

SCHEDA 11 Dicembre 2023

ORDINE EUROPEO DI INDAGINE PENALE E COMUNICAZIONI CRIPTATE: IL CASO SKY ECC/ENCROCHAT IN ATTESA DELLE SEZIONI UNITE

Marcello Daniele

Cass. sez. III, ord. 3 novembre 2023 (dep. 30 novembre 2023), n. 47798, Pres. Gentili, rel. Noviello

**Contributo redatto nell'ambito del progetto MEIOR (Mould EIO Review), finanziato dal Justice Programme (Just) 2021-2027 dell'Unione Europea, Project ID: 101046446.*

1. Come acquisire le comunicazioni criptate conservate in server stranieri? Si sta parlando molto di *Sky ECC* e di *Encrochat*: due piattaforme online di tipo criptato utilizzate dagli esponenti di alcune associazioni criminali per comunicare in via riservata attraverso *smartphone* appositamente modificati.

Trattandosi di comunicazioni rinvenibili in *server* situati all'estero, in diverse occasioni le autorità giudiziarie italiane si sono avvalse dell'ordine europeo di indagine penale (OEI) per ottenerne la decriptazione e la trasmissione ad opera delle competenti autorità straniere (le quali erano riuscite a "bucare" le piattaforme in questione attraverso apposite attività di *hacking*).

Si discute, nondimeno, quale sia la **natura giuridica** di tali operazioni acquisitive e, di conseguenza, da quali **garanzie procedurali** dovrebbero essere assistite.

Ne è sorta una **diatriba giurisprudenziale**, che ha portato la Sezione III della Corte di cassazione, tramite l'ordinanza n. 47798 del 3 novembre 2023 più sopra allegata, a rimettere alle **Sezioni Unite** una **duplice questione**:

- i) se "l'acquisizione di messaggi su *chat* di gruppo scambiati con sistema cifrato, mediante OEI, presso autorità giudiziaria straniera che ne ha 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. o sia riconducibile in altra disciplina relativa all'acquisizione di prove";
- ii) "se inoltre, tale acquisizione debba essere oggetto, ai fini della utilizzabilità dei dati in tal modo versati in atti, di preventiva o successiva verifica giurisdizionale della sua legittimità da parte dell'autorità giurisdizionale nazionale".

2. Il metodo di acquisizione "libera". La **prima** delle questioni rimesse alle Sezioni Unite discende dal fatto che nella giurisprudenza della Corte di cassazione sono emersi **due distinti metodi** di acquisizione delle comunicazioni in questione.

Un **primo metodo**, che si potrebbe definire di "**acquisizione libera**", sostenuto, tra le molte, dalla Sezione I con la sentenza n. 6364 del 13 ottobre 2022-15 febbraio 2023 più sopra allegata, si fonda su **varie argomentazioni**[1].

a) Le operazioni investigative di cui si discute riguarderebbero "rappresentazioni comunicative incorporate in una base materiale con un metodo digitale": vere e proprie **prove documentali**, dunque, come tali acquisibili *ex art.* 234 *bis* o 234 c.p.p.

b) Trattandosi di dati non "disponibili al pubblico", in questi casi vi sarebbe stato il **consenso** da parte del **legittimo titolare** all'acquisizione, così come richiesto dall'art. 234 *bis* c.p.p.: soggetto 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*".

c) Avendo a che fare con documenti, sarebbe sufficiente, ai fini della loro acquisizione, un OEI emesso dal pubblico ministero italiano, **senza** la necessità di un **controllo** da parte di un **organo giurisdizionale italiano**, nè antecedente nè successivo.

d) Varrebbe, comunque, una **presunzione di legittimità** delle attività svolte dalle competenti autorità straniere che avevano proceduto alla decriptazione e trasmissione delle comunicazioni. Spetterebbe, al più, al "giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità"[2].

