

SP

SISTEMA
PENALE

FASCICOLO

4/2025

COMITATO EDITORIALE Giuseppe Amarelli, Roberto Bartoli, Hervè Belluta, Michele Caianiello, Massimo Ceresa-Gastaldo, Adolfo Ceretti, Cristiano Cupelli, Francesco D'Alessandro, Angela Della Bella, Gian Paolo Demuro, Emilio Dolcini, Novella Galantini, Mitja Gialuz, Glauco Giostra, Antonio Gullo, Stefano Manacorda, Vittorio Manes, Luca Masera, Anna Maria Maugeri, Melissa Miedico, Vincenzo Mongillo, Francesco Mucciarelli, Claudia Pecorella, Marco Pelissero, Lucia Riscato, Marco Scoletta, Carlo Sotis, Costantino Visconti.

COMITATO SCIENTIFICO (REVISORI) Andrea Abbagnano Trione, Alberto Alessandri, Silvia Allegrezza, Chiara Amalfitano, Enrico Mario Ambrosetti, Ennio Amodio, Gastone Andrezza, Ercole Aprile, Giuliano Balbi, Marta Bargis, Enrico Basile, Fabio Basile, Alessandra Bassi, Teresa Bene, Carlo Benussi, Alessandro Bernardi, Marta Bertolino, Francesca Biondi, Rocco Blaiotta, Manfredi Bontempelli, Carlo Bonzano, Matilde Brancaccio, Carlo Bray, Renato Bricchetti, David Brunelli, Carlo Brusco, Silvia Buzzelli, Alberto Cadoppi, Lucio Camaldo, Gaia Caneschi, Stefano Canestrari, Giovanni Canzio, Francesco Caprioli, Matteo Caputo, Fabio Salvatore Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Francesco Centonze, Federico Consulich, Carlotta Conti, Stefano Corbetta, Roberto Cornelli, Fabrizio D'Arcangelo, Marcello Daniele, Gaetano De Amicis, Cristina De Maglie, Alberto De Vita, Jacopo Della Torre, Ombretta Di Giovine, Gabriella Di Paolo, Giandomenico Dodaro, Massimo Donini, Salvatore Dovere, Tomaso Emilio Epidendio, Luciano Eusebi, Riccardo Ferrante, Giovanni Fiandaca, Giorgio Fidelbo, Stefano Finocchiaro, Carlo Fiorio, Roberto Flor, Luigi Foffani, Dèsirèe Fondaroli, Gabriele Fornasari, Gabrio Forti, Piero Gaeta, Alessandra Galluccio, Marco Gambardella, Alberto Gargani, Loredana Garlati, Giovanni Grasso, Giulio Illuminati, Gaetano Insolera, Roberto E. Kostoris, Giorgio Lattanzi, Sergio Lorusso, Ernesto Lupo, Raffaello Magi, Vincenzo Maiello, Adelmo Manna, Grazia Mannozi, Marco Mantovani, Luca Marafioti, Enrico Marzaduri, Maria Novella Masullo, Oliviero Mazza, Francesco Mazzacuva, Claudia Mazzucato, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Andrea Montagni, Gaetana Morgante, Lorenzo Natali, Renzo Orlandi, Luigi Orsi, Francesco Palazzo, Carlo Enrico Paliero, Lucia Parlato, Annamaria Peccioli, Chiara Perini, Lorenzo Picotti, Carlo Piergallini, Paolo Pisa, Luca Pistorelli, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Serena Quattrocchio, Tommaso Rafaraci, Paolo Renon, Maurizio Romanelli, Bartolomeo Romano, Gioacchino Romeo, Alessandra Rossi, Carlo Ruga Riva, Francesca Ruggieri, Elisa Scaroina, Laura Scomparin, Nicola Selvaggi, Sergio Seminara, Paola Severino, Rosaria Sicurella, Piero Silvestri, Fabrizio Siracusano, Nicola Triggiani, Andrea Francesco Tripodi, Giulio Ubertis, Maria Chiara Ubiali, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, Francesco Viganò, Daniela Vigoni, Francesco Zacchè, Stefano Zirulia.

REDAZIONE Francesco Lazzeri, Giulia Mentasti (coordinatori), Dario Albanese, Enrico Andolfatto, Silvia Bernardi, Patrizia Brambilla, Pietro Chiaraviglio, Beatrice Fragasso, Elisa Grisonich, Alessandro Malacarne, Cecilia Pagella, Emmanuele Penco, Gabriele Pontepino, Sara Prandi, Tommaso Trinchera.

Sistema penale (SP) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.

La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La *Rivista* si uniforma agli standard internazionali definiti dal *Committee on Publication Ethics* (COPE) e fa proprie le relative linee guida.

I materiali pubblicati su *Sistema Penale* sono oggetto di licenza CC BY-NC-ND 4.00 International. Il lettore può riprodurli e condividerli, in tutto o in parte, con ogni mezzo di comunicazione e segnalazione anche tramite collegamento ipertestuale, con qualsiasi mezzo, supporto e formato, per qualsiasi scopo lecito e non commerciale, conservando l'indicazione del nome dell'autore, del titolo del contributo, della fonte, del logo e del formato grafico originale (salve le modifiche tecnicamente indispensabili). La licenza è consultabile su <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

Peer review I contributi che la direzione ritiene di destinare alla sezione "Articoli" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "Altri contributi" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.

Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2023, p. 5 ss.

ANCORA IN MATERIA DI ESECUZIONE DELL'ORDINE EUROPEO D'INDAGINE (OEI) TRA FORMAZIONE DELLA PROVA E SORVEGLIANZA DI MASSA: DUE QUESTIONI APERTE

di Teresa Russo

Il presente contributo intende ragionare sulle questioni emerse in sede di esecuzione dell'Ordine Europeo d'Indagine (OEI), con specifico riferimento a prove già acquisite dall'autorità dello Stato di esecuzione ed aventi ad oggetto dati decrittografati, nonché evidenziare la tensione tra la ritualità della formazione della prova negli ordinamenti processuali nazionali, la circolazione e l'utilizzabilità dei risultati probatori, le garanzie di tutela dei diritti degli indagati ed imputati e le esigenze delle indagini penali nella lotta alla criminalità di "piattaforme digitali".

SOMMARIO: 1. Considerazioni introduttive sull'OEI e sulle prime questioni sorte nella sua esecuzione. – 2. L'emersione di ulteriori questioni: la formazione della prova e la sua utilizzabilità nei processi penali con specifico riferimento ai dati decrittati. – 3. La decisione della Corte di giustizia nel caso *M.N. (EncroChat)* sull'acquisizione di prove già in possesso dell'autorità di esecuzione ed il rimando agli ordinamenti processuali nazionali. – 4. La sottesa questione della sorveglianza di massa nell'intercettazione dei dati. – 5. Conclusioni aperte tra "adattabilità" del regime probatorio in assenza di armonizzazione e finalità di accertamento dei reati: quale preminenza per le esigenze delle indagini penali?

1. Considerazioni introduttive sull'OEI e sulle prime questioni sorte nella sua esecuzione.

Sin dal momento della sua adozione l'ordine europeo d'indagine (OEI)¹ ha inteso affrontare alcune questioni che gli altri strumenti di cooperazione giudiziaria europea

¹ Come è noto, introdotto dalla direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014, un OEI è una decisione giudiziaria emessa o convalidata da un'autorità giudiziaria di uno Stato membro («lo Stato di emissione») per far eseguire una o più misure investigative specifiche in un altro Stato membro («lo Stato di esecuzione») ai fini di acquisire prove (art.1). L'OEI può essere emesso anche per ottenere prove che sono già in possesso delle autorità competenti dello Stato di esecuzione, per la raccolta di informazioni su conti bancari e altri conti finanziari, per audizioni tramite videoconferenza di testimoni e persone sotto inchiesta. Un OEI può essere rifiutato solo al ricorrere di determinati motivi di cui all'art. 11 della direttiva: tra gli altri, per la tutela di interessi essenziali di sicurezza nazionale, contrarietà al principio *ne bis in idem*, o allorquando sussistano seri motivi per ritenere che l'esecuzione dell'atto di indagine richiesto nell'OEI sia incompatibile con gli obblighi dello Stato di esecuzione ai sensi dell'art. 6 TUE e della Carta dei diritti fondamentali. Al di fuori dell'elenco delle ipotesi tipizzate, gli Stati membri sono tenuti a riconoscere ed eseguire un OEI tempestivamente, entro il termine di trenta giorni (art. 12) e senza formalità aggiuntive. La direttiva stabilisce, inoltre, scadenze per l'ottenimento delle prove necessarie, oltre a contenere moduli standard per la compilazione di un OEI (allegato A), per la conferma di ricezione (allegato B) e per la notifica

avevano lasciato alla determinazione di ciascun Stato membro secondo il proprio diritto interno², richiedendo per la loro emissione la convalida da parte del giudice³. Invece, la direttiva OEI introduce una procedura di convalida *ad hoc*, subordinata alla verifica della sussistenza delle condizioni di emissione (proporzionalità ed equivalenza), di cui all'art. 6, par. 1, da parte dell'autorità di emissione che, ai sensi dell'art. 2, par. 1, nn. i) e ii), può essere un giudice, un organo giurisdizionale, un magistrato inquirente, un pubblico ministero o qualsiasi altra autorità competente, definita dallo Stato di emissione, che agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità al diritto nazionale. Tanto è stato inteso come diretto ad evitare un conflitto tra il reciproco riconoscimento da un lato e gli standard nazionali costituzionali, qualora più elevati⁴. Ed infatti, già dalle prime

a un altro Stato membro di un'intercettazione di telecomunicazioni sul suo territorio (allegato C). Essa include anche una serie di garanzie per proteggere i diritti della difesa, in particolare nell'art. 1, parr. 3-4, e artt. 6 e 14. In generale sull'OEI, cfr., tra gli altri, C. HEARD – D. MANSELL, *The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases*, in *New Journal of European Criminal Law*, vol. 2, n. 4, 2011, pp. 353-367; S. ALLEGREZZA, *Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality*, in S. RUGGERI (ed.), *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Cham, 2014, pp. 51-77; E. DE CAPITANI – S. PEERS, *The European Investigation Order: A New Approach to Mutual Recognition in Criminal Matters*, in *EU Law Analysis*, 23 marzo 2014; A. MANGIARACINA, *A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order*, in *Utrecht Law Review*, vol. 10, n. 1, 2014, pp. 113-133; I. ARMADA, *The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?*, in *New Journal of European Criminal Law*, vol. 6, n. 1, 2015, pp. 8-31; R. BELFIORE, *The European Investigation Order in Criminal Matters: Developments in Evidence-Gathering Across the EU*, in *European Criminal Law Review*, vol. 5, n. 3, 2015, pp. 312-324; M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Processo penale e giustizia*, n. 3, 2015, pp. 1-11; T. BENE – L. LUPARIA – L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2016; M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017*, in *Diritto Penale Contemporaneo*, 28 luglio 2017; 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*, Torino, 2018; F. SIRACUSANO, *The European Investigation Order for Evidence Gathering Abroad*, in T. RAFARACI – R. BELFIORE (eds.), *EU Criminal Justice. EU Criminal Justice Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019, pp. 85-101; M.A. BIASOTTI – F. TURCHI (eds.), *European Investigation Order*, Berlino, 2023.

