Acquisizione di prove digitali criptate all'estero mediante Ordine Europeo d'Indagine penale (OEI)

Acquisition of encrypted digital evidence abroad through the European Criminal Investigation Order (EIO)

Nunzio Gallo
Dottorando di ricerca in *Law and Cognitive Neuroscience*
Università degli Studi di Roma Niccolò Cusano

Sommario: 1. Introduzione. - 2. Cenni sull'OEI - 3. Gli arresti giurisprudenziali in merito alla qualificazione dei dati informatici acquisiti all'estero. – 4. I principi stabiliti dalle fonti sovraordinate. – 5 Competenza per l'emissione dell'OEI e rimedi difensivi. – 6. L'utilizzabilità della prova digitale acquisita tramite OEI. - 7. La direzione indicata dalle Sezioni unite: finalmente verso soluzioni univoche?.

ABSTRACT

L'elaborato è incentrato sul tema della corretta qualificazione degli elementi probatori digitali acquisiti all'estero mediante l'ordine europeo di indagine, nonché sulla competenza ad accogliere le doglianze della difesa in merito all'illegittima emissione dell'OEI. Dopo averne analizzato presupposti sovranazionali ed interni, sulla scorta dei principi espressi dalla giurisprudenza di legittimità, la disamina si focalizza sui risvolti nel procedimento penale di destinazione.

***

The paper focuses on the topic of the correct qualification of digital evidence acquired abroad through the European Investigation Order, as well as on the competence to accept the defense's complaints regarding the illegitimate issuance of the EIO. After analyzing supranational and internal prerequisites, on the basis of the principles expressed by the jurisprudence of legitimacy, the examination focuses on the implications in the criminal proceedings of destination.

1. Introduzione.

L'evoluzione tecnologica ha coniato un quadro casistico estremamente va-riegato suscettibile di ulteriori distinzioni generate dalle specificità della natura tecnico-informatica dell'informazione oggetto dell'investigazione, a cui le regole del diritto dovrebbero adeguarsi cercando di trovare soluzioni

univoche in ossequio al principio di uguaglianza processuale[1]. Ebbene, nell'ambito di questo intricato coacervo di esperienze investigative digitali, che talvolta originano pro-nunce contrastanti, risalta la *quaestio* dell'acquisizione della messaggistica crip-tata allocata sul server estero ed il conseguente "dilemma procedimentale" sulla tipologia di mezzo di ricerca della prova in cui ricondurre questo tipo di attività. Interrogativo che è stato parzialmente risolto da un lato, dal duplice intervento della Corte di cassazione con due sentenze "gemelle"[2] e, dall'altro, dall'inter-vento delle Sezioni unite che si sono pronunciate recentemente su alcuni aspetti della tematica[3].

In primis, la Sesta sezione penale con due sentenze "gemelle" - emesse lo stesso giorno dallo stesso collegio -, pronunciandosi sulla impugnazione proposta dalle difese dei prevenuti avverso due ordinanze del Tribunale delle libertà[4], ha espresso una serie di principi che hanno ridefinito, ancora una volta, la tematica della acquisizione di elementi probatori digitali, da un server allocato all'estero, mediante OEI[5]. In particolare, nell'ambito di un'indagine per reati in materia di traffico internazionale di stupefacenti, il Tribunale del riesame aveva ravvisato i gravi indizi di colpevolezza sulla base delle comunicazioni intercorse tra gli indagati attraverso un sistema di messaggistica criptato (Sky – ECC). Materiale che era stato acquisito dal Pubblico ministero italiano mediante l'emissione di ordini europei di indagine, finalizzati ad ottenere dall'Autorità giudiziaria francese le *chat* e le altre conversazioni intercorse tramite la piattaforma di messaggistica in parola.

Si tratta di un sistema di messaggistica che consente di acquistare una licenza annuale per l'utilizzo dei dispositivi forniti dall'azienda, che tra le varie caratteristiche permettono di disabilitare i microfoni, il GPS e le videocamere,

[1] F. DINACCI, *I modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, in *Arch. pen. web.*, 3/2024, p. 1, evidenzia che un quadro così variegato di pronunce conduce, per contro, al «diritto del caso singolo».

[2] Si tratta di Cass. Pen, Sez. VI, 26 ottobre 2023, Iaria e Kolgjokaj, rispettivamente n. 44154 e 44155, con nota di N. GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo di Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, in *Arch. pen. web.*, 3/2023, pp. 1 ss..

[3] C. CONTI, *Il principio di non sostituibilità: il sistema probatorio tra costituzione e legge ordinaria*, in *Cass. pen.*, 2/2024, p. 452, sul punto rileva che si è al cospetto di una vera e propria «opera di "sussunzione" [che] viene ormai condotta attraverso schemi logici ricorrenti, che si traggono nitidamente dall'analisi di una giurisprudenza di altissimo livello scientifico oggi pervenuta alla piena consapevolezza di aver avviato un vero e proprio percorso metodologico».

[4] Ordinanza del Tribunale di Milano del 29 maggio 2023 e Ordinanza del Tribunale di Reggio Calabria del 16 giugno 2023.

[5] Sulla tematica della c.d. *data retention*, intesa come consultazione dei dati conservati dal gestore di rete o dal *provider*, L. CUOMO, *La prova digitale*, in G. Canzio, L. Luparia (a cura di), *Prova scientifica e processo penale,* Cedam, Milano, 2022, pp. 663 ss..

nonché la cancellazione dei messaggi criptati inviati dopo soli 30 secondi; inoltre, qualora un dispositivo destinatario non sia raggiungibile dalla rete, il messaggio non ricevuto viene cancellato dopo 48 ore dall'invio. L'utente ha anche la possibilità di fruire di una *sim-card* di proprietà del gestore che garantisce l'anonimato anche se, ovviamente, all'atto dell'utilizzo, tramite le convenzionali tecnologie di comunicazione, vengono comunque rilasciati tutta una serie di dati (i cd. dati esteriori di comunicazioni, come i codici IMSI ed IMEI) che possono essere acquisiti dagli organi inquirenti nazionali e, dopo essere stati incrociati con i messaggi già decodificati dall'Autorità giudiziaria estera, rendono possibile l'individuazione degli utilizzatori degli apparecchi telefonici criptati Sky-Ecc[6]. Un sistema che peraltro, nel 2021, era stato attinto proprio da un'operazione di polizia coordinata dall'Europol, che aveva permesso di sgominare operazioni di narcotraffico su larga scala e attacchi alle persone[7].

2. Cenni sull'OEI.

L'istituto è stato coniato per favorire il «Roaming probatorio»[8] tra gli stati membri, con l'obiettivo di contrastare le nuove forme di criminalità attraverso una sempre maggiore cooperazione giudiziaria ed ha trovato positivizzazione normativa con l'entrata in vigore del d.lgs., 21 giugno 2017, n. 108 che ne ha scandito presupposti e *steps* procedurali, che qui si ripercorreranno solamente nei tratti essenziali[9].

[6] Sull'obbligo della società detentrice dei dati di collaborare con l'autorità inquirente, M. TORRE, *Sull'obbligo per il privato di collaborare ad attività di digital forensics: il caso "Apple – F.B.I."* in A. Cadoppi, S. Canestrari, A. Manna, V. Papa (diretto da), *Cybercrime*, Utet, Vicenza, 2019, pp. 1675 ss..