3. Le critiche al metodo di acquisizione "libera". Dal punto di vista dell'efficienza investigativa, il metodo di acquisizione libera presenta **innegabili vantaggi**, poichè, non richiedendo il rispetto di particolari garanzie, massimizza la rapidità delle operazioni.

Esistono, tuttavia, solide ragioni, poste opportunamente in rilievo da diversi studiosi[3] e, in particolare, dalla Sezione VI della cassazione con la sentenza n. 44154 del 26 ottobre 2023 più sopra allegata[4], per ritenere che il richiamo agli artt. 234 *bis* e 234 c.p.p. risulti **inconferente**.

A) Non si può dire che le comunicazioni in questione siano elementi conoscitivi del tutto preesistenti ed indipendenti dal procedimento, come avviene per i tradizionali documenti fisici. La loro natura digitale fa sì che le operazioni tecniche di captazione e di decriptazione necessarie per acquisirle in una forma intellegibile siano **atti procedurali**, spesso tali da avvenire in spazi coperti dal **diritto alla riservatezza**, e comunque suscettibili di alterarne il contenuto qualora non avvengano nel modo dovuto.

Depone in questo senso anche l'inquadramento giuridico di recente offerto dalla **Corte costituzionale**, in ambito nazionale, in merito ad elementi conoscitivi che presentano un'analogia con le comunicazioni criptate rinvenibili all'estero: i **messaggi elettronici di testo** (ad esempio gli *sms*, o i messaggi scambiati tramite l'applicazione *whatsapp*) già letti dai propri destinatari e conservati negli *smartphone*, qualificati dalla Corte non come documenti, ma come vera e propria "**corrispondenza**"[5].

B) Più specificamente, l'art. **234 bis**, che trova la sua matrice nell'art. 32 della Convenzione di Budapest sulla criminalità informatica, è stato concepito proprio per **evitare** il ricorso agli strumenti di **cooperazione giudiziaria**[6].

Nei casi in esame, per converso, l'impiego dell'OEI è un indice del fatto che gli organi inquirenti italiani non sarebbero riusciti ad acquisire le comunicazioni senza l'aiuto delle competenti autorità straniere

C) In ogni caso, non si potrebbe considerare "**legittimo titolare**" ai sensi dell'art. 234 *bis* c.p.p. l'autorità straniera che ha decriptato le comunicazioni, dovendo quest'ultima essere qualificata come "mero detentore qualificato di quei dati a fini di giustizia"[7].

Ebbene, il ricorso all'OEI ha le sue conseguenze, poichè comporta l'adozione di tutte le garanzie ricavabili dalla lettura integrata della **direttiva n. 41 del 3 aprile 2014**, che lo ha istituito a livello eurolunitario, e del **d.lgs. 21 giugno 2017, n. 108**, che lo ha trasposto all'interno del nostro sistema: garanzie che l'adozione del metodo di acquisizione "libera" porterebbe, inevitabilmente, ad aggirare.

4. Il metodo di acquisizione "garantita" tramite l'OEI: proporzionalità, equivalenza, controllo giurisdizionale. Per comprendere la portata delle garanzie in questione, si devono tenere presenti i **capisaldi** su cui poggia l'acquisizione delle prove all'estero tramite l'OEI.

L'emissione dell'OEI deve, anzitutto, soddisfare il criterio della **proporzionalità**, in base al quale i diritti fondamentali, il cui rispetto va assicurato sia nello Stato di emissione sia nello Stato di esecuzione, potrebbero essere compressi per ragioni legate alle esigenze investigative solo nella misura strettamente necessaria, lasciandone comunque intatto il nucleo essenziale[8].

Certo, la proporzionalità ha una valenza applicativa non semplice da individuare, inevitabilmente variabile da caso a caso. Un ulteriore criterio, nondimeno, concorre a definirne meglio la portata: il principio, che si potrebbe definire di "**equivalenza**", in base al quale gli atti di indagine richiesti nell'OEI dovrebbero poter essere emessi "alle stesse condizioni in un caso interno analogo"[9].