² Si pensi all'art. 6 della decisione 2002/584/GAI: Decisione quadro del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati; o, ancor prima, alla Convenzione stabilita dal Consiglio conformemente all'articolo 34 del trattato sull'Unione europea, relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, come completamento dell'applicazione della convenzione del Consiglio d'Europa sull'assistenza giudiziaria in materia penale del 1959 e il suo protocollo del 1978, che rimette ancora una volta agli Stati membri la determinazione dell'autorità giudiziaria competente (art. 24).

³ Tant'è vero che la delega dell'autorità giudiziaria alle agenzie di polizia in alcuni Stati membri aveva già comportato l'aggiunta di uno specifico motivo di rifiuto. Si veda la decisione quadro 2008/978/GAI sul mandato europeo di ricerca delle prove, sebbene non più in vigore (art. 11, parr. 4 e 5 in combinato disposto con l'art. 13).

⁴ In questi termini, A. ERBEŽNIK, *A New EU System on Cross-Border Gathering of E-Evidence – Analysis and Open Questions*, in *Dignitas*, n. 98, 2023, p. 65 ss., che riflette su, quella che chiama, problematica asimmetria tra gli Stati membri relativamente al ruolo dei pubblici ministeri. L'A. ritiene, invece, che il controllo

applicazioni, la Corte di giustizia è stata chiamata a chiarire le nozioni di «autorità giudiziaria» e di «autorità di emissione»⁵, ai sensi dell'art. 1, par. 1, e dell'art. 2, lett. c), che includono il pubblico ministero di uno Stato membro o, più in generale, la procura di uno Stato membro, indipendentemente da qualsiasi rapporto di subordinazione giuridica che possa esistere tra il pubblico ministero o la procura e l'esecutivo dello Stato membro, e dall'esposizione del pubblico ministero o della procura al rischio di essere soggetti, direttamente o indirettamente, a ordini o istruzioni individuali dell'esecutivo quando adottano un OEI. Tale statuizione è anche il frutto di un ragionamento in cui la Corte effettua una comparazione con la previsione dell'art. 6, par.1 della decisione quadro sul mandato d'arresto europeo, che utilizza la nozione di «autorità giudiziaria emittente» senza ulteriori specificazioni, evidenziando le differenze tra i due strumenti⁶. Tuttavia, successivamente, la Corte ha avuto modo di precisare che, nella fase istruttoria del procedimento penale, l'emissione di un OEI finalizzato all'acquisizione di dati relativi al traffico e all'ubicazione connessi alle telecomunicazioni, non può essere emesso dal pubblico ministero allorché, nell'ambito di una procedura nazionale analoga, l'adozione di un atto di indagine per l'accesso a siffatti dati rientri nella competenza esclusiva del giudice⁷. Nella sostanza, non ci sarebbe "uguaglianza" nelle

giurisdizionale sia fondamentale atteso il potenziale pericolo di abusi da parte delle forze dell'ordine nelle intrusioni nella privacy soprattutto a fronte delle nuove possibilità offerte dalle tecnologiche moderne.

⁵ Cfr. Corte giust., sent. 8.12.2020, *Staatsanwaltschaft Wien*, C-584/19 PPU, su cui v. A. GAUDIERI, *Conformità del rapporto di subordinazione del pubblico ministero con la direttiva 2014/41/UE: l'orientamento adottato dalla Corte di giustizia nella sentenza A. e A.*, in *slsg.unisa.it*, dicembre 2020.

⁶ Cfr. la sentenza della Corte giustizia nel *Staatsanwaltschaft Wien* (punto 75). Più nello specifico, la Corte rileva che i due strumenti (OEI e MAE) presentano differenze di ordine testuale, contestuale e teleologico (punto 74) e, sebbene riconosca che anche gli atti di indagine possono essere intrusivi, in quanto ledono il diritto alla vita privata o il diritto di proprietà delle persone interessate, ritiene che l'OEI, a differenza di un mandato d'arresto europeo, non è atto a ledere il diritto alla libertà della persona interessata, sancito all'articolo 6 della Carta (punto 73). Inoltre, l'OEI sarebbe assistito sia nella fase di emissione che di esecuzione da un insieme di garanzie al fine di assicurare la tutela dei diritti fondamentali delle persone interessate (punto 69). Per una sorta di "gradazione" dell'impatto sui diritti fondamentali da parte dei due strumenti, si rimanda alle considerazioni dell'Avvocato generale Campos Sánchez-Bordona nelle sue conclusioni del 16 luglio 2020, laddove afferma che «... la decisione quadro 2002/584 e la direttiva 2014/41 obbediscono a logiche che non coincidono: la decisione quadro 2002/584 incide sul diritto che può essere più intensamente colpito dall'azione pubblica di repressione dell'attività criminale. L'oggetto immediato e diretto del MAE è la privazione della libertà di una persona allo scopo di consegnarla a un altro Stato membro, nel quale dovrà scontare una pena o partecipare a un processo penale. Tale libertà è una di quelle riconosciute dalla Carta (articolo 6) e, pertanto, deve potersi avvalere della debita protezione giurisdizionale (articolo 47). La direttiva 2014/41 insiste, naturalmente, sulla tutela dei diritti fondamentali e dei diritti processuali della persona interessata (indagato o imputato) dagli atti d'indagine. Ma, sebbene alcuni di tali atti possano, a loro volta, tradursi in una limitazione di un diritto fondamentale, nessuno di essi ha l'intensità di un MAE. Gli OEI devono ovviamente essere istruiti nel rispetto dei diritti fondamentali, ma ciò non significa, di per sé, che tali diritti vengano sempre limitati, da qualunque atto autorizzato» (punto 69). Si segnala, tuttavia, che la Corte di giustizia è recentemente ritornata *per incidens* sulla distinzione tra MAE e OEI, delimitando *ratione materiae* l'ambito di applicazione dell'OEI e la nozione di atti d'indagine, e escludendo che un OEI, fatte salve le eccezioni degli artt. 22 e 23 della direttiva 2014/41, possa contenere una richiesta diretta a collocare o a trattenere in custodia la persona oggetto di un procedimento penale. In questo senso, cfr. Corte giust., sent. 9 gennaio 2025, *Delda*, C-583/23 (punto 40).

⁷ V. Corte giust., sent. 16.12.2021, *Procedimento penale a carico di HP*, Causa C-724/19, punto 42.

condizioni di emissione, anche in conformità alle considerazioni più garantiste espresse, in materia di accesso ai dati relativi alle comunicazioni elettroniche, nell'ormai famosa sentenza *Prokuratuur*⁸.

Come è noto, infatti, ai sensi dell'art. 6, par. 1, un OEI può essere emesso solamente se: (a) è necessario e proporzionato ai fini dei procedimenti penali di cui all'art. 4 della direttiva, tenendo conto dei diritti dell'imputato o della persona sottoposta a indagine; e (b) l'atto o gli atti di indagine richiesti avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo. Ne consegue che l'autorità di emissione è chiamata a valutare caso per caso (par. 2) la sussistenza dei requisiti di proporzionalità degli atti di indagine ed equivalenza di tali atti nel diritto nazionale, anche dal punto di vista dell'obbligo del rispetto dei diritti fondamentali e dei principi di cui all'art. 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale (art. 1, par. 4)⁹. Così, nella prima pronuncia pregiudiziale nel caso *Gavanozov I*, la Corte di giustizia si concentra sulle modalità di compilazione della sezione J (mezzi di impugnazione) del modulo dell'allegato A alla direttiva 2014/41, con un approccio diretto a consentire all'autorità di esecuzione di adottare la decisione sul riconoscimento dell'OEI e di compiere l'atto di indagine richiesto entro i termini previsti dall'art. 12 della direttiva¹⁰. Nella successiva decisione sempre nel caso *Gavanozov II*, la Corte, però, non può far a meno di affermare che l'assenza dei mezzi di impugnazione appropriati che consentano, da un lato, di contestare la regolarità e la necessità di un OEI, avente ad oggetto nella specie lo svolgimento di perquisizioni e di sequestri, nonché l'organizzazione di un'audizione di testimoni mediante videoconferenza e, dall'altro di chiedere un adeguato rimedio qualora tali misure siano state disposte o eseguite illegalmente, costituisce una violazione del diritto ad un ricorso effettivo di cui all'art.

⁸ Cfr. Corte giust., sent. 2.03.2021, *Prokuratuur*, Causa C-746/18, punto 59.

⁹ Secondo M. CAIANIELLO, cit., p. 6, dal momento che entrambe le autorità giudiziarie devono effettuare separatamente lo stesso controllo in materia di proporzionalità, provvedendo anche a consultarsi in caso di contrasto si assisterebbe ad una deroga al mutuo riconoscimento. Per ulteriori considerazioni critiche sul rispetto del principio di proporzionalità nell'emissione dell'OEI v. L. SCOMPARIN – A. CABIALE, *The Proportionality Test in Directive 2014/41/EU: Present and Future of a Fundamental Principle*, in *Eurojus*, n. 2, 2022, pp. 72-86. In generale, v. anche L. BACHMAIER WINTER, *The Role of the Proportionality Principle in Cross-Border Investigations Involving Fundamental Rights*, in S. RUGGERI (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings. A Study in Memory of Vittorio Grevi and Giovanni Tranchina*, Berlino, 2013, pp. 85-103.

¹⁰ Cfr. Corte giust., sent. 24.10.2019, *Procedimento penale a carico di Ivan Gavanozov*, Causa C-324/17 in cui, non essendo ancora stato emesso l'OEI, a causa delle difficoltà riscontrate nella compilazione del modulo da parte del giudice del rinvio, la Corte pone l'accento sulla piena realizzazione dell'obiettivo perseguito dalla direttiva – consistente nel facilitare e accelerare la cooperazione giudiziaria tra gli Stati membri sulla base dei principi di fiducia e di riconoscimento reciproci – e corroborata dall'art. 14, par. 5, il quale prevede che l'autorità di emissione e l'autorità di esecuzione si informano reciprocamente sui mezzi di impugnazione contro l'emissione, il riconoscimento o l'esecuzione di un OEI. La Corte, infatti, non entra nel merito dell'assenza dei mezzi di impugnazione nel diritto nazionale, richiesti dalla direttiva (art. 14), e, viceversa, sollevata dal giudice bulgaro ed evidenziata dall'Avvocato generale Bot nelle sue conclusioni dell'11 aprile 2019 (punti 51 ss., in part. punti 83-87). In generale, cfr. C. DE LUCA, *La prima pronuncia della Corte di giustizia sull'ordine europeo d'indagine penale: un approccio formale diretto a favorire l'efficacia della cooperazione giudiziaria*, in *Cassazione penale*, vol. 60, n. 10, 2020, pp. 3854-3863.