[7] Sul punto, il *board* della piattaforma negava di aver subito alcun tipo di penetrazione da parte della polizia, rilasciando il seguente comunicato «SKY ECC si basa su principi di sicurezza "zero-trust" che presuppongono che ogni richiesta sia trattata come una violazione e operano una verifica utilizzando più livelli di sicurezza per proteggere i messaggi dei suoi utenti. Tutte le comunicazioni SKY ECC sono crittografate attraverso tunnel privati tramite reti private distribuite. Tutti i messaggi sono crittografati con il più alto livello di crittografia odierno». P. ARNTZ, *Police credit "unlocked" SKY ECC encryption for organized crime bust, Malwarebites Labs,* 11.03.2021 (testo tradotto).

[8] L'espressione è di L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento* in T. Bene, L. Lupária, L. Marafioti (a cura di), *L'ordine europeo di indagine. Criticità e prospettive,* Giappichelli, Torino, 2016, p. 24.

[9] Sul d.lgs., 21 giugno 2017, n. 108, si vedano per tutti M. 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, pp. 208 ss. e A. 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, pp. 158 ss.. Più in generale sull'istituto, F. FALATO, *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale,* in *Arch. pen. web.*, 1/2018, pp. 1 ss..

Il meccanismo, finalizzato al compimento in altro Stato membro di atti d'indagine mirati all'acquisizione delle prove, comprese quelle già in possesso dell'autorità di esecuzione ed in tempistiche contenute, prevede che il P.m. nella fase delle indagini preliminari ed il giudice, in quelle successive, possono emettere l'Ordine Europeo d'Indagine, nell'ambito di un procedimento penale (al quale la legge affianca il procedimento per l'applicazione di una misura di prevenzione patrimoniale) ed in funzione delle rispettive attribuzioni[10]. L'ordine, che deve essere elaborato secondo il modello allegato allo stesso decreto, deve indicare una serie di dati che sono necessari per porre l'autorità di esecuzione nelle condizioni di valutare i requisiti di ammissibilità previsti dalla *lex loci* e l'eventuale sussistenza di motivi di non riconoscimento o di non esecuzione. Una volta emesso l'ordine, in linea con le caratteristiche degli strumenti fondati sul mutuo riconoscimento, questo è trasmesso (nella lingua ufficiale dello Stato di esecuzione o in quella eventualmente indicata) direttamente all'autorità di esecuzione, eventualmente individuata anche mediante i punti di contatto della Rete giudiziaria europea. Nell'ottica di semplificare la trasmissione dell'ordine e delle eventuali comunicazioni correlate, è stata prevista la possibilità di ricorrere al Ministero della Giustizia, soltanto nei casi in cui sia necessario, ovvero in caso di difficoltà nelle comunicazioni con l'autorità di esecuzione, o quando insorgano questioni sulla provenienza e autenticità dell'atto, conformemente a quanto stabilito dalla direttiva 2014/41/UE. Mentre, nel caso di ordini relativi a procedimenti per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., occorre informare il Procuratore nazionale antimafia e antiterrorismo.

Per quanto riguarda la procedura passiva, è previsto un vaglio ai fini del riconoscimento dell'OEI effettuato dall'organo requirente entro trenta giorni dalla sua ricezione, ovvero entro il diverso termine – comunque non superiore a sessanta giorni – indicato dall'autorità emittente. Il Procuratore della Repubblica presso il Tribunale del capoluogo del distretto in cui gli atti devono essere compiuti, una volta ricevuta la richiesta di acquisizione probatoria da parte dell'autorità estera, è tenuto ad effettuare una valutazione preliminare sulla possibilità di dar corso all'assistenza sollecitata, controllando la compatibilità giuridica dell'atto richiesto, che deve presentare determinati requisiti formali e sostanziali. Si tratta di un giudizio sull'ammissibilità della domanda di cooperazione, condotto alla luce dei parametri fissati agli artt. 2, comma 1, lett. a), 7, 9, commi 1, 2 e 3 e 10 del d.lgs. n. 108 del 2017 e quindi di una verifica funzionale al proficuo dialogo tra le autorità giudiziarie interessate dalla procedura di cooperazione. Parametri, tra i quali rientra quello della verifica del requisito della doppia

[10] Sulla tematica dell'acquisizione extraterritoriale della prova, C. VALENTINI, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Cedam, Padova, 1998, pp. 212 ss.

incriminazione, in questo campo inteso in senso elastico, risultando sufficiente che il nucleo essenziale del fatto integri un illecito in entrambi i sistemi giuridici[11].

L'eventuale sussistenza di una delle condizioni impeditive previste dal decreto, conduce ad un'interlocuzione con l'autorità emittente, finalizzata a consentire alla stessa di emendare, correggere, integrare i difetti riscontrati, mentre il diniego del riconoscimento e dunque l'esecuzione dell'ordine, è circostanza che si verifica solamente in caso di mancato adeguamento o rettifica.

In assenza di rilievi, ovvero, in caso di risoluzione di quelli eventualmente riscontrati, il Procuratore adotta apposito decreto motivato, a mezzo del quale riconosce l'OEI e quindi l'atto di indagine richiesto. Provvedimento che deve essere notificato al difensore dell'indagato nei termini e con le modalità previsti dalla normativa interna per lo specifico atto da compiere. Nel caso in cui la disciplina nazionale preveda solo il diritto del difensore di assistere al compimento dell'atto, senza preventivo avviso, la comunicazione deve avvenire al momento in cui l'atto è compiuto, o quantomeno immediatamente dopo, in modo tale da poter consentire all'indagato di formulare, nei termini previsti, eventuale opposizione al G.I.P.[12]. L'eventuale accoglimento dell'opposizione implica l'annullamento del decreto di riconoscimento e, dunque, l'impossibilità di procedere

[11] Sui connotati di quest'ultimo requisito M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in A. Cadoppi, S. Canestrari, A. Manna, V. Papa (diretto da), *Cybercrime*, cit., p. 1625.

[12] Per M. R. GERACI, *Ordine europeo di indagine ricevuto dall'estero e rimedi impugnatori praticabili*, in *Cass. pen*., 9/2019, p. 3193, si tratta di «un adempimento di fondamentale importanza, che segna un ulteriore profilo di discontinuità rispetto alla vecchia disciplina rogatoriale: mentre quest'ultima non contemplava alcun rimedio avverso la decisione (positiva o negativa che fosse) della Corte di appello sull'exequatur, la nuova normativa prevede un'apposita impugnazione nei confronti del decreto di riconoscimento dell'O.E.I., che può essere contestato dalla persona indagata e dal suo difensore con un'opposizione presentata al Giudice per le indagini preliminari. E a tal fine la comunicazione del decreto di riconoscimento svolge un ruolo essenziale, segnando il dies a quo di decorrenza del termine di cinque giorni concesso per presentare il gravame in parola». Sulle conseguenze del ritardo della comunicazione del decreto di riconoscimento dell'OEI, cfr. Cass. Pen., Sez. VI, 5 novembre 2020, n. 30885, Con nota di G. MAZZA, *Ordine europeo di indagine: la forma soccombe davanti alla sostanziale assenza di pregiudizio*, in *Dir. Pen. Proc*., 10/2021, pp. 1343 ss., ove la Corte ha precisato che «In tema di ordine europeo di indagine passivo, avente ad oggetto la richiesta di atti di perquisizione e sequestro, la tardiva comunicazione al difensore del decreto di riconoscimento, oltre i termini previsti dall'art. 4, comma 4, D.Lgs. 21 giugno 2017, n. 108, non è causa di nullità dello stesso, ma comporta solo il differimento del "*dies a quo*" di decorrenza del termine per proporre opposizione ai sensi dell'art. 13, comma 1, del medesimo D.Lgs. n. 108 del 2017, trattandosi di violazione formale, priva di sanzione processuale, che non influisce sull'esito del giudizio di opposizione, limitato in via esclusiva alla valutazione della legittimità dell'ordine di indagine». Pronuncia annotata anche da A. FABBRICATORE, *Effetti della ritardata comunicazione del decreto di riconoscimento dell'OIE*, in *GI*, 6/2021, pp. 1474 ss.,

all'esecuzione dell'ordine, ovvero – se già eseguito – di provvedere al trasferimento dei risultati degli atti posti in essere[13].