Ne discendono precise implicazioni quanto all'individuazione della tipologia di autorità competente ad emettere un OEI: il quale dovrebbe essere emesso o, comunque, autorizzato da un **giudice**, e **non solo** disposto da un **pubblico ministero**, laddove in un caso interno analogo quell'atto di indagine fosse soggetto ad un'approvazione giurisdizionale *ex ante*.

Se ne può ricavare, oltretutto, l'esigenza di prevedere dei **mezzi di impugnazione**, ossia dei rimedi tali da assicurare un controllo giurisdizionale *ex post*, di tipo perlomeno equivalente a quelli disponibili in un caso interno analogo[10].

Si aggiunga che, sotto quest'ultimo profilo, la **Corte di giustizia dell'Unione Europea** ha compiuto un passo ulteriore: secondo la sentenza **Gavanzov II** dell'11 novembre 2021, il diritto ad un "ricorso effettivo" di fronte ad un giudice previsto in generale dall'art. 47 della Carta di Nizza comporta che gli Stati adottino **adeguati mezzi di impugnazione** nei confronti degli OEI suscettibili di impattare sui diritti fondamentali; ciò, si badi bene, anche qualora tali *legal remedies* non fossero contemplati in rapporto ad un caso interno analogo[11].

La Corte di giustizia ha ritenuto, in questo modo, di introdurre una misura di **armonizzazione** dei vari sistemi nazionali[12]: vale a dire, un superiore *standard* di tutela unitario indipendente dalle caratteristiche dell'ordinamento del singolo Stato di emissione.

5. Garanzie a geometria variabile. L'acquisizione delle comunicazioni criptate di cui stiamo parlando presenta la complicazione di avvenire sulla base di **protocolli variabili** a seconda della situazione concreta e, in particolare, della circostanza che le comunicazioni siano o no in corso di svolgimento al momento della loro apprensione.

È pertanto inevitabile che, trasposto in una realtà così fluida, l'appena menzionato corredo di garanzie che emerge dalla legislazione sull'OEI non possa operare sempre con la stessa intensità, ma assuma varie declinazioni.

Quello che è certo è che esso sarebbe completamente pretermesso qualificando le comunicazioni criptate come dati acquisibili alle sole condizioni previste dagli artt. 234 *bis* o 234 c.p.p.

Ciò premesso, occorre distinguere. Si dovrebbe utilizzare la forma dell'ordine europeo di **intercettazione** se le comunicazioni fossero **ancora in corso di svolgimento**: evenienza in cui, in applicazione del principio di equivalenza, l'OEI andrebbe autorizzato *ex ante* dal giudice per le indagini preliminari[13].

Si dovrebbe, invece, disporre un ordine europeo di **sequestro** (e, se necessario, anche di **perquisizione**) quando si trattasse di **comunicazioni già inviate e lette**, e conservate in determinati dispositivi, sistemi o *server* informatici[14]: in questa diversa ipotesi, l'OEI, emesso dal pubblico ministero, sarebbe soggetto ad un controllo giurisdizionale di tipo *ex post* attraverso il **riesame del sequestro**[15], finalizzato a verificare la presenza delle condizioni per autorizzare l'attività di apprensione delle comunicazioni[16].

Nè va trascurato che, come a quanto pare si era verificato in diversi dei casi giunti all'attenzione della nostra Corte di cassazione, potrebbe trattarsi di **comunicazioni** di cui l'autorità straniera fosse già **autonomamente** venuta in **possesso** ai fini di un procedimento interno, a prescindere dalla richiesta dell'autorità italiana.

Nessun dubbio che, anche in casi del genere, dovrebbe essere pur sempre utilizzato lo strumento dell'OEI. Lo si ricava, fra l'altro, dall'art. 10 § 2 *a* della direttiva 2014/41, il quale ne prescrive l'impiego ai fini dell'"acquisizione di informazioni o prove che sono già in possesso dell'autorità di esecuzione, quando, in base al diritto dello Stato di esecuzione, tali informazioni o prove avrebbero potuto essere acquisite nel quadro di un procedimento penale o ai fini dell'OEI"[17].