47 della Carta e all'art. 13 CEDU¹¹. Inoltre, concretizzando tale violazione, come ribadito dall'Avvocato generale Bobek, un'ipotesi di rifiuto dello Stato membro di esecuzione conformemente all'art. 11, par. 1, lett. f), l'OEI stesso non è compatibile con i principi di fiducia reciproca e di leale cooperazione¹².

Al di là di queste pronunce, come era immaginabile, altre questioni sono emerse in sede di esecuzione dell'OEI derivanti, in parte dal testo della direttiva stessa, e in parte, come si cercherà di dimostrare, da una sorta di "adattabilità" dei sistemi processuali nazionali in nome della circolazione delle prove tra procedimenti penali ed in assenza di un'armonizzazione, anche minima, in materia¹³. Le conclusioni evidenzieranno, infatti, una preminenza delle attività investigative di accertamento dei reati condotte dalle autorità di polizia e giudiziarie nazionali, con un *favor* per l'utilizzabilità dei risultati degli atti d'indagine nei confronti di "categorie" di indagati non identificati (nella specie utenti di piattaforme digitali) e senza la sussistenza di indizi concreti di reato grave a carico di ciascun di loro.

¹¹ La questione dell'assenza dei mezzi di impugnazione evidentemente si ripropone e diventa oggetto della pronuncia della Corte giust., sent. 11.11.2021, *Procedimento penale nei confronti di Ivan Gavanozov*, Causa C-852/19 su cui cfr. I. SZIJÁRTÓ, *The Implications of the European Investigation Order for the Protection of Fundamental Rights in Europe and the Role of the CJEU*, in *Pécs Journal of International and European Law*, n. 1, 2021, pp. 66-72; A. HERNANDEZ WEISS, *Effective Protection of Rights as a Precondition to Mutual Recognition: Some Thoughts on the CJEU's Gavanozov II Decision: Case C-852/19, Ivan Gavanozov II*, in *New Journal of European Criminal Law*, vol. 13, n. 2, 2022, pp. 180-197; A. MARTÍNEZ SANTOS, *Emisión de órdenes europeas de investigación por el Ministerio Fiscal español? Consideraciones sobre la compatibilidad del art. 13.4 de la Ley de reconocimiento mutuo con el derecho de la Unión a la luz de las Sentencias del TJUE en los Asuntos Gavanozov I y II*, in *Revista General de Derecho Europeo*, vol. 57, 2022, pp. 272-317; J. TRIBOUT, *Coopération judiciaire en matière pénale – Décision d'enquête pénale européenne*, in *Europe*, vol. 12, 2022; M.S. BARATA, *Case C-852/19, Gavanozov II: European Investigation Order and the Right to an Effective Remedy in the CFREU*, in *Revista Jurídica Portucalense*, vol. 34, 2023, pp. 186-203; E. GOTOVUSA, *The CJEU Ruling on Cases Gavanozov I and Gavanozov II*, in *Regional Law Review*, 2023, pp. 117-131.

¹² Cfr. le conclusioni dell'Avvocato generale Michal Bobek del 29 aprile 2021, punti 81-84, già precedentemente espresse dall'Avvocato Generale Bot. V. *supra* nota 9.

¹³ Trattasi di una questione che la dottrina ha da tempo evidenziato e che viene considerata come una limitazione alla realizzazione piena del mutuo riconoscimento in ambito probatorio. In questo senso, Cfr. S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo*, in T. RAFARACI (a cura di), *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio tra priorità repressive ed esigenze di garanzia*, Milano, 2007, p. 708 ss.; ID., *L'armonizzazione della prova europea alla luce del Trattato di Lisbona*, *Cassazione Penale*, vol. 48, n. 10, 2008, pp. 3882-3893. Inoltre, come è stato rilevato, S. RAGAZZI – F. SPIEZIA, [Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano](#), in questa *Rivista*, n. 2, 2024, p. 225, «permane una oggettiva e fisiologica divergenza tra ordinamenti anche sul piano degli istituti processuali penali, mentre non è stata ancora adottata (né in seno alla direttiva OIE né in seguito) una sorta di tavola dei principi generali condivisi, ossia di più specifiche disposizioni calibrate sulle diverse tipologie di prova».

2. L'emersione di ulteriori questioni: la formazione della prova e la sua utilizzabilità nei processi penali con specifico riferimento ai dati decriptati.

Non è tardata, infatti, a (ri-)presentarsi la questione relativa alla formazione (raccolta) della prova che il testo della direttiva non affronta. Invero, la summenzionata assenza di armonizzazione delle discipline probatorie nazionali pone alla raccolta transnazionale della prova, innanzitutto, un problema di disciplina applicabile (*lex loci* o *lex fori*) e di conseguenza un problema relativo alla sua utilizzabilità in un procedimento penale in corso¹⁴. Quanto alla prima questione, l'art. 9, par. 2 della direttiva OEI precisa che l'autorità di esecuzione si attiene alle formalità e alle procedure espressamente indicate dall'autorità di emissione, salvo che non disponga diversamente e sempre che tali formalità e procedure non siano in conflitto con i principi fondamentali del diritto dello Stato di esecuzione¹⁵. C'è in questa previsione un rapporto di mutua assistenza tra le due autorità di emissione e di esecuzione per assicurare l'utilizzabilità del risultato probatorio¹⁶. Tuttavia, la direttiva non chiarisce se la richiamata verifica dell'autorità di emissione, in particolare delle condizioni interne, debba riguardare solo l'atto di indagine richiesto o debba tenere conto anche delle specifiche procedure di indagine che lo Stato di esecuzione ha posto in essere¹⁷. Tanto, a maggior ragione, quando un OEI viene emesso per ottenere prove già in possesso delle autorità competenti dello Stato di esecuzione in modo da bypassare del tutto la suddetta verifica "istruttoria" sulla ritualità dell'acquisizione. Il principio di mutuo riconoscimento impedisce, infatti, all'autorità giurisdizionale di emissione di sindacare la legittimità del procedimento di formazione della prova nello Stato di esecuzione, sia pur, come si vedrà, senza poter derogare alle garanzie processuali previste dal proprio ordinamento a presidio della tutela dei diritti fondamentali dei soggetti indagati o imputati.

Tale questione è emersa, in particolare, nell'acquisizione e nello scambio di dati decrittografati¹⁸ nell'ormai noto caso *EncroChat* in cui le autorità coinvolte erano riuscite

¹⁴ Sul punto, cfr. già G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA (a cura di), *Liber Amicorum per Massimo Panebianco*, Napoli, 2020, pp. 991-1016.

¹⁵ «Ne consegue una prevalenza dello Stato di emissione volta ad assicurare la spendita del "risultato" probatorio raccolto *ultra fines*, [per cui] si prevede espressamente la possibilità che la prova sia confezionata dall'autorità di esecuzione secondo le "indicazioni" formali e procedurali richieste dall'autorità emittente, con sostanziale prevalenza della *lex fori*». Così, G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, in *PenaleDP*, n. 2, 2024, p. 270.

¹⁶ Si tratterebbe di una soluzione normativa ibrida tra mutuo riconoscimento e mutua assistenza. In questo senso, cfr. ancora M. CAIANIELLO, cit., p. 3.

¹⁷ Cfr. F. LIGUORI, *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, in *Quaderni AISDUE*, n. 1, 2024, pp. 1-25.

¹⁸ Sul punto, v. le considerazioni M. KOOMEN, *The Encryption Debate in the European Union*, in *Carnegie*, 30 maggio 2019; ID., *The Encryption Debate in the European Union: 2021 Update*, in *Carnegie*, 31 marzo 2021. Più in generale, sull'evoluzione delle indagini penali, cfr., tra gli altri, M. DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Processo Penale e Giustizia*, n. 5, 2018, pp. 831-837; S.

ad hackerare i server e gli smartphone e a decriptare il linguaggio degli utenti di questa piattaforma¹⁹. Tali attività investigative, condotte principalmente dalle autorità francesi, anche nell'ambito di una *joint investigation team*, consentivano l'accesso ad un notevole ammontare di informazioni che le autorità inquirenti di diversi paesi europei provvedevano a richiedere emettendo, appunto, vari OEI. A fronte della decisione di apporre il «*secret de la défense nationale*», ex artt. da 230-1 a 230-5 e 706-102-1 del codice di procedura penale francese sulle modalità di acquisizione di tali informazioni²⁰, i difensori degli intercettati coinvolti in procedimenti penali nei diversi Paesi europei sollevavano la questione relativa alla verifica della "legalità" delle attività svolte in Francia ed alla loro attendibilità e affidabilità, tale da incidere sul diritto di difesa e, in particolare, sul contraddittorio relativo alle modalità di formazione della prova²¹. Il metodo di acquisizione dei dati, non conoscibile per gli imputati, è diventato così impossibile da contestare per le parti. Ciononostante, alcune corte nazionali,

SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018; e, più recentemente, L. BACHMAIER WINTER, S. RUGGERI (eds.), *Preventing and Investigating Crime in the Digital Era*, Cham, 2022.

¹⁹ Per maggiori informazioni sull'operazione si rinvia al *Europol/Eurojust Joint Press Release* consultabile al seguente link <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe#empact>, nonché alla Relazione annuale 2020 di Eurojust (sezione 7.2) consultabile al seguente indirizzo <https://www.eurojust.europa.eu/sites/default/files/assets/ar2020-it.pdf> e ancora al *First Report on Encryption by the EU Innovation Hub for Internal Security*, consultabile al seguente indirizzo [https://www.europol.europa.eu/cms/sites/default/files/documents/EU Innovation Hub First%20Report%20on%20Encryption.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/EU%20Innovation%20Hub%20Report%20on%20Encryption.pdf).