In chiave critica, in dottrina è stato sottolineato che nel coniare questo meccanismo di cooperazione giudiziaria non è stata riprodotta la regola contenuta all'art. 6, par. 1, lett. b della direttiva 2014/41/UE, secondo cui l'OEI può essere disposto soltanto quando l'atto istruttorio avrebbe potuto essere emesso «alle stesse condizioni in un caso interno analogo» e che, parimenti, non è stato inserito il riferimento al principio di proporzionalità che, sempre secondo l'art. 6, par. 1, lett. a, deve orientare l'autorità emittente[14]. Omissione, quest'ultima, che a parere della Relazione illustrativa, deriverebbe dal fatto che «il principio di proporzione è immanente al sistema relativo ai mezzi di prova e di ricerca della prova, calibrato anche in relazione alla gravità dei reati per cui si procede»[15].

3. Gli arresti giurisprudenziali in merito alla qualificazione dei dati informatici acquisiti all'estero.

Delineato l'istituto nelle sue direttrici essenziali, ci si focalizzerà sulle argomentazioni recentemente intessute dalla giurisprudenza di legittimità sulla tematica *de quo*, con particolare riferimento alle casistiche al vaglio del Tribunale delle libertà esaminate dalle due sentenze gemelle della Sesta sezione. Impianti motivazionali che, seppur elaborati in seno a differenti scrutini, verranno trattati congiuntamente per la molteplicità dei punti di contatto tra le due vicende processuali, nonché in ragione dell'unitarietà dei principi enucleati dalla Corte di Cassazione.

Chiamata a pronunciarsi all'esito di un'indagine per reati in materia di traffico internazionale di stupefacenti, la Suprema corte ha ritenuto meritevoli di accoglimento le doglianze promosse dalle difese degli indagati nelle due vicende

[13] M. R. GERACI, *Ordine europeo di indagine ricevuto dall'estero e rimedi impugnatori praticabili,* cit., 3194, evidenzia che la tardiva comunicazione del decreto di riconoscimento, «di fatto "costringe" l'indagato all'accettazione delle determinazioni del suo antagonista processuale, privandolo della possibilità di una pronta reazione alle stesse, attivando un vaglio giurisdizionale su quello che è un atto di parte – il decreto ex art. 4, cit., appunto – con conseguente integrazione di una nullità ex art. 178, comma 1, lett.c), c.p.p.» per la lesione delle prerogative difensive del prevenuto, come chiarito anche da Cass. Pen., Sez. VI, 31 gennaio 2019, n. 8320 in *Cass. pen*., 9/2019, pp. 3178 ss..

[14] A. MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale,* cit., p. 170. Sul punto M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017*, cit., p. 2101 osserva anche che il mancato esplicito riferimento al principio di legalità può essere colmato sulla scorta di un'interpretazione del testo orientata al contenuto della direttiva che, sul punto risulta sufficientemente dettagliata.

[15] Così la Relazione illustrativa, allegata allo Schema di D.Lgs. recante norme di attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale, p. 18.

analizzate, ritenendo per contro gravemente deficitarie le ordinanze impugnate nella parte in cui il Tribunale del riesame ha ritenuto che gli ordini europei di indagine, emessi dal procuratore della Repubblica, abbiano avuto ad oggetto esclusivamente forme di acquisizione di documenti e dati informatici, qualificabili ai sensi dell'art. 234-*bis* c.p.p.. In particolare, in entrambi i provvedimenti gravati non sarebbe stato chiarito se l'Autorità giudiziaria estera avesse avviato autonomamente le indagini, sulla base di una precedente iscrizione della *notitia criminis*, oppure se le investigazioni fossero state attivate anche su impulso dei Pubblici ministeri italiani e ciò nonostante le eccezioni sollevate dalle difese nel corso della trattazione dell'udienza di riesame.

Secondo il Giudice di legittimità si tratta di circostanze dirimenti, atteso che lo stesso Tribunale delle libertà (in questo caso, di Milano) aveva specificato che l'acquisizione dei c.d. "dati freddi" era avvenuta a seguito del compimento di una ulteriore - non meglio precisata - attività di indagine disposta dall'Autorità giudiziaria francese. Attività investigativa che, secondo la ricostruzione difensiva, era consistita, da un lato, nell'utilizzo di strumenti di intercettazione di comunicazioni in corso, nonché di captatori informatici (come *trojan* e *malware*), impiegati per ottenere le chiavi di decifrazione presenti nei *devices* utilizzati dai fruitori del sistema di messaggistica in questione e, dall'altro, nel sequestro di materiale nella disponibilità della società di messaggistica. Seppur, sottolinea la Corte, in quest'ultimo caso non è chiaro se l'acquisizione avesse ad oggetto interi sistemi informatici ovvero solo i relativi dati riversati su altri supporti a disposizione del *provider*.

Al fine di definire l'utilizzabilità degli elementi probatori raccolti all'estero mediante OEI, si deve inquadrare volta per volta il mezzo di ricerca della prova di cui si richiede l'autorizzazione di impiego e ciò in ossequio al principio di equivalenza di cui all'art. 6, par. 1, lett. b direttiva 2014/41/UE[16], secondo il quale tale

[16] Si tratta della direttiva del Parlamento europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine. In letteratura, M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale*, in *Proc. pen. giust*., 3/2015, pp. 1 ss. e L. CAMALDO – F. CERQUA, *La direttiva sull'ordine europeo di indagine penale: le nuove prospettive per la libera circolazione delle prove*, in *Cass. pen.*, 2014, pp. 3511 ss., con specifico riferimento al *background* ed alla fase immediatamente precedente la sua adozione, G. FIORELLI, *Nuovi orizzonti investigativi: l'ordine europeo d'indagine penale*, in *Dir. Pen. Proc*., 6/2013, pp. 705 ss..
Sul punto v'è da segnalare che successivamente alla direttiva sull'OEI, in GUUE del 4 maggio 2016, n. 119, sono stati pubblicati due provvedimenti che assumono rilievo in materia di protezione dei dati personali: la Dir. UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Direttiva che abroga la decisione del Consiglio 2008/977/GAI; e il regolamento UE 2016/679, emesso a Bruxelles

strumento di cooperazione giudiziaria internazionale può essere utilizzato a condizione che l'autorità dello Stato di emissione verifichi che «l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere ammessi alle stesse condizioni in un caso interno analogo»[17]. Proprio sulla scorta di queste considerazioni, la Corte ha effettuato una corretta qualificazione giuridica degli atti di indagine compiuti dall'autorità straniera (in entrambe le vicende al vaglio si trattava, principalmente, dell'acquisizione di conversazioni telematiche, intercorse mediante piattaforma di messaggistica criptata) osservando come nel caso di specie non sia possibile applicare l'art. 234-*bis* c.p.p., che come noto permette di acquisire documenti e dati informatici conservati all'estero, con il consenso del legittimo titolare. In particolare, secondo i giudici di Piazza Cavour, detta disposizione può trovare operatività solamente nell'ipotesi di acquisizione di documenti e dati informatici che preesistevano rispetto all'avvio delle indagini da parte dell'autorità estera, ovvero elementi dematerializzati formati al di fuori delle stesse investigazioni. Nella vicenda in esame invece l'organo inquirente ha acquisito, da un lato, documentazione di attività di indagine e, dall'altro, documentazione preesistente e già oggetto di ulteriori iniziative istruttorie da parte dell'autorità straniera[18]. Pertanto, l'art. 234-*bis* è senza dubbio inutilizzabile se l'attività acquisitiva si sia concretizzata nell'apprensione occulta del contenuto archiviato in un server ovvero nel sequestro dei dati ivi (o anche in altri supporti) memorizzati nella disponibilità della società che gestisce la piattaforma di messaggistica. In questo contesto a nulla rileva se l'acquisizione sia avvenuta con il consenso del legittimo titolare e quindi il mittente o il destinatario dei messaggi in argomento o la stessa società, dovendo l'Autorità giudiziaria straniera essere considerata mero detentore qualificato del dato acquisito. Questa cornice di intervento deve essere invece inquadrata nelle norme in materia di perquisizione e sequestri ed in particolare nella