Nessuno contesta che questo tipo di OEI dovrebbe essere disposto dal **pubblico ministero**^[18]. Non potrebbe, del resto, essere diversamente, se si considera che l'art. 6 della direttiva prevede che gli OEI vadano emessi o, comunque, convalidati perlomeno da un magistrato, fissando una condizione minimale al di sotto della quale non sarebbe possibile scendere.

Ciò detto, il fatto che l'art. 10 § 2 a della direttiva 2014/41 si limiti a richiamare l'osservanza del solo diritto dello Stato di esecuzione, non significa che l'acquisizione delle comunicazioni di cui l'autorità straniera fosse già in possesso potrebbe avvenire senza nessun riguardo per il **diritto dello Stato di emissione**.

Una conclusione del genere sarebbe in contrasto con le garanzie che, come si è detto, dovrebbero assistere la raccolta delle prove attraverso qualunque tipologia di OEI: garanzie che, comunque, dovrebbero includere la possibilità di un **controllo giurisdizionale** nello Stato di emissione **perlomeno ex post**.

Questa è la ragione per cui, come osserva la sentenza 44154/2023, anche le comunicazioni già autonomamente raccolte dall'autorità straniera dovrebbero essere acquisite sì attraverso un ordine europeo di sequestro emesso dal pubblico ministero, ma impugnabile dalla difesa con il **riesame**, così da ottenere una verifica giurisdizionale della presenza dei requisiti per il sequestro in base alla legge nazionale.

6. Inutilizzabilità per la mancanza di un controllo giurisdizionale nazionale sull'acquisizione delle comunicazioni? Stabilito che le comunicazioni di cui si discute non rientrano fra le prove documentali nel senso stretto del termine, e che la loro acquisizione tramite l'OEI debba sottostare ad un controllo giurisdizionale perlomeno di tipo *ex post* nello Stato di emissione, si può affrontare la **seconda** delle **questioni** devoluta all'attenzione delle **Sezioni Unite**: se tale controllo sia previsto a pena di **inutilizzabilità** delle comunicazioni nei processi instaurati nello Stato di emissione.

Per cercare di rispondere a questo interrogativo, va subito detto che, riguardo al regime di utilizzazione in Italia delle prove raccolte all'estero tramite l'OEI, il quadro normativo è lacunoso.

Nulla prescrive la direttiva 2014/41, il cui art. 14 § 7 rinvia alle “norme processuali nazionali”, limitandosi a richiedere che “nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite”^[19].

A livello interno, l'art. 36 d.lgs. 108/2017 prevede, genericamente, l'inserimento nel fascicolo per il dibattimento degli atti compiuti all'estero tramite OEI rispetto ai quali i **difensori** sono stati “posti in grado” di “esercitare le **facoltà** loro consentite dalla **legge italiana**”, senza meglio specificare quali siano le facoltà in questione.

Quanto agli atti già autonomamente compiuti dall'autorità giudiziaria straniera, rileva l'art. 78 disp. att. c.p.p., il quale rinvia all'art. 238 c.p.p. Quest'ultimo, a sua volta, richiede il rispetto delle modalità di assunzione delle prove dei dibattimenti italiani: regole di cui però sarebbe irragionevole pretendere l'integrale osservanza, venendo in gioco elementi già raccolti in base al diritto straniero.

Anche sotto il profilo in esame, tuttavia, è bene non fermarsi alla lettura di singoli articoli di legge, ma considerare il sistema dell'OEI nel suo complesso.

Non si potrebbe, *in primis*, ignorare il più sopra considerato principio di **proporzionalità**, da cui deriva che, anche ai fini dell'utilizzazione e della valutazione delle prove raccolte con l'OEI, i diritti fondamentali e, in particolare, le garanzie difensive dovrebbero essere rispettate perlomeno nel loro nucleo fondamentale.