²⁰ Su tale questione, la Corte costituzionale francese (*Décision* 8.4.2022, n. 2022-987 QPC), su richiesta della Corte di Cassazione, stabiliva che le disposizioni del codice di procedura penale, che consentono agli investigatori di porre informazioni tecniche sotto il segreto di difesa nazionale, non violassero i diritti degli imputati a un ricorso giurisdizionale effettivo, il loro diritto alla privacy, la libertà di espressione o altri diritti garantiti dalla Costituzione, in quanto sussiste una «*conciliation équilibrée*», perseguendo tali disposizioni l'obiettivo di valore costituzionale della ricerca degli autori di reati e attuando esigenze costituzionali di tutela degli interessi fondamentali dello Stato. In seguito, la Corte di Cassazione, ritenendo che non fosse stata adeguatamente affrontata l'assenza di un certificato di convalida dei risultati delle operazioni, annullava parzialmente la decisione contestata della Corte d'appello di Nancy e rinviava il caso alla Corte d'appello di Metz per una nuova sentenza. Analogamente, annullava parzialmente un'altra decisione contestata sempre della Corte d'appello di Nancy rinviandola alla Corte d'appello di Parigi (Corte cass. francese, Camera penale, sent. 11.10.2022, ric. n. 21-85.148). Tuttavia, come è stato evidenziato la Corte di Cassazione francese si è limitata a rilevare un mero errore procedurale relativo ad un certificato richiesto dalla legge francese, escludendo così la questione dell'affidabilità dei dati. Qualsiasi conclusione del genere avrebbe, infatti, inciso sull'ammissibilità dei dati *EncroChat* in tutta Europa. In tal senso, cfr. H. DICKINSON, *The Latest EncroChat ruling from the French 'Supreme Court'*, in *Bedfordrow*, 2022.

²¹ Secondo l'*open letter* dell'ONG *Fair Trails*, consultabile al seguente indirizzo https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf, l'infiltrazione di *EncroChat* avrebbe rivelato tendenze preoccupanti con riferimento al diritto al giusto processo, alla mancanza di trasparenza, agli effetti extraterritoriali, alle implicazioni sulla privacy. V., già in passato, D. CIMADOMO, *Ordine europeo di indagine penale e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, in T. BENE – L. LUPARIA – L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2016, pp. 219-236.

specificamente olandese²² e tedesca²³, con ragionamenti logico-giuridici in parte simili, hanno concluso per l'utilizzabilità dei dati nei processi pendenti. Analogamente, le

²² Così, la Corte Suprema dei Paesi Bassi fa leva sul principio di mutua fiducia, ritenendo che la valutazione fatta dal giudice d'emissione sulla utilizzabilità della prova acquisita in regime di OEI è per lo più "ideale". Salvo, infatti, concreti indizi contrari, la Corte olandese ritiene che non si può fare a meno di constatare la legittimità della prova straniera con una evidente riduzione dello spazio di convincimento concesso alla difesa. Essa sostiene, infatti, che il diritto alla conoscenza delle prove non sia un diritto assoluto, dovendo essere temperato con gli eventuali interessi concorrenti: in particolare, la sicurezza nazionale e la segretezza dei metodi di indagine della polizia giudiziaria (Corte Suprema dei Paesi Bassi, sent. 13.6.2023, n. 913). La posizione della Corte olandese è stata, però, particolarmente criticata. La sentenza avrebbe «subordinato l'ordinamento processuale non allo Stato di diritto ma alla ragion di Stato, mortificando i diritti dell'imputato, a favore del principio di fiducia interstatale». In questo senso, cfr. R. DE VITA – M. DELLA BRUNA, *Corte Suprema dei Paesi Bassi: utilizzabilità all'estero dei dati Sky-ECC e Encrochat*, in *DeVitaLaw*, 23 luglio 2023. Ancora, alcuni autori hanno contestato la motivazione della Corte nella parte in cui sostiene che il diritto alla conoscenza delle prove non sia un diritto assoluto, ritenendo, viceversa, che al fine di contestare le prove derivate dall'operazione *EncroChat*, i dati avrebbero dovuto essere accessibili per verificarne l'integrità e l'affidabilità (perché tutti i messaggi di *EncroChat* erano inviati sotto pseudonimo) e, per trovare, se possibile, prove a discarico degli indagati/imputati. L'art. 6, par. 1 CEDU prevede, infatti, che le autorità giudiziarie comunichino alla difesa tutte le prove materiali in loro possesso a favore o contro l'imputato. Sebbene alcune prove possano essere tenute "nascoste", al fine di preservare i diritti fondamentali di altre persone o di salvaguardare un interesse pubblico rilevante, come la sicurezza nazionale o la necessità di proteggere i testimoni o di mantenere segreti i metodi di indagine della polizia sui reati, le eventuali difficoltà causate alla difesa da una limitazione dei suoi diritti dovrebbero essere sufficientemente controbilanciate dalle procedure seguite dalle autorità giudiziarie per garantire il rispetto del principio del giusto processo. In questo senso, J.J. OERLEMANS – D. VAN TOOR, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 30, 2022, pp. 309-328.

²³ Quanto ai giudici tedeschi, i tribunali regionali superiori di Brema e di Amburgo confermavano la custodia cautelare nei confronti di persone le cui attività criminali erano state rivelate a seguito dell'infiltrazione in *EncroChat*. Essi stabilivano che la raccolta effettuata dalle autorità francesi è utilizzabile anche nei procedimenti penali nazionali se l'intercettazione riguarda le attività criminali condotte da persone residenti in Germania. Nel caso del tribunale di Brema (sent. 18.12.2020, 1 Ws 166/20), veniva richiamata la giurisprudenza della Corte costituzionale tedesca per la quale l'ammissibilità delle informazioni raccolte deve essere misurata esclusivamente in base al diritto a un processo equo, oltre che di (eventuali) espressi divieti legali, in assenza di "altra" garanzia costituzionale che fornisca uno standard completo per l'utilizzabilità delle informazioni raccolte (sent. 7.12.2011, 2 BvR 2500/09, 2 BvR 185 7/10, punti 115-116). Perciò, ritenendo rispettati i requisiti formali per l'OEI e per lo scambio transfrontaliero e non ravvisando una violazione del diritto al giusto processo, il tribunale di Brema concludeva per l'ammissione delle prove in questione. Nell'altro caso, il tribunale di Amburgo (sent. 21.3.2021, 1 Ws 2/21) riteneva che le intercettazioni fossero corrette, mancando altre valide opzioni meno invasive (proporzionalità). Lo stesso Tribunale riteneva che, nel caso di specie, l'intercettazione del dispositivo dell'imputato fosse proporzionata rispetto all'entità del traffico di stupefacenti di cui era accusato e che inoltre misure analoghe potessero essere comunque autorizzate ai sensi del codice di procedura penale tedesco (equivalenza). Nel concludere sulla legittimità del trasferimento delle prove, il tribunale di Amburgo osservava che non è possibile derivare la legittimità di atti e decisioni straniere dal diritto processuale penale tedesco, poiché esso non si applica alle questioni estere. Al massimo, parametri di valutazione nel giudizio di proporzionalità interno (in particolare, sull'emissione di un OEI) possono essere i diritti fondamentali, come enucleati nella carta costituzionale, o garantiti dalla CEDU. Infine, anche la Corte di giustizia federale (sent. 2.3.2022, 5 StR 457/21, N. 038/2022) riteneva che il controllo della legge straniera non è un prerequisito per il trasferimento delle prove e che, attesa la loro rilevanza, non ci sarebbe stata alcuna violazione dei diritti umani o del diritto europeo o di altri requisiti fondamentali per l'emissione degli OEI contestati. Viene, quindi, confermata nel

Sezioni Unite della Corte di Cassazione italiana²⁴, dopo orientamenti confliggenti²⁵, hanno concluso per l'applicazione della disciplina relativa alla circolazione delle prove tra procedimenti penali, quale desumibile dagli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p. Secondo le Sezioni Unite, trattandosi di prove già autonomamente raccolte dalle autorità straniere prima dell'emissione dell'OEI, l'equivalenza con i casi interni analoghi è da parametrarsi alla disciplina della circolazione delle prove fra procedimenti diversi, di modo che queste possono essere legittimamente richieste ed acquisite dal pubblico

giudizio di proporzionalità la "presunzione di colpevolezza" nei confronti degli indagati, giustificabile in quanto *EncroChat* si presentava alle autorità francesi come una rete concepita fin dall'inizio per sostenere gravi attività criminali ed operare in segreto. Proprio la questione della gravità dei reati che risulta solo dopo l'acquisizione dei dati *EncroChat* sarà uno dei dubbi che solleverà il giudice del rinvio davanti alla Corte di giustizia (*infra* paragrafo 3).

²⁴ Cfr. Cass. pen., Sez. Un., sent. 29.02.2024, nn. 23755 e 23756.

²⁵ Le questioni su cui le diverse sezioni della Corte di Cassazione italiana si sono scontrate hanno riguardato principalmente la natura giuridica delle operazioni acquisitive poste in essere dall'autorità straniera e poi oggetto di un OEI, nonché l'inquadramento dei dati con la determinazione della disciplina probatoria applicabile e, di conseguenza, le relative garanzie procedurali, rilevando tanto la disciplina sull'acquisizione di documenti e dati informatici (art. 234-*bis* c.p.p.), quanto quella sul sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni (254-*bis* c.p.p.) o, ancora, quella sulle intercettazioni di conversazioni o comunicazioni (art. 266 c.p.p. e ss.). Più specificamente, le sezioni I e IV della Cassazione ritenevano che la messaggistica scambiata con i sistemi come *EncroChat*, e acquisita mediante OEI da autorità giudiziaria straniera che ne aveva eseguito la decrittazione, costituisse dato informativo documentale conservato all'estero 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. (Cass., Sez. I, sent. 13.10.2022, nn. 6363 e 6364; Cass., Sez. III, sent. 19.10.2023, n. 47201; Cass., Sez. IV, sent. 5.4.2023, n. 16347). La Sezione VI della Corte di Cassazione (sent. 26.10.2023, n. 46833), muovendo da un arresto della Corte costituzionale italiana del 2023 (sent. 22.6. 2023, n. 170), secondo cui anche la messaggistica – informatica o cartacea – conservata dopo la consegna non ha natura di generico documento, bensì mantiene il suo carattere di «corrispondenza», riteneva che la messaggistica sulle chat criptate, costituendo del pari registrazione di conversazioni già avvenute e, quindi, dati «statici», fossero assimilabili alla corrispondenza, la quale non necessita di un provvedimento del giudice, potendo essere acquisita con decreto motivato di sequestro probatorio disposto dal pubblico ministero. La sezione VI della Corte di Cassazione (Cass., Sez. VI, sent. 26.10.2023, nn. 44154 e 44155) aveva, poi, ritenuto che, in tema di OEI, l'oggetto dell'acquisizione all'estero della messaggistica criptata non costituisse dato informatico utilizzabile ai sensi dell'art. 234-*bis* c.p.p., sicché, in tale ipotesi, l'attività acquisitiva, se riguardante comunicazioni avvenute nella fase "statica", dovesse essere inquadrata nelle disposizioni in materia di perquisizione e sequestro e, in particolare, in quella di cui all'art. 254-*bis* c.p.p., mentre, se avesse avuto ad oggetto comunicazioni avvenute nella fase "dinamica", dovesse essere inquadrata nella disciplina dell'art. 266 ss. c.p.p. in materia di intercettazioni telefoniche. Sulla questione, poi, dell'emissione dell'OEI da parte del pubblico ministero, la VI Sezione riconosceva la competenza del pubblico ministero ad emanare un ordine di sequestro delle comunicazioni già autonomamente raccolte dall'autorità straniera, impugnabile dalla difesa per mezzo di riesame, così da ottenere una verifica giurisdizionale della presenza dei requisiti richiesti per il sequestro in base alla legge nazionale (controllo *ex post*). Quanto all'utilizzabilità di prove acquisite all'estero a seguito dell'emissione di un OEI, la Sezione VI la subordinava 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, pena l'inutilizzabilità. Sul punto, cfr. M. DANIELE, [Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite](#), in questa *Rivista*, 11 dicembre 2023, nonché P. PUJA, *L'acquisizione della messaggistica criptata conservata su server straniero tra classificazioni concettuali e divergenze giurisprudenziali*, in *Archivio Penale*, 2024, n. 2, in part. p. 8 ss.

