità Giudiziaria di uno Stato Estero.

Proprio per tali ragioni, la Corte ha ritenuto che la normativa applicabile fosse quella di cui al combinato disposto degli art. 238 c.p.p., 270 c.p.p. e 78 disp. att. c.p.p., sempre che, a seguito di un accertamento del Giudice italiano sull'attività di indagine espletata dall'Autorità estera non si tratti di "vere e proprie" intercettazioni che implicherebbero l'attuazione della disciplina di cui agli artt. 266 e ss. c.p.p., così come sempre sostenuto dalla Giurisprudenza di legittimità.

Ora, secondo le Sezioni Unite, l'art. 78 disp. att. c.p.p., concepito dal Legislatore avendo riguardo esclusivamente alle rogatorie, annovera un principio di carattere generale ed è pertanto applicabile anche all'OEI conformemente ai principi sovranazionali di equivalenza[27] e proporzionalità[28], sempreché non si tratti di "vera e propria" attività intercettiva.

Ma non solo.

La Corte di cassazione ha stabilito che, a differenza di tutti i pregressi orientamenti, al fine di comprendere quale normativa sia suscettibile di applicazione, ovvero se quella in materia di circolazione della prova o quella delle intercettazioni, è compito del Giudice dello Stato di emissione espletare un accertamento sulla singola attività di indagine i cui risultati sono oggetto di richiesta di acquisizione mediante OEI.

Sarà, dunque, compito del Giudice italiano effettuare un controllo *ex post* che, oltre a verificare la normativa applicabile a seguito di un'indagine sulla natura dell'atto di cui si chiede l'acquisizione, dovrà, altresì, verificare che l'attività

[27] Secondo il quale, l'atto di indagine oggetto di OEI deve essere previsto ed attuato alle stesse condizioni di un caso interno analogo.

[28] Il quale richiede che le compromissioni dei diritti fondamentali, derivanti dall'attività di indagine svolta, siano limitate allo stretto necessario.

investigativa sia stata posta in essere rispettando i diritti fondamentali della persona, senza causarne una loro compromissione o violazione, ciò rispettando anche il *dictum* dei principi sovranazionali[29].

3.3 L'utilizzabilità di quanto acquisito. Il vaglio del Giudice.

Quanto appena riferito ha, non vi è dubbio, notevoli conseguenze in tema di utilizzabilità di quanto acquisito tramite OEI.

Ed infatti, contrariamente ad alcuni degli orientamenti di legittimità sopra indicati, le Sezioni Unite hanno definitivamente cassato la questione afferente alla preventiva autorizzazione del Giudice dello Stato di emissione.

Nel dettaglio, la Corte ha statuito che l'autorizzazione, in nessuno caso, debba sussistere poiché la normativa interna relativa alla circolazione delle prove tra diversi procedimenti non la richiede.

Ma non solo, le sentenze hanno, altresì, consegnato alcune precisazioni in tema di utilizzabilità.

A tal proposito, la Corte ha attribuito, come detto, al Giudice dello Stato di emissione un potere di controllo postumo, afferente sia alla normativa applicabile sia alla legittimità di quanto attutato nello Stato di esecuzione, ovvero alla conformità di tale attività con i principi sovranazionali e con i diritti fondamentali.

Tale controllo sulla legittimità di quanto acquisito e, di conseguenza, il vaglio sull'utilizzabilità, dovrà essere, comunque, accompagnato dall'onere di allegazione proprio della parte che eccepisce la violazione dei diritti fondamentali della persona direttamente coinvolta dall'attività di indagine svolta nello Stato di esecuzione.

Pertanto, pur non essendo previsto un vero e proprio diritto di impugnazione dell'OEI, nonostante la previsione di cui all'art. 14, paragrafo secondo della direttiva 2014/14/UE[30], in capo alla parte che ritiene leso un proprio diritto, ad avviso delle Sezioni Unite, viene comunque garantita la facoltà della stessa di rivolgersi al Giudice dello Stato di emissione, allegando le prove della presunta violazione, attivando il potere di controllo al medesimo attributo.