Su tale assunto convergono, in particolare, sia la sentenza 6364/2023 sia la sentenza 44154/2023, le quali ribadiscono qui un criterio già ampiamente utilizzato dalla Corte di cassazione nel settore delle rogatorie internazionali: le comunicazioni criptate raccolte all'estero tramite l'OEI, pur assunte nel pieno rispetto della *lex loci*, non potrebbero essere utilizzate se il loro impiego determinasse un contrasto con i **“principi fondamentali dell'ordinamento giuridico italiano”**, suscettibili di ricomprendere anche il diritto di difesa.

Non si tratta, però, di un'affermazione risolutiva, se si tiene conto del fatto che, come già emerso dall'esperienza delle rogatorie, il concetto di “principio fondamentale dell'ordinamento” è tutt'altro che univoco.

È, piuttosto, il principio di **equivalenza** che, applicato sul terreno dell'inutilizzabilità, risulta capace di offrire indicazioni più chiare agli interpreti. Ne discende, infatti, che le prove raccolte con l'OEI sarebbero inutilizzabili in Italia in tutte le situazioni in cui si verificassero violazioni di legge tali da originare un divieto probatorio in un caso interno analogo.

La **Corte di giustizia dell'Unione Europea** offre uno spunto in questa direzione, laddove afferma che le modalità di tutela dei diritti operanti a livello eurounitario non dovrebbero essere “meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno”, e non dovrebbero rendere “in pratica impossibile o eccessivamente difficile l'esercizio dei diritti”, evitando che “informazioni ed elementi di prova ottenuti in modo illegittimo rechino indebitamente pregiudizio a una persona sospettata di avere commesso reati”^[20].

Alla luce di queste considerazioni, si può individuare un **caso di inutilizzabilità** delle comunicazioni dovuta all'assenza di un controllo giurisdizionale preventivo: quando esse dovessero essere raccolte con le modalità delle **intercettazioni**, se si considera che, in un caso interno analogo, la mancata autorizzazione del giudice per le indagini preliminari sarebbe colpita dalla regola di esclusione stabilita dall'art. 271 comma 1 c.p.p.

Non così, invece, qualora le comunicazioni dovessero essere acquisite nelle forme dei **sequestri** emessi dal pubblico ministero (modalità, come si è detto, da adottare per le comunicazioni non più in corso di svolgimento, sia non ancora in possesso sia già in possesso dell'autorità straniera).

In tale diversa ipotesi, in un caso interno analogo non opererebbe **nessun divieto probatorio** connesso alla mancanza di un'autorizzazione giurisdizionale. Si potrebbe, al più, ottenere l'esclusione delle comunicazioni dal materiale probatorio a disposizione del giudice di merito tramite il **riesame** del sequestro.

7. Inutilizzabilità per la violazione del diritto della difesa di interloquire sulla modalità di acquisizione delle comunicazioni? Al profilo delle possibili conseguenze in caso di mancanza di un controllo giurisdizionale se ne aggiunge un altro: quello delle conseguenze in caso di **violazione** del diritto della **difesa di interloquire** sulle **modalità di raccolta** delle comunicazioni all'estero.

Va infatti detto che, indipendentemente dalle modalità di acquisizione impiegate, i risultati conoscitivi ottenuti dall'autorità straniera con la decrittazione delle comunicazioni non potrebbero essere accettati acriticamente a prescindere dalle loro modalità di svolgimento.

Quest'ultima sarebbe, per l'appunto, un'altra delle conseguenze determinate dall'inquadramento delle comunicazioni fra i documenti: come se si trattasse di prove precostituite, dotate di un valore conoscitivo autonomo ed impermeabile rispetto alle attività procedurali impiegate per venirne in possesso.