ministero italiano senza la necessità della preventiva autorizzazione da parte del giudice del procedimento nel quale si intende utilizzarle²⁶. Viceversa, la loro utilizzabilità andrebbe esclusa solo se il giudice italiano rilevasse con il loro impiego una violazione dei diritti fondamentali. Nel ragionamento delle Sezioni Unite, l'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per decriptarne il testo non determina, però, una violazione dei diritti fondamentali, dovendo escludersi, salvo specifiche allegazioni di segno contrario, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non avrebbe alcuna possibilità di decriptarlo anche solo parzialmente²⁷. Resta ferma, pertanto, la garanzia di un controllo giurisdizionale perlomeno di tipo posticipato²⁸, per cui spetta, comunque, al giudice dello Stato di emissione dell'OEI la competenza a valutare se vi siano i presupposti per ammettere ed utilizzare le prove già in possesso delle autorità competenti dello Stato di esecuzione ai fini delle decisioni di sua spettanza, nonché se vi sia stata violazione dei diritti fondamentali riconosciuti dalla Costituzione e dalla Carta dei diritti fondamentali, e, quindi, del diritto di difesa e della garanzia di un giusto processo, conformemente all'art. 14, par. 7 della direttiva OEI, sebbene, come ricordano le Sezioni Unite, l'onere di allegare e provare i fatti da cui inferire tale violazione gravi sulla parte interessata.

3. La decisione della Corte di giustizia nel caso *M.N. (EncroChat)* sull'acquisizione di prove già in possesso dell'autorità di esecuzione ed il rimando agli ordinamenti processuali nazionali.

A fronte del dibattito dottrinale e giurisprudenziale negli Stati membri (e non solo)²⁹, molta era l'attesa per la pronuncia della Corte di giustizia chiamata ad interpretare per la prima volta la direttiva OEI con riferimento all'ipotesi di trasferimento di prove già in possesso delle autorità competenti dello Stato di esecuzione, secondo le molteplici questioni sottopostele dal giudice del Tribunale del Land, Berlino. Questi, in evidente disaccordo con gli altri tribunali tedeschi³⁰, solleva,

²⁶ Ciò anche quando le prove richieste siano già state raccolte all'estero attraverso intercettazioni o acquisizione di tabulati: vale a dire, operazioni istruttorie che, a differenza delle perquisizioni e dei sequestri, a livello nazionale non potrebbero essere disposte direttamente dal pubblico ministero, necessitando, appunto, una preventiva autorizzazione del giudice.

²⁷ In senso critico, soprattutto con riferimento al controllo sulle modalità di raccolta delle prove da parte dell'autorità straniera, v. M. DANIELE, [Le sentenze "gemelle" delle Sezioni Unite sui criptofonini](#), in questa *Rivista*, 17 luglio 2024.

²⁸ Cfr. anche Cass., Sez. I, sent. 12.3.2024, n. 13535.

²⁹ Anche in Norvegia, la Corte suprema stabiliva che le prove recuperate dalle autorità nazionali a seguito della collaborazione con quelle francesi fossero ammissibili (dec. 30.6.2022, HR-2022-1314-A, punti 26, 39 e 42), purché: acquisite in conformità con la procedura penale francese, non potendo sindacare la legittimità di tale procedura; l'imputato avesse avuto integralmente accesso ai dati acquisiti; l'uso delle prove non fosse stato fatto a detrimento dei diritti umani e dei valori fondamentali dello Stato.

³⁰ Cfr. *supra* nota 22.

innanzitutto, dubbi sull'autorità competente ad adottare un OEI in tale caso e sulle modalità di raccolte delle prove. Così, ritiene che il pubblico ministero non possa emettere un OEI diretto alla trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione quando, in forza del diritto dello Stato di emissione in un procedimento puramente interno, la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice. In altri termini, egli ritiene che il controllo sotto il profilo del diritto nazionale dovrebbe estendersi all'atto di indagine che è all'origine della raccolta dei dati.

La Corte di giustizia³¹, però, guarda alla natura dell'autorità di emissione, che l'art. 6, par. 1 della direttiva non stabilisce, e all'art. 2, lett. c) n. ii) che, come precedentemente affermato, include il pubblico ministero tra le autorità di emissione, rinviando alle previsioni del diritto nazionale. In particolare, ritenendo che il codice di procedura penale tedesco (art. 100e, par. 6, punto 1) autorizzi la trasmissione di prove da un'autorità nazionale di indagine ad un'altra senza l'autorizzazione da parte di un giudice, diversamente dalla norma nazionale per la raccolta iniziale di dati, la Corte conclude che spetti al giudice del rinvio, il solo competente ad interpretare il diritto nazionale, stabilire se sia così³². Tuttavia, ritiene che le condizioni sostanziali per l'emissione di un OEI nel caso di specie debbano essere verificate dall'autorità di emissione alle stesse condizioni applicabili in una situazione puramente interna relativa alla trasmissione di dati³³ e non alla loro raccolta³⁴. L'autorità di emissione non può valutare la legittimità degli atti mediante i quali sono state raccolte le prove nello Stato membro di esecuzione, perché contraria all'art. 6, par. 1, in quanto condurrebbe in

³¹ Cfr. Corte giust., sent. 30.4.2024, M.N. (*EncroChat*), Causa C-670/22 su cui v. E. LORENZETTO, *Il caso EncroChat e l'ordine europeo di indagine penale nella staffetta fra Corte di giustizia e diritto dello Stato di emissione*, in *Cassazione penale*, n. 9, 2024, pp. 2887-2897.

³² Specificamente, la Corte di giustizia precisa che: «l'art. 1, paragrafo 1, e l'art. 2, lettera c), della direttiva 2014/41 devono essere interpretati nel senso che un OEI inteso a ottenere la trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione non deve essere adottato necessariamente da un giudice quando, in forza del diritto dello Stato di emissione, in un procedimento puramente interno a tale Stato, la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice, ma competente ad ordinare l'acquisizione di dette prove è il pubblico ministero» (punto 77). In senso parzialmente dissimile, l'Avvocato generale Tamara Čapeta nelle sue conclusioni del 26 ottobre 2023, afferma che quando il diritto nazionale legittima il pubblico ministero a chiedere il trasferimento di prove a condizione che la loro acquisizione iniziale sia stata autorizzata da un giudice, tale previsione diventa rilevante ai fini della verifica delle condizioni di cui all'art. 6, par. 1, lett. b) della direttiva. Tuttavia, se l'autorizzazione giudiziaria sussiste, questa non può essere messa in discussione (punti 68-69).

³³ Di conseguenza, se il diritto dello Stato di emissione subordina tale trasmissione all'esistenza di indizi concreti di commissione di reati gravi da parte dell'imputato o all'ammissibilità delle prove costituite dai dati di cui trattasi, l'adozione di un ordine europeo di indagine è soggetta a tutte le medesime condizioni (punto 95 della sentenza M.N.).

³⁴ La Corte, infatti, chiarisce che «l'articolo 6, paragrafo 1, lettera b), della direttiva 2014/41 non richiede – neppure in una situazione come quella in causa nel procedimento principale, in cui i dati in questione sono stati raccolti dalle autorità competenti dello Stato di esecuzione nel territorio dello Stato di emissione e nell'interesse di quest'ultimo – che l'emissione di un ordine europeo di indagine diretto alla trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione sia soggetta alle stesse condizioni sostanziali applicabili, nello Stato di emissione, in materia di raccolta di tali prove».

pratica ad un sistema più complesso e meno efficace, così nuocendo all'obiettivo perseguito dalla direttiva³⁵.

In definitiva, si tratterebbe di elementi di prova autonomamente raccolti dalle autorità straniere sulla base della *lex loci* ed acquisite attraverso l'emissione di un OEI diretto al trasferimento di prove esistenti che l'autorità di emissione è tenuta a riconoscere, salvo che sia accertata l'illegittimità dell'atto sottostante in un procedimento giudiziario nello Stato di esecuzione che la persona interessata deve poter instaurare³⁶. Inoltre, come affermato dalla Corte e ricordato dall'Avvocato generale, nel caso di specie, gli OEI riguardavano l'acquisizione da parte della Procura generale di Francoforte, attraverso le autorità investigative francesi, di dati raccolti da telefoni cellulari dotati del servizio *EncroChat*, utilizzati da utenti tedeschi, a seguito di autorizzazione del giudice francese, nella specie il tribunale penale di Lille.

L'altra serie di questioni che il giudice del rinvio sottopone riguarda la qualificazione della misura connessa all'infiltrazione negli apparecchi, diretta a estrarre i dati relativi al traffico, all'ubicazione e alle comunicazioni, nonché la tutela dei diritti degli utenti interessati da tale misura e l'utilizzo dei dati così raccolti nell'ambito di procedimenti penali avviati. Più specificamente, egli ritiene che si tratti di intercettazione di telecomunicazioni che, ai sensi dell'art. 31 della direttiva OEI, avrebbe richiesto la notifica ad un giudice dello Stato membro sul cui territorio si trova la persona sottoposta all'intercettazione. Ebbene, la Corte, facendo leva su una interpretazione autonoma e uniforme del diritto dell'Unione, ritiene che una simile misura sia un'intercettazione di telecomunicazioni³⁷, ma che, nulla specificando la direttiva, la notifica vada inviata all'autorità designata come competente da ciascun Stato membro o a qualsiasi autorità dello Stato membro notificato che lo Stato membro di intercettazione ritenga idonea a tal fine, dovendo quest'ultimo trasmettere d'ufficio la notifica all'autorità competente al fine di preservare l'effetto utile della previsione in questione. Inoltre, sulla tutela dei diritti degli intercettati e l'utilizzabilità dei dati, la Corte precisa che l'intercettazione di telecomunicazioni di cui all'art. 31 della direttiva non è oggetto di OEI³⁸ con la

³⁵ Cfr. punto 100 della sentenza *M.N.* Inoltre, come evidenzia l'Avvocato Ćapeta, la direttiva OEI non si occupa della questione se sia possibile trasferire prove consistenti in dati di comunicazioni intercettate raccolti nell'ambito di un'indagine o di un procedimento penale, rinviando al diritto dello Stato di emissione, nella specie il diritto tedesco sulla base del quale valutare se gli atti con i quali sono state raccolte le prove in Francia assumano rilevanza o meno.