il 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la Dir. 95/46/CE. In particolare, sulla Dir. UE 2016/680, ma più in generale anche sul rapporto tra il "pacchetto" di norme eurounitarie in tema di *privacy* e i diritti fondamentali dell'individuo, B. GALGANI, *Giudizio penale, habeas data e garanzie fondamentali,* in *Arch. pen. web.*, 1/2019, pp. 1 ss..

[17] Art. 6., comma 1, lett. b, direttiva 2014/41/UE, rinvenibile al link https://eur-lex.europa.eu.

[18] Il Tribunale del riesame sul punto aveva invece richiamato l'orientamento giurisprudenziale secondo il quale la messaggistica intercorsa su chat di gruppo, mediante sistema Sky ECC, acquisita mediante OEI dall'autorità estera che ne ha eseguito la decriptazione, costituisce dato informativo documentale utilizzabile ai sensi dell'art. 234-*bis* c.p.p. e non flusso comunicativo, non trovando applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266-*bis* c.p.p.. Così, *ex plurimis*, Cass. Pen., Sez. IV, 5 aprile 2023, Papalia, n. 16347, Rv. 284563-01, non rileva neppure se i messaggi siano acquisiti dall'autorità giudiziaria straniera *ex post* oppure in tempo reale, poiché ciò che conta è se al momento della richiesta i flussi comunicativi siano o meno in atto.

disposizione di cui all'art. 254-*bis* c.p.p. in tema di sequestri di dati informatici allocati presso fornitori di servizi informatici, telematici e di comunicazioni.

Il Supremo consesso ha evidenziato inoltre che l'art. 43, comma 4, d.lgs., n. 108 del 2017[19] stabilisce che la richiesta contenuta in un ordine europeo di indagine penale possa avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate e pertanto anche questo tipo di attività, se richieste dall'autorità italiana, devono essere previamente autorizzate dal giudice.

4. I principi stabiliti dalle fonti sovraordinate.

Nell'affrontare la tematica in disamina, non si può prescindere dall'effettuare un *focus* sul *trend* eurounitario formatosi in materia, che ha di fatto mutato la nozione di intercettazione, intesa quale apprensione e acquisizione del contenuto di comunicazioni. Mutazione esegetica che prende l'abbrivio, *in primis*, dalla sentenza del 2 marzo 2021 (H.K., C-746/18), a mezzo della quale la Grande Camera ha chiarito una volta per tutte quali sono le condizioni per l'accesso, per finalità di prevenzione o accertamento di reati, ai dati relativi al traffico telefonico/informatico o ai dati relativi all'ubicazione ad esso associati. La Corte lussemburghese ha puntualizzato che questi dati "esterni" alle comunicazioni sono in grado di svelare informazioni sensibili sulla vita privata delle persone (come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati) ed ha stabilito in primo luogo che l'accesso deve essere circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica; e in secondo luogo che non possa essere il pubblico ministero l'autorità competente ad autorizzare l'accesso a tali dati.

Con riguardo al primo profilo, la Corte di giustizia ha ribadito come le deroghe alla protezione dei dati personali e le limitazioni di quest'ultima devono compiersi entro i limiti dello stretto necessario: quindi l'accesso deve soddisfare

[19] Si tratta della norma che regola le modalità di intercettazione di telecomunicazioni con l'assistenza tecnica dell'autorità giudiziaria di altro Stato membro UE. In dottrina, C. MARINELLI, *Le intercettazioni di comunicazioni*, in M. Daniele – R. Kostoris (a cura di), *L'ordine europeo di indagine penale*, Giappichelli, Torino, 2018, 221 ss.; R. G. GRASSIA, *La disciplina delle intercettazioni: l'incidenza della direttiva 2014/41/UE sulla normativa nazionale*, in T. Bene - L. Luparia - L. Marafioti (a cura di), *L'ordine europeo di indagine*, Giappichelli, Torino, 2016, pp. 199 ss.; C. PARODI, *Ordine di indagine europeo: la disciplina delle intercettazioni*, in *Cass. pen.*, 3/2020, pp. 1314 ss. e C. DE LUCA, *Intercettazioni eseguite mediante ordine europeo di indagine: qualcosa di nuovo sul fronte occidentale?*, in *Cass. pen.*, 2/2023, pp. 590 ss..

il requisito di proporzionalità, con la conseguenza che «tanto la categoria o le categorie di atti interessati, quanto la durata per la quale è richiesto l'accesso a questi ultimi, siano, in funzione delle circostanze del caso di specie, limitate a quanto è strettamente necessario ai fini dell'indagine in questione». Per quanto attiene invece al secondo profilo, la Corte ha rilevato come solo un giudice o comunque un'autorità indipendente terza nel processo, possano esercitare in modo imparziale ed obiettivo il controllo della sussistenza delle condizioni sostanziali e procedurali per l'accesso, così da garantire «un giusto equilibrio tra, da un lato, gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso».

Chiaramente questa pronuncia ha avuto un effetto inevitabilmente deflagrante sulla normativa interna che ha risposto mediante l'implementazione dell'art. 132 Cod. privacy, al fine di regolare la procedura di acquisizione dei dati esterni di traffico telefonico e telematico (che richiede ora un provvedimento autorizzativo e motivato del giudice) all'interno del rito criminale, circoscrivendone l'ambito di applicazione ai procedimenti iscritti per reati connotati da una certa gravità indiziaria, configurata sulla base della pena irrogabile.

Quanto al criterio di proporzionalità, il legislatore ha ancorato l'accesso, da un lato, al presupposto indiziario e, dall'altro, alle esigenze investigative. Il primo requisito è stato individuato in un livello di accertamento inferiore (sufficienti indizi) rispetto a quello previsto per l'autorizzazione del diverso e ben più invasivo mezzo di ricerca della prova delle intercettazioni. Il secondo («ove rilevanti ai fini della prosecuzione delle indagini») viene ad attuare il *dictum* della Corte di giustizia che ha imposto la verifica in concreto dell'effettiva necessità di un'azione di acquisizione, così da escludere la sua utilizzazione per *inquisitio generalis*.

Pertanto, l'acquisizione all'estero di documenti e dati informatici inerenti la corrispondenza o ad altre forme di comunicazione dovrebbe essere sempre autorizzata da un giudice.