Proprio muovendo da un assunto del genere, la decisione 6364/2023 della Sezione I della cassazione sostiene che sarebbe possibile **presumere** che i testi rappresentati dalle comunicazioni trasmesse dall'autorità straniera siano privi di alterazioni e manipolazioni, salvo che la difesa riesca a dimostrare il contrario. In questa logica, sarebbe sufficiente, ai fini della protezione della c.d. catena di custodia, l'inserimento dei *files* contenenti le comunicazioni in "supporti ottici non riscrivibili (*cd-rom*)", trasmessi dall'autorità straniera "all'interno di buste sigillate antieffrazione"**[21]**.

Sono **affermazioni criticabili**, se si tiene conto del fatto che le comunicazioni in questione, per poter essere convertite in dati informativi comprensibili, richiedono lo svolgimento di attività procedurali spesso ad alto tasso tecnico-specialistico: operazioni che, come avviene per l'acquisizione di qualunque tipo di prova digitale, potrebbero condizionarne e perfino pregiudicarne la resa conoscitiva se non venissero svolte nel modo dovuto.

Di qui la necessità di porre la difesa nelle condizioni di contraddire sulle modalità della loro raccolta, mettendole a disposizione la **versione originale** delle comunicazioni e, soprattutto, gli **algoritmi** utilizzati per la loro decriptazione**[22]**.

La sentenza 6364/2023 obietta che la conoscenza da parte della difesa delle tecniche di decriptazione sarebbe irrilevante, per la ragione che, in caso di utilizzo di algoritmi scorretti, sarebbe impossibile ottenere testi intellegibili, potendosi al più conseguire "stringhe informatiche prive di valore informativo".

Ma l'assunto dà per scontato che esista un unico metodo di decifrazione utilizzabile, semplificando forzatamente una realtà che, dal punto di vista tecnico-informatico, potrebbe possedere molte più sfaccettature e opacità, dipanabili solo attraverso un pieno contraddittorio.

C'è, naturalmente, da chiedersi se il mancato assolvimento di tali oneri informativi determini un'**inutilizzabilità****[23]**. Pure qui la risposta passa dal principio di equivalenza, da cui però emerge l'**assenza** di un **divieto probatorio** quando, in un caso interno analogo, la difesa non avesse la possibilità di accedere alla documentazione relativa alle modalità investigative utilizzate, sia quando si impieghi la forma delle intercettazioni**[24]** sia quando si usi la forma del sequestro**[25]**.

Al contempo, il fatto che la difesa non possa sapere in che modo le comunicazioni sono state decifrate, impedendole di verificare che il loro contenuto non sia stato alterato, integrerebbe una **violazione** delle norme in tema di **assistenza tecnica** dell'imputato. Si può quindi sostenere che, almeno di regola, ne deriverebbe una **nullità intermedia** ai sensi dell'art. 178 comma 1 lett. c.c.p.**[26]**.

Sotto questo profilo non vanno, però, dimenticate possibili esigenze di segno opposto alla trasparenza delle operazioni acquisitive suscettibili di manifestarsi nello Stato straniero. La sentenza 44154/23 non lo trascura, menzionando l'eventualità che l'autorità straniera eviti di comunicare le modalità di raccolta delle comunicazioni per ragioni di **sicurezza nazionale** o di **segretezza dei metodi di indagine** (per non consentire agli esponenti della criminalità di prendere contromisure volte a nascondere le proprie comunicazioni attraverso tecniche informatiche ancora più efficaci)**[27]**.

In tali evenienze, per evitare di perdere completamente il contributo conoscitivo di comunicazioni magari preziose per la ricostruzione dei fatti, non resterebbe che una via: ritenere che il rispetto del diritto della difesa di conoscere le modalità di acquisizione diventi **oggettivamente impossibile**, a causa di una scelta dell'autorità straniera competente a raccogliere le prove non sindacabile dall'autorità italiana.

Certo, in questo modo si neutralizzerebbe la possibilità di rilevare o dedurre la nullità, rendendo le comunicazioni pienamente utilizzabili nel processo italiano.