³⁶ Vale la pena ricordare che due ricorsi alla Corte europea dei diritti umani, presentati da cittadini britannici arrestati e detenuti in Gran Bretagna, sempre grazie all'utilizzo dei dati recuperati dalle autorità francesi sulla piattaforma *EncroChat* (Corte EDU, ricorso n. 44715/20, *A.L. c. Francia*, Corte EDU, ricorso n. 47930/20, *E.J. c. Francia*), per l'accertamento della violazione del diritto alla *privacy* (art. 8 CEDU) e del diritto ad un ricorso effettivo (art. 13 CEDU), sono stati dichiarati inammissibili, per mancato esaurimento delle vie di ricorso interno (*A.L. e E.J. c. Francia* (dec.) - 44715/20 e 47930/21). Tali decisioni conseguivano all'esito di quesiti che la Corte di Strasburgo poneva alle parti per verificare, in particolare, se esse avessero avuto la possibilità di contestare le misure di intercettazione dinanzi ai giudici francesi competenti (ma non ne avessero fatto uso).

³⁷ Cfr. punti 111-114 della sentenza *M.N.*

³⁸ Diversamente dall'art. 30, par. 1 della direttiva che prevede che «un OEI può essere emesso per l'intercettazione di telecomunicazioni nello Stato membro la cui assistenza tecnica è necessaria».

conseguenza che le diverse condizioni e le garanzie di un tale OEI, cioè diretto alla trasmissione dei dati, non si estendono alle intercettazioni. Tuttavia, ad avviso della Corte, la formulazione del par. 3 dell'art. 31 della direttiva 2014/41³⁹ lascia all'autorità competente dello Stato membro notificato una discrezionalità diretta a preservarne la sovranità e ad assicurare che il livello di tutela previsto in tale Stato membro in materia di intercettazioni non sia compromesso. Si tratta, infatti, di un'ingerenza nel diritto al rispetto della vita privata e delle comunicazioni di cui all'art. 7 della Carta, che, secondo la Corte, l'art. 31 mirerebbe a limitare, assicurando la protezione dei diritti delle persone interessate da tali misure, e ammettendo l'inutilizzabilità dei dati intercettati per l'esercizio dell'azione penale nello Stato notificato⁴⁰.

Tuttavia, l'utilizzabilità o meno delle prove acquisite dipende dagli ordinamenti processuali degli Stati membri. Più specificamente, nutrendo dubbi sugli approcci seguiti da altri giudici tedeschi basati principalmente sulla gravità dei reati individuati grazie ai dati acquisiti (*ex post*)⁴¹, il giudice del rinvio paventa la violazione del diritto dell'Unione e specificamente del principio di equivalenza per la violazione della competenza riservata al giudice in materia e per l'assenza di una presunzione concreta della gravità dei reati, nonché del principio di effettività che impone al giudice penale nazionale di espungere, nell'ambito di un procedimento penale avviato a carico di una persona sospettata di atti di criminalità, informazioni ed elementi di prova che siano stati ottenuti in violazione delle prescrizioni del diritto dell'Unione, anche conformemente alla giurisprudenza europea in materia di condizioni di accesso ai dati relativi alle comunicazioni elettroniche. La Corte, però, ritiene che tali questioni dipendano dalle decisioni del giudice del rinvio rispetto alla legittimità dell'emissione dell'OEI, in quanto, richiamando la sua stessa giurisprudenza, «allo stato attuale del diritto dell'Unione, spetta, in linea di principio, unicamente al diritto nazionale determinare le norme relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale, di informazioni e di elementi di prova che sono stati ottenuti con modalità contrarie al diritto dell'Unione e spetta ancora all'ordinamento giuridico interno di ciascuno Stato membro, ai sensi del principio dell'autonomia procedurale, stabilire le modalità procedurali dei ricorsi intesi a garantire la tutela dei diritti spettanti

³⁹ Testualmente il par. 3 dell'art. 31 della direttiva sancisce: «Qualora l'intercettazione non sia ammessa in un caso interno analogo, l'autorità competente dello Stato membro notificato può notificare all'autorità competente dello Stato membro di intercettazione che tale intercettazione non può essere effettuata o che si deve porre fine alla medesima o anche, se del caso, che i dati intercettati non possono essere utilizzati o possono essere utilizzati solo alle condizioni da essa specificate».

⁴⁰ Tuttavia, le maggiori critiche hanno riguardato l'intercettazione segreta ai sensi della legge francese, che ha interessato una massa di persone senza sospetti penali concreti a quella data: cosa che non sarebbe stata possibile ai sensi della legge tedesca e che avrebbe gravemente violato il diritto alla privacy dei tedeschi intercettati. Le altre critiche hanno riguardato la legalità delle modalità di trasferimento dei dati in Germania. Questi sarebbero stati inizialmente scambiati tramite canali di polizia di modo che il successivo OEI sarebbe servito solo a convalidare queste operazioni senza controllo giudiziario in Germania. Inoltre, anche il mancato rispetto delle disposizioni dell'art. 31 della direttiva OEI, avrebbe dovuto produrre conseguenze sulla legalità dell'uso delle prove. In questo senso, T. WAHL, *Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases*, in *Eucrim*, n. 1, 2022, pp. 36-37.

⁴¹ V. ancora *supra* nota 22.

ai singoli in forza del diritto dell'Unione, a condizione tuttavia che esse non siano meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano in pratica impossibile o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività)»⁴².

La Corte conclude, quindi, che la direttiva OEI impone espressamente agli Stati membri (art. 14, par. 7) di garantire che, in un procedimento penale nello Stato di emissione, siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove ottenute mediante l'OEI, il che, secondo la Corte, impone al giudice penale nazionale di espungere informazioni ed elementi di prova qualora la persona indagata non sia in grado di svolgere efficacemente le proprie osservazioni su tali informazioni ed elementi di prova e questi ultimi siano idonei ad influire in modo preponderante sulla valutazione dei fatti, ma sempre se il giudice del rinvio decida per l'illegittima emissione dell'OEI (punto 127). Nella sostanza, la Corte ammetta che le conclusioni a cui può giungere il giudice nazionale siano, in ordine alla tutela dei singoli, le stesse della pregressa giurisprudenza in materia di *data retention*⁴³, sia pur con una sorta di *favor* per l'esecuzione dell'OEI, quale strumento della cooperazione giudiziaria penale di cui all'art. 82, par. 1, TFUE, fondato sul principio del mutuo riconoscimento e della fiducia reciproca, nonché sulla presunzione relativa che gli altri Stati membri rispettino il diritto dell'Unione e, in particolare, i diritti fondamentali, ed il diritto all'equo processo.

In definitiva, la Corte si concentra sul rispetto delle condizioni di emissione di un OEI, così superando alcune criticità sollevate dal giudice del rinvio ed emerse nei giudizi nazionali, precedentemente richiamati⁴⁴, in cui la valutazione delle prove si è ridotta ad una sorta di "automatismo"⁴⁵ di decifrazione dell'algoritmo delle chat crittografate sulla

⁴² Cfr. punti 126 ss. della sentenza *M.N.*

⁴³ Cfr. Corte giust., sent. 6.10.2020, *La Quadrature du Net e a. contro Premier ministre e a.* nella parte in cui afferma: «Pertanto, il principio di effettività impone al giudice penale nazionale di non tenere conto degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate di avere commesso atti di criminalità, qualora dette persone non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova, che provengono da un settore che esula dalla competenza dei giudici e possono influenzare in maniera preponderante la valutazione dei fatti» (punto 227). Sul punto, v., per tutti, M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione europea*, n. 1, 2021, pp. 93-124; ID., *La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle corti di Strasburgo e Lussemburgo: verso il cambio di paradigma del rapporto privacy v. security*, in *Freedom, Security & Justice: European Legal Studies*, n. 3, 2022, pp. 105-133.

⁴⁴ V. *supra* paragrafo 2, anche note 23, 24 e 25.

⁴⁵ Si ricorda, come, sempre nella sentenza *La Quadrature du Net*, la Corte di giustizia richiamava una sua precedente sentenza (sent. 10.4.2003, *Joachim Steffensen*, Causa C-276/01, punto 77) in cui rinviava all'interpretazione della Corte europea sul diritto al contraddittorio come autentica possibilità di dedurre efficacemente, dinanzi al tribunale, su un mezzo di prova, affinché il procedimento abbia il carattere equo richiesto dall'art. 6, n. 1, della CEDU, «in particolare quando il mezzo di prova rientra in un ambito tecnico che esula dalla competenza dei giudici e può influenzare in modo preponderante la valutazione dei fatti ad opera del tribunale».

piattaforma *EncroChat*, oggetto di intercettazione senza alcuna distinzione dei soggetti intercettati ed in assenza di indizi concreti della commissione di gravi reati né al momento dell'intercettazione né al momento dell'emissione dell'OEI. Ne consegue una discrepanza nell'approccio all'accesso ai dati tenuti e conservati da provider e all'accesso ai dati conseguente alle indagini condotte dagli Stati su piattaforme presunte criminali che, per quello che si dirà in seguito, appare giustificabile dalla criminalizzazione della piattaforma stessa con evidenti ricadute, però, su tutti i suoi utilizzatori.