Sarà dunque del Giudice endogeno l'onere di verificare la conformità e legittimità di quanto acquisito tramite l'attività di indagine estera e la normativa nazionale annoverata dal codice di rito in tema di utilizzabilità.

---

[29] Sul punto, cfr. MANGIARACINA, *L'esecuzione dell'OEI e i margini nazionali di rifiuto, in L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, a cura di Kostoris, Daniele, Torino, 2019, 128.

[30] Art. 14, paragrafo secondo della Direttiva 2014/14/UE: *Le ragioni di merito dell'emissione dell'OEI possono essere impugnate soltanto mediante un'azione introdotta nello Stato di emissione, fatte salve le garanzie dei diritti fondamentali nello Stato di esecuzione.*

4. Le Garanzie difensive alla luce dei principi di diritto espressi dalle Sezioni Unite. La differenza procedurale rispetto al Diritto interno. Criticità.

L'aspetto che, forse, alla luce di quanto statuito dalle Sezioni Unite, può destare qualche preoccupazione agli interpreti è legato, appunto, in generale al tema dell'utilizzabilità.

Nello specifico, le Sezioni Unite hanno statuito che, nel caso di acquisizione di attività intercettiva non statica, la norma interna applicabile è l'art. 270 c.p.p., il quale, come è noto, non richiede alcuna preventiva autorizzazione del giudice ai fini dell'acquisizione di intercettazioni disposte in altro procedimento.

Senonché, in tema di intercettazioni quando viene formulata la richiesta di acquisizione in un procedimento di attività intercettiva disposta in un altro procedimento, che possiamo definire "originario", queste sono state disposte dietro autorizzazione del primo Giudice.

Pertanto, in questi casi, anche se proveniente da un Giudice diverso, un'autorizzazione "preventiva" delle attività di indagini intercettiva da parte dell'organo giudicante, sussiste.

Ecco, tale circostanza non è stata presa in considerazione delle Sezioni Unite, le quali nulla statuiscono in tal senso.

Alla luce di ciò, il rischio è quello di acquisire a livello endogeno delle intercettazioni che siano state disposte nello Stato di esecuzione, in seno al procedimento "originario", senza alcun vaglio del Giudice estero, qualora la normativa interna dello Stato di esecuzione non preveda tale adempimento. Ciò, tra l'altro, in spregio anche al *dictum* della normativa sovranazionale, che richiede la presenza di una norma interna analoga[31].

In tale circostanza, quindi, l'unico mezzo a disposizione della difesa sarebbe quello di richiedere un vaglio di legittimità su quanto acquisito, che potrebbe essere oggetto di una pronuncia di inutilizzabilità solo laddove venga accertata la violazione dei diritti fondamentali della persona o comunque la violazione della normativa sovranazionale.

Eguale critica, può essere sollevata nei confronti dell'acquisizione dei c.d. "dati statici", considerato che in tal caso nemmeno la normativa nazionale, in tema di circolazione delle prove *ex* art. 238 c.p.p., annovera un controllo sull'attività di acquisizione del Pubblico ministero nel procedimento originario.

Ed infatti, pur acquisendo delle comunicazioni private, senza far uso direttamente degli strumenti intercettivi, poiché qualificabili come documentazione e nonostante l'evidente lesione del diritto alla *privacy* della persona, non è richiesto alcun intervento del Giudice, ma solo un provvedimento autonomo del Pubblico Ministero.

[31] Come visto, infatti, il Considerando n. 32 della Direttiva 2014/41/UE, in tema di attività di intercettazione, richiede di verificare che l'atto di indagine possa essere compiuto anche in un caso di specie analogo.

Si può, dunque, affermare che sicuramente la Sezioni Unite abbiamo messo fine ai contrasti giurisprudenziali susseguiti nel tempo in tema di acquisizione delle comunicazioni criptate tramite OEI relativamente alla normativa applicabile, però, allo stesso tempo, le pronunce gemelle non possono dirsi complete in tema di utilizzabilità e del rispetto delle garanzie difensive, ambito in cui continuano e permangono alcuni dubbi interpretativi.
Al tal proposito, è auspicabile che le successive pronunce di merito o legittimità facciano chiarezza e risolvano questi dubbi interpretativi non affrontati dalla Sezioni Unite.