Sul tema, assume inoltre una rilevanza centrale la posizione assunta dalla Corte costituzionale in ordine alla estensione applicativa delle garanzie previste dall'art. 15 Cost. in materia di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione. I Giudici delle leggi hanno recentemente chiarito che - ferma restando la distinzione tra l'attività di intercettazione, che concerne la captazione occulta da parte di un *extraneus* di comunicazioni nella loro fase c.d. dinamica, e l'attività di sequestro, che attiene all'acquisizione del supporto recante la memoria di comunicazioni già avvenute, cioè nella loro fase c.d. statica -

il concetto di corrispondenza, cui va assicurata la copertura dell'art. 15 Cost., è «ampiamente comprensivo, atto ad abbracciare ogni comunicazione di pensiero umano (...) tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza; ...(di talché) la tutela accordata dall'art. 15 Cost. - che assicura a tutti i consociati la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione», consentendone la limitazione «soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge» - prescinde dalle caratteristiche del mezzo tecnico utilizzato e deve essere estesa, quindi, ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici. Ne consegue che l'art. 15 Cost., riferibile alla «generalità dei cittadini», tutela la corrispondenza «ivi compresa quella elettronica, anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in mero documento storico»[20].

Si tratta di principi che, seppur affermati nell'ambito di una pronuncia emessa in un giudizio per conflitto di attribuzione tra poteri dello Stato (in riferimento alle immunità di cui gode il parlamentare ai sensi dell'art. 68 Cost.), possiedono una valenza di carattere generale nella parte in cui è stata considerata la portata precettiva dell'art. 15 Cost., ed ha indotto la Corte di cassazione a valorizzarne le implicazioni in relazione al caso di specie. Con questa decisione la Consulta ha stravolto completamente l'orientamento giurisprudenziale che attribuisce natura documentale, ai sensi dell'art. 234 c.p.p., alle forme di comunicazione digitale (come per es. le *e-mail* e la messaggistica *whatsapp*), e tanto sulla falsariga di quanto già da tempo chiarito in ambito eurounitario, ove si riconduce nell'alveo del concetto di corrispondenza tutelata dall'art. 8 C.E.D.U., sia i messaggi informatico-telematici (anche nella loro dimensione statica), che i messaggi di posta elettronica e la messaggistica istantanea inviata e ricevuta tramite internet. Un concetto ampiamente comprensivo, idoneo a contenere ogni comunicazione di pensiero umano tra due o più persone determinate, e che si attua anche in modo diverso dalla conversazione in itinere. Ciò in considerazione del fatto che la tutela dei precetti costituzionali non può esaurirsi con la ricezione del messaggio da parte del destinatario, ma deve perdurare fin tanto che esso conservi carattere di attualità e di interesse per gli interlocutori e deve riportare sotto il

[20] Corte cost., sent. n. 170 del 2023, per una disamina della quale si rimanda a C. FONTANI, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza,* in *Dir. Pen. Proc.*, 10/2023, pp. 1312 ss..

cono di protezione dell'art. 8 CEDU la corrispondenza *tout court*, nonché consentire all'interessato di poter promuovere un adeguato rimedio impugnativo[21].

Sotto questo punto di vista, infatti, la decisione del Giudice delle leggi si fonde con l'orientamento esegetico della giurisprudenza costituzionale, in base al quale si era puntualizzato che la tutela prevista da quella disposizione della carta fondamentale - che assicura a tutti i consociati la libertà e la segretezza «della corrispondenza di ogni altra forma di comunicazione», consentendone la limitazione «soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge» - proietta «il testo costituzionale alla possibile emersione di nuovi mezzi e forme della comunicazione riservata»[22] e si estende «ad ogni strumento che l'evoluzione tecnologica mette a disposizione a fini comunicativi, compresi quelli elettronici e informatici, ignoti al momento del varo della Carta costituzionale», in relazione ai quali le limitazioni della libertà costituzionale sono consentite solamente nel rispetto «della riserva assoluta di legge e di giurisdizione»[23].

Né vi è dubbio che la Corte costituzionale, proprio considerando le garanzie connesse alla riserva di giurisdizione, ha esteso alla libertà delle comunicazioni i criteri applicati per legittimare le limitazioni della libertà personale: spiegando che «il significato sostanziale, e non puramente formale, dell'intervento dell'autorità giudiziaria, in presenza di misure di prevenzione che comportino restrizioni rispetto a diritti fondamentali assistiti da riserva di giurisdizione», comporta che quel controllo vada inteso come «vaglio dell'autorità giurisdizionale (...) associato alla garanzia del contraddittorio, alla possibile contestazione dei presupposti applicativi della misura, della sua eccessività e sproporzione, e, in ultima analisi, consente il pieno dispiegarsi allo stesso diritto di difesa»[24].

5. Competenza per l'emissione dell'OEI e rimedi difensivi.

L'art. 6 della citata Direttiva sull'OEI, prevede che per compiere atti di indagine specifici in un altro Stato membro, sia emessa una decisione giudiziaria (l'OEI) da una autorità che secondo l'ordinamento vigente nello Stato di esecuzione, sia competente ad emettere i medesimi atti, in modo tale da garantire che gli atti di indagine richiesti mediante l'OEI avrebbero potuto essere parimenti

[21] Corte EDU, 5 settembre 2017, Barbulescu c. Romania, § 72; Corte EDU, sent. 3 aprile 2007, Copland c. Regno Unito, cfr. § 41, Corte EDU, 17 dicembre 2020, Saber c. Norvegia, § 48 e Corte giust. UE, 11 novembre 2021, Gavanozov, C-852-19.

[22] Corte cost., sent. n. 2 del 2023, in tema di illegittimità della norma sui divieti, stabiliti dall'autorità amministrativa, di possesso e utilizzo di apparecchi di comunicazione.

[23] Corte cost., sent. n. 20 del 2017, a proposito delle forme di controllo della corrispondenza epistolare del detenuto.

[24] Corte cost., sent. n. 2 del 2023.

emessi in un caso interno analogo. È onere dell'autorità di emissione accertare se le prove da acquisire sono necessarie e proporzionate ai fini del procedimento, se l'atto di indagine scelto è necessario e proporzionato per l'acquisizione delle prove e se l'acquisizione non rechi pregiudizio ai diritti stabiliti nell'art. 48 della Carta fondamentale dell'Unione europea, secondo quello che viene definito "controllo a monte"[25].

Orbene si è detto che l'art. 27 d.lgs n. 108 del 2017, prevede che le autorità competenti ad emettere l'OEI sono il Pubblico ministero ed il giudice che procede nell'ambito delle rispettive attribuzioni. Quindi il nomoteta ha designato il *dominus* delle indagini preliminari quale autorità incaricata ad emettere l'OEI anche nei casi in cui l'atto di indagine richiesto debba essere preventivamente autorizzato dal giudice (e ciò sulla base del fatto che il controllo del Giudice, di natura prettamente incidentale, come noto, in questa fase si sostanzia di fatto in sporadici interventi *ad acta*) escludendo la benché minima appendice di contraddittorio tra le parti, salvo nei pochi casi in cui sia il giudice a dover emettere lo stesso ordine[26]. La norma ha creato così una distorsione tra l'autorità competente ad emettere l'OEI e quella competente ad autorizzare l'atto di indagine richiesto. Nei casi invece in cui, l'atto da eseguire all'estero sia di competenza dello stesso Pubblico ministero è lo stesso OEI a costituire l'atto interno di indagine. Ed infatti, l'art. 28 prevede che in caso di sequestro probatorio è l'OEI a dover essere oggetto di impugnazione[27].

Quando si tratta di acquisire prove già in possesso dell'autorità dello Stato di esecuzione, non avendo né la disciplina comunitaria né quella di cui al citato decreto legislativo previsto alcunché, la giurisprudenza di legittimità ha ritenuto che deve ritenersi ferma anche per questo tipo di ordine, la competenza del P.m. nella fase delle indagini preliminari.