Nondimeno, la mancanza di trasparenza nella loro raccolta dovrebbe trovare una **compensazione** sul piano della **valutazione** del loro peso conoscitivo**[28]**. Vale a dire che il giudice di merito, per non rischiare di incorrere in un vizio di motivazione, dovrebbe andare alla ricerca di un **adeguato grado di conferma** dei fatti rappresentati dalle comunicazioni nel rimanente materiale probatorio: un'esigenza logica che non avrebbe certo bisogno di un'apposita statuizione legislativa**[29]**, risultando connaturata alla necessità di osservare lo *standard* dell'**al di là di ogni ragionevole dubbio** ex art. 533 comma 1 c.c.p.

[11] V. anche, a favore dell'applicabilità dell'art. 234 *bis*, Cass., Sez. III, 19 ottobre 2023, n. 47201; Id., Sez. IV, 28 marzo 2023, n. 19623; Id., Sez. I, 8 febbraio 2023, n. 19155; Id., 13 gennaio 2023, n. 19083. Nel senso, invece, dell'applicabilità dell'art. 234, Id., Sez. VI, 26 ottobre 2023, n. 46833; Id., 27 settembre 2023, n. 46482.

[12] Così, fra le molte, Cass., Sez. I, 6364/2023, da cui sono tratte anche le precedenti citazioni.

[13] Cfr. L. Filippi, *Quattro miti da sfatare sull'intercettazione dei cellulari BlackBerry*, *penalepd.it*, 28 aprile 2023; N. Gallo, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, in *archiviopenale.it*, 2023, n. 3, p. 8 s.; F. Resta, *Criptofonini e ordine europeo d'indagine: le questioni poste alle Sezioni Unite*, in *giustiziainsieme.it*, 16 novembre 2023; G. Spangher, *Chat. Saranno le Sezioni Unite a "decriptare" le questioni giuridiche*, *ivi*, 13 novembre 2023.

[14] V. anche la sentenza "gemella" del 26 ottobre 2023, n. 44155.

[15] In quanto tale, acquisibile con le garanzie previste dall'art. 15 Cost. e con le modalità dell'apposito sequestro stabilite dall'art. 254 c.c.p.: cfr. Corte cost., 27 luglio 2023, n. 170. Va peraltro aggiunto che la Corte costituzionale ha indicato, ai fini dell'inquadramento nella categoria della corrispondenza, un requisito di incerta determinazione: il carattere di "attualità", il quale dovrebbe "presumersi, sino a prova contraria, quando si discuta di messaggi scambiati" "a una distanza di tempo non particolarmente significativa rispetto al momento in cui dovrebbero essere acquisiti", "e per giunta ancora custoditi in dispositivi protetti da codici di accesso".

[16] Tanto è vero che, in base all'art. 32 della Convenzione di Budapest, i dati in esame, se "disponibili al pubblico (fonti aperte), oppure con il consenso del legittimo titolare (la "persona legalmente autorizzata a divulgare i dati"), sono direttamente acquisibili da ciascuna Parte della Convenzione, "senza l'autorizzazione di un'altra Parte".

[7] Così Cass., Sez. VI, 44154/2023.

[8] Artt. 1 § 5 e 6 § 1 a direttiva 2014/41; art. 7 d.lgs. 108/2017. Cfr. L. Scomparin-A. Cabiale, *The Proportionality Test in Directive 2014/41/EU: Present and Future of a Fundamental Principle*, in *rivista.eurojus.it*, 2022, n. 2.

[9] Art. 6 § 1 b direttiva 2014/41; art. 27 comma 1 d.lgs 108/2017.

[10] Così come, del resto, prescrive l'art. 14 § 1 direttiva 2014/41.

[11] Corte giust., 11 novembre 2021, *Gavanozov II*, C-852/19.