4. La sottesa questione della sorveglianza di massa nell'intercettazione dei dati.

In effetti, l'altra questione sollevata dall'intera vicenda giudiziaria *EncroChat*, principalmente nel dibattito dottrinale, rimanendo, viceversa, sottesa nella sentenza della Corte, è quella di una sorta di sorveglianza di massa ai fini delle indagini penali che precluderebbe al pubblico ministero il potere di emettere un OEI. Trattandosi, infatti, di dati del servizio *EncroChat*, il giudice del rinvio ritiene che la giurisprudenza relativa alle limitazioni alla riservatezza delle comunicazioni, alla memorizzazione e conservazione dei dati su traffico, all'identificazione ed all'ubicazione di tali dati, conseguente all'interpretazione dell'art. 15, par. 1, della direttiva 2002/58⁴⁶, alla luce dei diritti fondamentali ex artt. 7, 8 e 11 della Carta, sia trasponibile all'interpretazione dell'art. 6, par. 1, lett. a), della direttiva 2014/41, non potendosi giustificare una soluzione diversa alle modalità di acquisizione delle prove/dati, che dovrebbe essere disposta soltanto da parte di un giudice, posta la gravità dell'ingerenza nei diritti fondamentali delle persone interessate. Anche per quanto riguarda il rispetto del principio di proporzionalità, richiamando ancora la giurisprudenza della Corte sulla liceità di conservazione dei dati relativi alle comunicazioni elettroniche, il giudice tedesco ritiene che debba sussistere, a carico di ciascuna persona interessata, una presunzione fondata su fatti concreti di partecipazione a un reato grave, anche perché la lotta alle forme gravi di criminalità non potrebbe giustificare una conservazione generalizzata e indifferenziata dei dati personali. Per quanto già detto, la Corte non se ne occupa, potendo riformulare le questioni che le sono sottoposte e trarre dall'insieme degli elementi forniti dal giudice nazionale e, in particolare, dalla motivazione della decisione di rinvio, gli elementi del diritto dell'Unione che richiedano un'interpretazione, tenuto conto dell'oggetto della controversia. Si attiene, in tal modo, strettamente all'interpretazione delle condizioni sostanziali (e cumulative) per l'emissione di un siffatto OEI, enunciate all'art. 6, par. 1, lett. a) e b), della direttiva 2014/41 e sintetizzate nel paragrafo precedente.

Tale questione viene, invece, affrontata dall'Avvocato generale Čapeta che sposa le perplessità del giudice del rinvio, chiedendosi, seguendo la logica della sentenza

⁴⁶ Trattasi della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), successivamente modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009.

Prokuratuur, se si possa affidare a un pubblico ministero la valutazione imparziale della proporzionalità per l'emissione di un OEI, nella specie, diretto al trasferimento di prove consistenti in dati di telecomunicazioni intercettate. Tuttavia, ritiene che la direttiva OEI dimandi, in modo sensato, tale apprezzamento agli ordinamenti giuridici nazionali, stante le differenze nell'organizzazione dei sistemi di giustizia penale negli Stati membri e anche perché, in caso contrario, l'art. 2, lett. c), n. i) della direttiva sarebbe privato di significato. L'Avvocato ricorda, poi, che nel contesto della direttiva relativa alla vita privata e alle comunicazioni elettroniche, il pubblico ministero accede ai dati relativi al traffico e all'ubicazione della popolazione in generale, conservati dagli operatori di telecomunicazioni in forza del diritto nazionale, di modo che la sua richiesta di accesso ai fini di un'indagine penale concreta sarebbe la prima occasione in cui possono essere prese in considerazione circostanze individuali. Ne consegue che l'intervento di un giudice è necessario per evitare un accesso in forma massiccia e generale ai dati conservati. Viceversa, a suo avviso, nel caso di specie, l'intercettazione sarebbe stata effettuata direttamente dagli Stati membri ai fini di un'indagine penale concreta in Francia, sotto il controllo di un giudice. La sua conclusione è, quindi, che la direttiva 2002/58 e la pertinente giurisprudenza non trovano applicazione nel caso di specie in quanto il livello di ingerenza nei diritti fondamentali alla vita privata e alla protezione dei dati che ha dato origine alla sentenza *Prokuratuur*, non equivarrebbe al livello di ingerenza di cui alla presente causa. I dati il cui trasferimento è stato richiesto mediante gli OEI emessi dalla procura di Francoforte erano limitati ai soli utenti di *EncroChat* in Germania, in un contesto caratterizzato dall'esistenza di sospetti che tale servizio fosse utilizzato principalmente ai fini della commissione di reati.

Ancor più, secondo l'Avvocato, proprio dalla giurisprudenza richiamata dal giudice del rinvio (specificamente la sentenza *La Quadrature du Net*), deriva che la direttiva relativa alla vita privata e alle comunicazioni elettroniche non si applichi all'intercettazione diretta di dati, ricadendo questa, viceversa, nell'ambito del diritto nazionale, e fatta salva l'applicazione della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie⁴⁷, che, viceversa, può effettivamente trovare applicazione nelle circostanze del caso di specie, sebbene non contenga, a suo avviso, alcuna norma che consenta alla Corte di concludere che il diritto dell'Unione impone agli Stati membri l'obbligo di garantire una previa autorizzazione giudiziaria ai fini dell'accesso diretto da parte del pubblico ministero ai dati ottenuti mediante l'intercettazione di comunicazioni. L'Avvocato ritiene, inoltre, che diversamente dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche, la direttiva OEI impone agli Stati membri di garantire mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo (art. 14, par. 1). Pertanto, l'indagato o l'imputato dovrebbero poter contestare la valutazione della proporzionalità effettuata dal pubblico ministero al momento dell'emissione di un OEI diretto al trasferimento di prove. Ne consegue che, pur seguendo il ragionamento

⁴⁷ Direttiva (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 e che abroga la decisione quadro 2008/977/GAI del Consiglio.

del giudice del rinvio, anche l'Avvocato generale considera, nella sostanza, l'ingerenza nella vita privata delle persone indagate ed imputate non comparabile alla sorveglianza di massa della popolazione in generale⁴⁸.

Ciononostante, le interpretazioni fornite inducono alcune riflessioni ed interrogativi. Ci si chiede, così, se le esigenze di accertamento dei reati per garantire la sicurezza pubblica non potranno, quindi, sempre consentire che le attività investigative delle autorità giudiziarie degli Stati membri si svolgano sotto forma di "intercettazioni/sorveglianza" informatica diffusa. Ancor più, dato che l'OEI può essere emesso anche per il trasferimento di dati acquisiti a seguito di indagini condotte quando sussistano indizi di plurimi reati commessi da persone non ancora identificate che interagiscono su una piattaforma digitale, ci si chiede come sarà possibile escludere una sorveglianza diffusa in quanto proprio l'anonimato e la crittografia consentono di isolare una chat specifica solo dopo aver intercettato e decifrato tutte le chat del sistema. Ci si chiede, infine, con riferimento al testo della direttiva, se la previsione dell'art. 30, relativo all'emissione di un OEI per le intercettazioni di telecomunicazioni per cui è necessaria l'assistenza tecnica di un altro Stato membro, così come dell'art. 31, che prevede la notifica allo Stato membro nel quale si trova la persona soggetta a intercettazione (*ex art. 31 direttiva*), non siano ormai del tutto superate, soprattutto se applicate a piattaforme digitali.

5. Conclusioni aperte tra "adattabilità" del regime probatorio in assenza di armonizzazione e finalità di accertamento dei reati: quale preminenza per le esigenze delle indagini penali?

In definitiva, ci sembra che non possa escludersi la riproposizione delle questioni evidenziate, soprattutto nell'attuale momento storico in cui il ricorso alla crittografia a fini criminosi è sempre maggiore, con evidenti ripercussioni sulla capacità delle autorità giudiziarie e di polizia di ottenere le informazioni necessarie da acquisire come prove nelle indagini penali e di perseguire e condannare gli autori dei reati⁴⁹. Viene, però, il

⁴⁸ Invero, la questione era già stata sollevata anche davanti ad alcune corti nazionali che, tuttavia, avevano escluso che le indagini fossero riconducibili ad ipotesi di sorveglianza di massa, con la conseguenza che il grado di necessità e proporzionalità richiesto fosse inferiore rispetto a quello altrimenti previsto dalla giurisprudenza europea sulla *mass surveillance*. Sul punto cfr., tra gli altri, R. STOYKOVA, *EncroChat: The Hacker with a Warrant and Fair Trials?*, in *Forensic Science International: Digital Investigation*, vol. 46, 2023, p. 3, la quale, inoltre, ritiene che non si tratti di intercettazione telefonica, ma di sorveglianza informatica: «*For legal purposes, in most documented sources the Encrochat operation is classified as phone interception, however its technical characteristics relate it more closely to computer surveillance. As will be examined further, the authorities acquired Encro-phone data by the use of a technical implant which captures data in a volatile memory. In technical terms, volatile memory is a combination of data that is part of the transmission, and additional temporary processed data that is not intended for storage or transmission such as passwords and encryption keys. Both types of data can be obtained only with computer surveillance technology because phone interception does not capture data that is not yet stored, in between transmission, or that is never intended to be stored or transmitted*».

⁴⁹ Particolarmente interessante appare l'indagine condotta da D. CURTOTTI ET AL., [Piattaforme criptate e prova penale](#), in questa *Rivista*, n. 6, 2023, pp. 173-174, che evidenziano come l'ultima frontiera delle investigazioni

dubbio che le finalità delle indagini penali possano assumere una preminenza⁵⁰ tale da consentire di bypassare il momento di formazione della prova e da produrre, in assenza di una sua pur minima armonizzazione a livello europeo, una sorta di “adattabilità” dei regimi probatori frutto delle applicazioni casistiche, abbassando gli standard di garanzia previsti dai singoli ordinamenti processuali nazionali⁵¹.

L’intera vicenda *EncroChat* ha, infatti, dimostrato che l’emissione di un OEI per l’acquisizione di dati già in possesso delle autorità dello Stato di esecuzione segue il regime della circolazione delle prove al fine di beneficiare dei risultati dell’iniziativa investigativa delle autorità degli altri Stati membri⁵². Vero è che la piattaforma stessa era utilizzata dalla criminalità per svolgere i propri traffici⁵³ e questo ha ingenerato una “presunzione di colpevolezza”. Tuttavia, ci sembra che se per l’emissione di un OEI diretto all’acquisizione di prove derivanti dall’accesso ai dati relativi a comunicazioni elettroniche possedute dai fornitori di servizi sia necessaria l’autorizzazione del giudice, come statuito dalla Corte di giustizia nel caso *Procedimento penale a carico di HP*, questo valga anche quando quegli stessi dati siano stati già acquisiti o si tratti di dati acquisiti nel corso di indagini condotte direttamente dalle autorità giudiziarie. In altri termini, ci sembra che nel momento dell’acquisizione delle prove concernenti comunicazioni elettroniche non sia possibile prescindere dal bilanciamento tra gli interessi legittimi connessi alle esigenze dell’indagine nell’ambito della lotta alla criminalità e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall’accesso; e tale bilanciamento ci sembra debba

sia rappresentata dalle attività esperite sulle piattaforme di comunicazioni criptate, utilizzate anche dalle organizzazioni criminali per condurre e pianificare i propri traffici illeciti. Mentre, infatti, «in passato l’investigazione risultava circoscritta a specifici “ambienti” (come nel caso delle microspie) o a determinate aree di interesse (come nel caso del virus *Trojan*), allo stato è l’etere digitale il nuovo spazio da “esplorare”, cioè il server sul quale transitano tutti i flussi informativi degli utenti che utilizzano servizi di comunicazioni criptati».