E' sempre la Suprema corte a determinare i rimedi esperibili nei confronti dell'illegittima emissione dell'OEI adottato in assenza del necessario e

[25] L'art. 48 della Carta fondamentale dell'Unione europea disciplina la versione europea del principio della presunzione di innocenza e del diritto di difesa dell'imputato.

[26] Nella fase delle indagini preliminari avviene, per esempio, in caso di attività di intercettazione. L'art. 43 del d.lgs n. 108 del 2017 prevede infatti che in questo caso l'OEI debba essere preceduto dal provvedimento di autorizzazione del GIP.

[27] Sul tema delle prerogative difensive nell'ambito di sequestro probatorio attuato mediante OEI, si veda G. BORGIA, *Riconoscimento dell'ordine europeo di sequestro probatorio e prerogative difensive*, in *GI*, 11/2019, pp. 2532 ss.. Mentre per una disamina del sistema dei controlli predisposti dal D.Lgs. n. 35 del 2016 avverso il provvedimento di blocco o di sequestro, C. VALENTINI, *I provvedimenti ablativi (dd.llgs. 7 agosto 2015, n. 137, 15 febbraio 2016, n. 35 e 29 ottobre 2016, n. 202)*, in F. Ruggieri (a cura di), *Processo penale e regole europee: atti, diritti, soggetti e decisioni*, Giappichelli, Torino, 2017, 50 ss..

prodromico provvedimento giurisdizionale, rammentando, in primo luogo, come la Direttiva preveda che la difesa possa far valere i mezzi di impugnazione disponibili presso lo Stato di esecuzione, in modo tale da impedire il riconoscimento dell'ordine ovvero la trasmissione della prova richiesta ovvero ancora la sua utilizzazione nel procedimento penale di destinazione[28]. D'altro canto, lo Stato di emissione deve consentire alla difesa di contestare la necessità e la regolarità dell'OEI[29]. Sul punto già le Sezioni unite avevano chiarito che nel silenzio della norma, la difesa deve potersi avvalere dei rimedi previsti dall'ordinamento nazionale per sottoporre a verifica il profilo dell'illegittimità dell'OEI[30].

6. L'utilizzabilità della prova digitale acquisita tramite OEI.

Con riguardo alla tematica degli effetti sul procedimento penale di destinazione, la Corte di cassazione, ha chiarito che, in linea generale, laddove risulti che l'attività di indagine svolta all'estero sulla base di un ordine illegittimo, perché emesso senza il necessario provvedimento del giudice, la genesi patologica della prova acquisita all'estero comporta l'inutilizzabilità della prova stessa. Ben più complessa risulta invece la questione delle conseguenze dell'illegittimità di un OEI emesso per acquisire prove già disponibili nello Stato di esecuzione. In questi casi, a prescindere dal fatto che la prova sia stata già trasmessa all'Autorità rogante, deve essere assicurata alla difesa la possibilità di poter verificare, attraverso i rimedi disponibili nella legislazione del paese di destinazione, la sussistenza delle condizioni di ammissibilità della prova. Laddove poi detta verifica non sia stata effettuata nel procedimento *a quo*, prima dell'emissione dell'OEI, può essere effettuata, incidentalmente, anche dal giudice del riesame. La Direttiva ha infatti lasciato spazi di discrezionalità nella valutazione dell'utilizzabilità della prova acquisita, affidando tale delicato compito allo Stato di emissione, che nell'effettuare tale valutazione, deve ad ogni modo assicurare i diritti della difesa

[28] In tema, Corte Giust. UE, 16 dicembre 2021, HP C-724/19 ha chiarito che è prerogativa della difesa far vagliare presso lo Stato di esecuzione la questione della competenza ad emettere l'atto di indagine richiesto. Sotto questo punto di vista assume rilevanza anche la possibilità di poter sorvegliare il rispetto delle *best practices* per l'acquisizione della prova digitale all'estero. In tema, G. COLAIOCCO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. pen. web.*, 1/2019, p. 9, sottolinea che il mancato rispetto delle *best practices* nell'acquisizione della prova mediante OEI e rogatoria, deve comportare l'inutilizzabilità della prova stessa. Sul punto C. CONTI, *La prova informatica e il mancato rispetto della best pratice: lineamenti sistematici sulle conseguenze processuali*, in A. Cadoppi, S. Canestrari, A. Manna, V. Papa (diretto da) *Cybercrime*, cit., p. 1337, evidenzia che «il contradditorio con la difesa – contestuale al momento dell'acquisizione – rappresenterebbe una formidabile garanzia di "controllabilità"».

[29] Corte giust. UE, 11 novembre 2021, Gavanozov, C-852-19.

[30] Cass. Pen., S.U., 16 aprile 2003, Monnier, n. 21420, Rv. 224184.

e le garanzie del giusto processo. È pertanto onere degli ordinamenti nazionali degli stati membri, in virtù del c.d. principio di autonomia procedurale, stabilire le modalità processuali dei ricorsi atti a garantire la tutela dei diritti spettanti ai singoli in forza del diritto eurounitario. Gli unici paletti sono rappresentati dal monito giurisprudenziale che richiede che dette modalità non siano meno garantite di quelle previste dal diritto interno per la gestione di situazioni analoghe; che non sia reso maggiormente difficoltoso l'esercizio dei diritti da parte dei singoli; ed evitando che informazioni ed elementi di prova ottenuti in modo illegittimo rechino pregiudizio a una persona sospettata di aver commesso un reato[31].

In questa prospettiva, il Supremo consesso ha evidenziato che per l'acquisizione dei risultati di un'intercettazione già effettuata all'estero, non è sufficiente che la prova in questione sia stata autorizzata dal giudice in ossequio alla normativa in vigore nello Stato in cui l'attività di indagine è stata eseguita, ma occorre un controllo – che non può che essere affidato al giudice dello Stato di emissione – sull'ammissibilità e sulla utilizzazione dell'intercettazione secondo la legislazione ivi vigente. Si tratta di quanto già era stato precedentemente espresso dal giudice di legittimità, allorquando veniva statuito che in materia di Ordine europeo d'indagine vige il principio di diritto (già espresso in tema di rogatoria internazionale), ai sensi del quale trovano applicazione, da un lato il principio "*locus regit actum*"; dall'altro, quello della prevalenza della "*lex loci*" sulla "*lex fori*" in conformità ai canoni di diritto internazionale [32], secondo cui l'atto è eseguito secondo le norme processuali dello Stato richiesto, a patto che detta attività non si ponga in contrasto con norme inderogabili e principi fondamentali, che, però, non si identificano necessariamente con il complesso delle regole dettate dal codice di rito[33]. In letteratura è stato però anche osservato che l'utilizzazione degli atti trasmessi da Autorità giudiziarie straniere, tanto più ove l'atto di indagine sia compiuto in precedenza, nel corso di investigazioni da quest'ultima autonomamente avviate, non possa essere condizionata, in forza del principio di reciproca fiducia, dall'accertamento da parte del giudice italiano della loro regolarità, vigendo, in *primis*, una presunzione di legittimità dell'attività svolta ed in secondo luogo, la verifica del giudice straniero circa la correttezza procedurale e l'eventuale risoluzione di ogni questione relativa alle irregolarità riscontrate[34].

[31] Corte Giust. UE, Grande Sez., 6 ottobre 2020, C-511/18.

[32] Cass. Pen., Sez. V, 18 maggio 2016, n. 26885, Rv. 267265.

[33] Sul punto, Cass. Pen., Sez. V, 13 luglio 2016, n. 45002, Rv. 268457. Precedentemente Cass. Pen., Sez. un., 25 febbraio 2010, Mills, n. 15208, Rv. 246583. In dottrina sul tema, R. KOSTORIS, *Ordine di investigazione europeo e tutela dei diritti fondamentali*, in *Cass. pen.*, 2018, pp. 1441 ss..