[12] V., sul punto, O. Calavita, *Un mezzo di impugnazione per ogni atto di indagine? Da Gavanozov II un ulteriore stimolo della Corte di giustizia verso l'armonizzazione dei sistemi processuali penali*, in *lalegislazionepenale.eu*, 8 marzo 2022; C. De Luca, **La Corte di giustizia si pronuncia nuovamente sull'ordine europeo di indagine penale: la tutela dei diritti fondamentali prevale sull'efficienza investigativa**, in questa *Rivista*, 9 marzo 2022.

[13] Art. 43 d.lgs. 108/2017.

[14] Art. 27 d.lgs. 108/2017; in un caso interno analogo, il sequestro presso *server* troverebbe la sua disciplina nell'art. 254 *bis* c.p.p.

[15] Art. 28 d.lgs. 108/2017, il quale a sua volta rinvia all'art. 324 c.p.p.

[16] Nè va trascurato che, talvolta, le operazioni potrebbero assumere natura mista, avendo ad oggetto, allo stesso tempo, comunicazioni in corso e comunicazioni già inviate. In situazioni del genere, si dovrebbero adottare le più elevate garanzie previste per il primo tipo di attività.

[17] Si vedano anche il Considerando 7 e l'art. 1 § 1 direttiva 2014/41. Lo presuppongono pure gli artt. 2 comma 1 lett. a e 9 comma 5 lett. a d.lgs. 108/2017.

[18] Così, in particolare, anche la sentenza 44154/2023.

[19] Ponendo la questione, quindi, sul piano dell'individuazione del peso conoscitivo delle prove raccolte.

[20] Corte giust., 6 ottobre 2020, *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, § 222 s.

[21] Cass., Sez. I, 6364/2023. V. anche Cass., Sez. VI, 25 ottobre 2022, n. 48330.

[22] Informazioni che, peraltro, nel sistema dell'OEI dovrebbero essere trasmesse dall'autorità di esecuzione all'autorità di emissione: si vedano gli artt. 6 § 3, 9 § 6, 11 § 4 e 16 direttiva 2014/41, nonché l'art. 6 d.lgs. 108/2017 e la lettera D dell'allegato B a quest'ultimo ("altre informazioni che possono essere utili all'autorità di emissione").

[23] Così come avverrebbe, come si è detto in precedenza, quando, dovendo utilizzare la forma delle intercettazioni, queste ultime non venissero sottoposte ad un'autorizzazione preventiva da parte del giudice per le indagini preliminari.

[24] In rapporto alle quali l'ipotesi non ricadrebbe nei divieti probatori previsti dall'art. 271 c.p.p.

[25] In senso analogo, v. W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni Unite*, in *penaledp.it*, 29 novembre 2023.

[26] Cass., Sez. VI, 44154/2023. Similmente, in rapporto all'acquisizione di messaggi criptati rinvenibili in *server* situati in Canada, v. Cass., Sez. IV, 15 ottobre 2019, n. 49896.

[27] Gli artt. 11 § 1 b direttiva 2014/41 e 10 § 1 lett. c d.lgs. 108/2017, del resto, consentono all'autorità di esecuzione perfino di rifiutare l'OEI per ragioni di sicurezza nazionale.

[28] In generale, sull'esigenza che la violazione del diritto alla *disclosure* della difesa venga compensato attraverso l'applicazione di altre garanzie processuali, v. Corte eur., Grande Camera, 26 settembre 2023, *Yüksel Yalcinkaya c. Turchia*, § 308, in un caso in cui i giudici nazionali avevano ritenuto decisivo ai fini dell'accertamento della colpevolezza, addirittura, il mero utilizzo da parte dell'imputato di un sistema di messaggistica criptato, equiparato in via presuntiva all'adesione consapevole e volontaria ad un'organizzazione criminale, indipendentemente dal contenuto dei messaggi e dall'identità dei loro destinatari.

[29] Come quella, per intenderci, contenuta nell'art. 192 comma 3 c.p.p. in rapporto alla valutazione delle dichiarazioni degli imputati in procedimenti connessi.