⁵⁰ Si pensi al recente caso concernente il tentativo di accesso ai dati contenuti in un telefono cellulare da parte delle autorità di polizia austriache in cui il giudice del rinvio chiedeva se l’art. 4, par. 1, lettera c), della direttiva 2016/680, letto alla luce degli articoli 7 e 8 nonché dell’articolo 52, paragrafo 1, della Carta, ostasse a una normativa nazionale che riconosce alle autorità competenti tale possibilità a fini di prevenzione, ricerca, accertamento e perseguimento dei reati in generale e che non assoggetta l’esercizio di tale possibilità a un controllo preventivo da parte di un giudice o di un organo amministrativo indipendente e che la Corte di giustizia, sia pur enucleando le condizioni, ha ritenuto compatibile con il diritto dell’Unione e non necessariamente limitato alla lotta contro i reati gravi. Cfr. Corte giust., sent. 4.10.2024, *Bezirkshauptmannschaft Landeck*, Causa C-548/21.

⁵¹ I. ARMADA, cit., p. 19, ritiene che: «*The possibility that Member States rely upon their implementing legislations as legal basis for ordering e.g. covert surveillance is to be feared, as the EIO Directive does not contain any provision organising the concrete procedural arrangements governing each investigative measure*».

⁵² Secondo R. STOYKOVA, cit., p. 10, l’operazione *EncroChat* solleva sospetti anche in termini di cosiddetto *forum shopping* di materiale probatorio. Inoltre, come è stato rilevato, il passaggio all’era digitale, la natura transfrontaliera dei flussi comunicativi nelle chat criptate in uso alla criminalità organizzata e la necessità per gli attori delle indagini di tenere il passo rispetto a tali innovazioni, oltre a generare trasformazioni della giurisdizione, delle tecniche intrusive, della cooperazione internazionale, hanno segnalato asimmetrie, disallineamenti e inadeguatezze tra apparati investigativi di diversi Paesi, anche europei, nel fronteggiare la sfida. In questo senso, S. RAGAZZI – F. SPIEZIA, cit., p. 227.

⁵³ Cfr. *Europol/Eurojust Joint Press Release*, cit. *supra* nota 19.

sussistere anche in sede di esecuzione di un OEI. Non si coglie, in tal caso, il *discrimen* nell'approccio all'accesso ai dati (v. *supra* paragrafo 4) se non nel senso di accordare alle finalità delle indagini penali condotte dagli Stati quella preminenza richiamata in precedenza.

Si ritiene, in definitiva, che l'utilizzabilità dei risultati probatori di indagini transfrontaliere conseguenti all'accesso a sistemi informatici dovrebbe richiedere la certezza di principi condivisi e di parametri di controllo sul rispetto del principio di proporzionalità⁵⁴ non solo quando l'accesso sia richiesto ai fornitori privati⁵⁵, ma anche quando lo stesso sia effettuato direttamente dalle autorità di polizia e giudiziarie. Né ci sembra che l'art. 31 della direttiva OEI concernente la notifica delle intercettazioni possa essere sufficiente, perché esigenze di segretezza potrebbero farla aggirare, come di fatto è avvenuto, ma anche per le caratteristiche stesse delle piattaforme digitali. Ci sembra, inoltre, che le indagini investigative transfrontaliere delle autorità di polizia e giudiziarie per le esigenze di accertamento dei reati, la cui gravità è rimessa agli ordinamenti nazionali, conducano, attraverso quell'adattabilità sopra richiamata, a scardinare la ritualità dell'acquisizione delle prove nei diversi ordinamenti degli Stati membri. In questa direzione, si ritiene, altresì, che il testo normativo di adozione dell'OEI, quale

⁵⁴ L. BACHMAIER WINTER, *Mutual Recognition and Cross-Border Interception of Communications the Way Ahead for the European Investigation Order*, in C. BRIÈRE – A. WEYEMBERGH (eds.), *The Needed Balances in EU Criminal Law: Past, Present and Future* Oxford, 2017, p. 317 ss.; ID., *Mutual Admissibility of Evidence and Electronic Evidence in the EU – A New Try for European Minimum Rules in Criminal Proceedings?*, in *Eucrim*, n. 2, 2023, pp. 223-229.

⁵⁵ Tant'è vero che, sempre in tema di acquisizioni di comunicazioni elettroniche da fornitori privati, la Corte di giustizia ha sottolineato l'importanza di un previo controllo di proporzionalità in concreto da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente sulla gravità del reato oggetto di indagine per garantire che sia soddisfatto il requisito di proporzionalità della raccolta di tutti i dati con metodi di tracciamento e localizzazione di conversazioni telefoniche in entrata e in uscita, comunicazioni e connessioni effettuate in un'indagine per furto aggravato di telefoni. Cfr. Corte giust., sent. 30.4.2024, *Procedimento penale a carico di Procura della Repubblica presso il Tribunale di Bolzano*, Causa C-178/22. Pur non trattandosi di indagini transfrontaliere, tali da richiedere un OEI, la suddetta sentenza consente di ragionare sul fatto che la Corte abbia precisato come, ai fini dell'applicazione dell'art. 15, par. 1, della direttiva 2002/58, la conservazione e l'accesso ai dati deve riguardare la prevenzione, ricerca, accertamento e perseguimento di reati la cui gravità, considerata la ripartizione delle competenze tra l'Unione e gli Stati membri ai sensi del TFUE e le notevoli differenze esistenti tra gli ordinamenti giuridici nazionali in materia penale, è rimessa alla determinazione degli Stati membri, ma nel rispetto degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta. Specificamente, la Corte si è mostrata particolarmente sensibile ad un controllo di proporzionalità approfondito per cui le condizioni alle quali l'accesso ai dati conservati può essere autorizzato sono la sussistenza di «sufficienti indizi di reati», «rilevanti per l'accertamento dei fatti» con riferimento ai reati soggetti alla pena della reclusione non inferiore nel massimo a tre anni, a condizione, tuttavia, che il giudice nazionale abbia la possibilità di negare detto accesso se quest'ultimo è richiesto nell'ambito di un'indagine vertente su un reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato. Sulla pronuncia, cfr. P. DI STEFANO, *La Corte di giustizia afferma che il giudice può negare l'accesso ai dati di traffico o unicazione dell'utente di mezzi di comunicazione elettronica se il reato in concreto è manifestamente non grave: è regola immediatamente applicabile nel processo italiano?*, in *Cassazione penale*, n. 9, 2024, pp. 2860-2875; F. DUMORTIER, *Arrêts «Quadrature du Net» et «Procura della Repubblica presso il Tribunale di Bolzano»: d'importants « aménagements » de la jurisprudence relative à la conservation et à l'accès aux métadonnées*, in *Journal de droit européen*, 2024, pp. 391-394; F. PALMIOTTO, *Criminal Investigations, Access to Data and Fundamental Rights: The Role of Judicial Review after Procura*, in *Common Market Law Review*, vol. 61, n. 6, 2024, pp. 1633-1644.

ulteriore strumento europeo di cooperazione giudiziaria basato sul mutuo riconoscimento e sulla mutua fiducia, abbia lasciato praticamente “in bianco” una serie di questioni, rimettendole alle autorità giudiziarie nazionali⁵⁶, con un preoccupante impatto non solo sull’esercizio del diritto di difesa e del diritto al contraddittorio, come garanzie ineludibili di qualsiasi processo che possa definirsi equo⁵⁷, ma anche a monte sull’esercizio della funzione di prevenzione e repressione dei reati da parte degli Stati, praticamente invocabile per qualsiasi esigenza di tutela della sicurezza nazionale. Si prospettano, quindi, una serie non prevedibile di questioni⁵⁸ che lasciano aperte le conclusioni. Si dovranno molto probabilmente attendere, come già avvenuto con il MAE, ulteriori pronunce della Corte di giustizia per definire meglio le garanzie di “sistema”⁵⁹ dell’esecuzione dell’OEI, ovvero un ulteriore intervento normativo del legislatore europeo⁶⁰ che tenga almeno conto delle questioni emerse.

⁵⁶ Tanto ci sembra confermare quell’idea in precedenza sostenuta di una nuova dimensione della sicurezza europea ancorata ad un sistema di giustizia e *governance* transnazionale, specificamente «*a model of cooperation among national public authorities that continue to operate and drive the European integration process, as well as the centralization of these cooperation activities within EU agencies*». In questo senso, T. RUSSO, *The New Dimension of EU Security in a Transnational Justice and Governance System*, in T. RUSSO – A. ORIOLO – G. DALIA (eds.), *Solidarity and the Rule of Law. The New Dimension of EU Security*, Berlino, 2023, pp. 295-301.

⁵⁷ V. le recenti considerazioni di P. TROISI, *I canali di ingresso delle intercettazioni assunte e decrittate all’estero*, in *Processo Penale e Giustizia*, n. 6, 2024, pp. 1590 ss.

⁵⁸ Alcune sono già pendenti: ad esempio se sia possibile emettere un OEI quando l’audizione in videoconferenza abbia l’ulteriore finalità di garantire all’imputato la partecipazione al processo, domanda di pronuncia pregiudiziale, *Bissili*, Causa C-325/24. Inoltre, non si esclude che la Corte sarà chiamata a pronunciarsi nuovamente sulla delimitazione degli “atti di indagine”, come ha fatto nel recente caso *Delda* (v. *supra* nota 6) e ad intervenire ancora nel rapporto con gli altri strumenti di cooperazione giudiziaria, su cui v., tra gli altri, G. DALIA, *La natura transnazionale della digital evidence tra richieste di cooperazione e pretese di sovranità - Un equilibrio necessario per il contrasto alle nuove forme di criminalità*, in *I-LEX*, Vol. 16 n. 1 2023, pp. 37-48, specificamente per le possibili implicazioni anche con l’ordine europeo di produzione delle prove digitali che si applicherà a decorrere dal 18 agosto 2026. Sul punto si rimanda, tra gli altri, a A. GAUDIERI, *Novità in tema di cooperazione giudiziaria: i nuovi ordini europei di conservazione e produzione delle prove elettroniche*, in *Dir. pen. e proc.*, n. 9, 2023, p. 1231 ss.

⁵⁹ Come già evidenziato, T. RUSSO, *Alcuni spunti riflessivi sull’evoluzione della competenza penale dell’Unione europea e sulle criticità “procedurali” della cooperazione giudiziaria in materia*, in *Rivista della Cooperazione giuridica Internazionale*, vol. 76, 2024, pp. 88-108.

⁶⁰ Invero, due modifiche sono intervenute, ma hanno riguardato l’allineamento alle norme dell’Unione in materia di protezione dei dati personali, Direttiva (UE) 2022/228 del Parlamento europeo e del Consiglio del 16 febbraio 2022, e la digitalizzazione della cooperazione giudiziaria, Direttiva (UE) 2023/2843 del Parlamento europeo e del Consiglio, del 13 dicembre 2023.

Editore

ASSOCIAZIONE
**"PROGETTO GIUSTIZIA
PENALE"**