[34] Così A. RAMPIONI, *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali.*, in *Giuris. Pen. web*, 10/2023, p. 9. Sul punto L. FILIPPI, *Criptofonini e diritto di difesa*, in *Pen. Dir. Proc.*, 2/2023, p. 322, sottolinea che «si

In punto di diritto dell'imputato di poter conoscere e contestare il materiale probatorio utilizzato a proprio carico, la Suprema corte ha ritenuto che deve essere garantito il diritto della difesa di accesso alla prova anche se raccolta all'estero: nel caso in cui l'attività di messa in chiaro di messaggi criptati sia stata svolta all'estero dal fornitore del servizio fuori dal contraddittorio, la difesa, a pena di nullità ai sensi dell'art. 178, lett. c., c.p.p., ha diritto di ottenere la versione originale e criptata dei messaggi e le chiavi di sicurezza necessarie alla decriptazione[35]. Al riguardo, come chiarito dalla Corte EDU, per stabilire l'equità del processo, va verificato se e con quale modalità sia stata data all'imputato la opportunità di accedere alla prova decisiva ai fini della condanna.

In questa prospettiva, con riferimento ad un caso in cui era stata compresso il diritto della difesa in relazione a dati raccolti in un server di messaggistica crittografata, poiché non era stata consentita la verifica dei dati grezzi nel loro contenuto e nella loro integrità, la Corte EDU[36] ha affermato che, nonostante le prove elettroniche differiscano sotto molti aspetti dalle prove tradizionali, anche per quanto riguarda la loro natura e le tecnologie speciali richieste per la raccolta, conservazione, trattamento ed analisi, non vi è alcuna ragione per una applicazione differenziata delle garanzie previste dall'art. 6, par. 1, C.E.D.U. In quest'ottica il diritto ad un processo in contraddittorio presuppone che l'autorità inquirente riveli alla difesa tutte le prove, anche quelle elettroniche e non solo quelle che l'accusa ritiene rilevanti. Si tratta tuttavia di un diritto non assoluto, potendo rendersi necessario un suo bilanciamento con interessi concorrenti, quali la sicurezza nazionale o la necessità di mantenere segreti i metodi di indagine dei reati da parte della polizia. Ad ogni modo, la limitazione del diritto di difesa che si viene a creare deve essere controbilanciata da adeguate garanzie procedurali (tra le quali *in primis* la possibilità per l'imputato di aver potuto preparare la propria difesa in giudizio), da determinare alla luce dell'importanza del materiale non divulgato e del suo utilizzo nel processo.

Tornando alle casistiche giurisprudenziali al vaglio della Sesta sezione, la Corte, con riguardo all'ordinanza del Tribunale di Reggio Calabria, ha ritenuto censurabile la pronuncia gravata, sia in ordine alla qualificazione dell'atto richiesto con l'ordine europeo di indagine sia alla ritenuta sufficienza del controllo

tratta di presunzione (di legittimità del mezzo istruttorio assunto all'estero) di natura soltanto relativa, dal momento che ogni elemento di prova, che dovesse essere stato acquisito in violazione di un principio fondamentale o di una norma inderogabile dell'ordinamento interno al Paese d'emissione, deve essere considerato inutilizzabile ex art. 191 c.p.p. in quanto acquisito "in violazione dei divieti stabiliti dalla legge"».

[35] Sempre Cass. Pen., Sez. VI, 26 ottobre 2023, Iaria. In senso conforme, Cass. Pen., Sez. IV, 15 ottobre 2019, n. 49896, Rv. 277949.

[36] Corte EDU, Grande Camera, 26 settembre 2023, Yuksel Yal Onkaya c. Turchia.

effettuato dall'autorità giudiziaria francese sull'atto eseguito in Francia. Il Tribunale delle libertà reggino, in particolare, avrebbe dovuto attribuire alle attività di indagine svolte all'estero la corretta qualificazione giuridica ed avrebbe dovuto verificare, ai fini della utilizzabilità dei dati informativi, se sussistevano le condizioni per l'autorizzazione in sede giurisdizionale delle relative attività investigative oggetto dell'ordine europeo.

Per ciò che concerne invece l'operato del Tribunale di Milano, il Supremo consesso, oltre alle medesime criticità emerse ed evidenziate nell'ambito della vicenda calabrese, ha rilevato che dal provvedimento di merito in questione non è emerso se sia stata data alla difesa - che ha l'onere, nel caso di trasmissione di prova già autonomamente acquisita da un'autorità di altro Stato membro dell'Unione europea, di rivolgersi alle autorità di tale Stato - l'opportunità di ottenere la versione originale dei messaggi nonché i dati necessari per rendere intellegibili i messaggi criptati. Resta in ogni caso, onere della difesa, al pari di quel che avviene per il diritto di accesso alle registrazioni di intercettazioni, allegare di non aver potuto beneficiare di tali opportunità per contestare il materiale indiziario utilizzato a carico del ricorrente[37].

Vulnus motivazionali che hanno fatto propendere per l'annullamento delle ordinanze vergate dai due Tribunali del Riesame in questione, con rinvio alla fase rescissoria ove dette lacune dovrebbero essere colmate effettuando una "prova di resistenza", finalizzata a verificare se il rispetto dell'art. 273 c.p.p. possa considerarsi ugualmente garantito, in base ad ulteriori elementi di conoscenza legittimamente acquisiti.

7. La direzione indicata dalle Sezioni unite: finalmente verso soluzioni univoche?

La *ratio* sottesa ai principi di diritto enucleati dalla copiosa giurisprudenza analizzata è scopertamente quella di evitare che, sotto l'egida dell'ordine europeo di indagine, attività inquirenti presentate con le vesti di acquisizione di copia informatica di messaggistica criptata, eludano le disposizioni inderogabili in tema di sequestro e di intercettazioni. Ed infatti si è visto che, secondo la giurisprudenza di legittimità, l'acquisizione all'estero della messaggistica criptata sulla piattaforma SKY-ECC, mediante OEI, non costituisce dato informatico utilizzabile ai sensi dell'art. 234-*bis* c.p.p., *id est*, in tale ipotesi, l'attività acquisitiva, se riguardante comunicazioni avvenute nella fase "statica", deve essere inquadrata nelle disposizioni dettate in materia di perquisizione e sequestro e, in particolare, in quella prevista dall'art. 254-*bis* c.p.p., mentre se, avente ad oggetto

[37] Conformemente a quanto precedentemente statuito da Cass. Pen., Sez. II, 3 ottobre 2013, n. 43772, Rv. 257304.

comunicazioni avvenute nella fase "dinamica", deve essere inquadrata nella disciplina degli artt. 266 e ss. c.p.p., in materia di intercettazioni telematiche.

In questa contesto, in data 3 novembre 2023, la Terza Sezione penale ha rimesso alle Sezioni unite le seguenti questioni di diritto: da un lato, se, in tema di mezzi di prova, l'acquisizione mediante OEI di messaggi su chat di gruppo presso l'A.g. straniera che ne ha eseguito la decrittazione costituisca o meno acquisizione di "documenti e di dati informatici" ai sensi dell'art. 234-*bis* c.p.p. e, dall'altro, se 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 della A.G. nazionale.

Sul punto, in relazione al primo quesito, le Sezioni unite hanno affermato il principio di diritto secondo il quale il trasferimento di prove in questione rientra nella acquisizione di atti di un procedimento penale che, a seconda della loro natura, trova alternativamente il suo fondamento negli artt. 78 disp. att. c.p.p., 238, 270 c.p.p. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE. Mentre al secondo quesito è stata data risposta negativa, poiché rientra nei poteri del pubblico ministero quello di acquisire atti di altro procedimento penale. Infine, per quanto riguarda il terzo quesito, l'organo nomofilattico ha fornito risposta positiva esplicando che l'autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo.

D'altro canto, su di un'altra sfaccettatura della tematica, parzialmente sovrapponibile alla prima, è intervenuta una seconda ordinanza, questa volta della Sesta sezione[38], la quale chiedeva, da una parte, se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'autorità giudiziaria estera su una piattaforma informatica criptata integri, o meno, l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 c.p.p. e, dall'altra, se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'autorità giudiziaria estera attraverso l'inserimento di un captatore informatico sul *server* di una piattaforma criptata sia soggetta nell'ordinamento interno ad un controllo giurisdizionale, preventivo o successivo, in ordine alla utilizzabilità dei dati raccolti[39]. Le Sezioni unite, con informazione provvisoria diffusa al termine dell'udienza, hanno fornito risposta positiva al primo ed al terzo quesito e negativa al secondo.

[38] Sez. VI, con ord. 15.1.2024, n. 2329/2024, Giorgi e altri.

[39] Su questo tema, L. FILIPPI, *Le S.U. ammettono le prove francesi sui criptofonini acquisite con l'ordine europeo di indagine*, in *Pen. Dir. Proc.*, 01.03.2024, *passim*.

Sull'altro versante di interesse, la Corte di cassazione ha ritenuto invece che la questione della illegittima emissione dell'OEI da parte del Pubblico ministero italiano non può essere dedotta dinanzi al giudice italiano, nel caso in cui tale ordine sia stato emesso per acquisire una prova già disponibile nello Stato di esecuzione e la stessa sia stata definitivamente trasmessa da detto Stato. In questo caso la difesa può soltanto far valere la mancanza delle condizioni di ammissibilità della prova secondo l'ordinamento interno. Pertanto, l'utilizzabilità di prove acquisite all'estero mediante OEI è subordinata all'accertamento, da parte del giudice italiano, delle condizioni di ammissibilità dell'atto di indagine secondo le regole dell'ordinamento nazionale e del rispetto delle norme inderogabili e dei relativi principi fondamentali[40]; tra i quali risaltano, il principio di legalità processuale (art. 111, comma 1, Cost.), il diritto al contraddittorio per la prova (art. 111, comma 4, c.p.p.) e sulla prova (art. 111, comma 2, Cost.), il diritto di difesa (art. 24, comma 2, Cost.) e la libertà morale della persona nell'assunzione della prova (art. 188 c.p.p.). Epperò, per accertare che l'acquisizione delle prove digitali da parte dell'autorità giudiziaria di esecuzione sia stata rispettosa dei principi fondamentali e delle norme inderogabili del sistema normativo italiano è necessario conoscere le modalità di acquisizione per confrontarle con i principi fondamentali del sistema giuridico di riferimento. Infatti, il confronto tra le ragioni dell'accusa e le controdeduzioni della difesa può esplicarsi appieno, in conformità al principio del contraddittorio, nella misura in cui la dialettica procedimentale investa non solo le risultanze probatorie raccolte, ma pure il relativo procedimento di acquisizione[41]. Contraddittorio che, come noto, non verte solo sull'oggetto da provare, bensì anche su tutte le attività intese a farlo[42]. Sulla scorta delle considerazioni in diritto elaborate dalla giurisprudenza di legittimità, ne deriva che deve essere garantita quindi la facoltà per gli interessati di conoscere le modalità, le procedure e puntualmente ogni passaggio prodromico all'estrapolazione e all'acquisizione dei dati immagazzinati mediante OEI. Facoltà di "accesso generalizzato"[43] che segnatamente deve ricomprendere, tra le altre attività di "controllo", la possibilità di poter ottenere l'algoritmo impiegato per decrittare i flussi comunicativi captati o comunque sequestrati all'interno del server, unitamente alle stringhe informatiche non ancora decriptate. In assenza di questi dati,

[40] Su questa tematica, cfr. A. MANGIARACINA, *L'esecuzione dell'OEI e i margini nazionali di rifiuto*, in M. Daniele – R. Kostoris (a cura di) *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, cit., p. 128.

[41] Cass. Pen., Sez. IV, 15 luglio 2022, n. 32915, in *Guida dir.*, 2022, 38.

[42] G. CONSO, *Considerazioni in tema di contraddittorio nel processo penale italiano*, in *Riv. it. dir. e proc. pen.*, 1966, p. 405.

[43] N. GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo di Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero,* cit., 21.

infatti, non sarebbe possibile esercitare a pieno il diritto di difesa su un tema delicato quale è quello della piena corrispondenza tra il testo originario (la stringa informatica) e il testo intellegibile introdotto come prova nel giudizio. Diversamente opinando, non avrebbe alcun senso gravare la difesa dell'onere di allegare l'inesattezza di un giudizio di identità tra due dati, il giudizio che dovrebbe descrivere il rapporto che intercorre tra il testo introdotto in giudizio, da un lato e il risultato effettivamente ricavabile dalla stringa informatica una volta decriptata dall'altro, se contestualmente gli si nega la possibilità di conoscere sia il dato grezzo da comparare, e quindi la stringa informatica, sia lo strumento necessario per rendere quel dato idoneo alla comparazione e cioè l'algoritmo[44].

In conclusione: in attesa di un intervento normativo organico, la Suprema corte, pronuncia dopo pronuncia, sta tracciando un percorso nitido il cui punto di arrivo è rappresentato dallo stesso obbiettivo che deve essere condiviso dalle parti in gioco e cioè a dire quello di riuscire a controbilanciare la ricerca dell'efficienza della cooperazione giudiziaria nell'attività di raccolta delle prove, con l'osservanza di uno standard elevato di protezione dei diritti fondamentali. Tenendo presente che l'efficienza è un concetto di relazione che andrebbe sempre rapportato all'obiettivo che si vuole raggiungere e che quindi qualcosa può dirsi efficiente solo se si chiarisce quale è lo scopo da raggiungere[45]. In questo senso, nell'ottica di favorire la creazione di uno *ius commune* per la tutela dei diritti fondamentali, appare imprescindibile intensificare un'interlocuzione mirata tra le competenti autorità dei rispettivi Stati, nella fase in cui occorre valutare i presupposti di ammissibilità dell'atto richiesto, coinvolgendo puntualmente ed effettivamente la difesa, soprattutto laddove si tratti di un atto coercitivo e quindi maggiormente capace di incidere sulla posizione giuridica soggettiva di chi è - soltanto - sospettato di aver commesso un crimine[46].

[44] Su queste, e quelle immediatamente precedenti, efficacemente L. LUDOVICI, *I criptofonini: sistemi informatici criptati e server occulti*, in *www.penaledp.it*, 14 ottobre 2023. Su questo tema anche W. NOCERINO, *L'acquisizione della messaggistica su sistemi criptati: intercettazioni o prova documentale?*, in *Cass. pen*., 2023, pp. 1435 ss..

[45] O. MAZZA, *Il processo che verrà: dal cognitivismo garantista al decisionismo efficientista*, in *Arch. pen. web.*, 2/2022, p. 3.

[46] In questo senso A. MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale,* cit., 180. Di questo avviso anche, V. MANES – M. CAIANIELLO, *Introduzione al diritto penale europeo: fonti, metodi, istituti, casi,* Giappichelli, Torino, 2020, *passim*.; volendo N. GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo di Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero,* cit., p. 22.