

**L'ACQUISIZIONE PROBATORIA NELLE INDAGINI TRANSNAZIONALI: COOPERAZIONE
GIUDIZIARIA E GARANZIE DIFENSIVE**

SOMMARIO: 1. Premessa – 2. La giurisprudenza della Corte EDU sull'uso di strumenti tecnologici investigativi e la tutela delle garanzie convenzionali – 3. L'interpretazione della Corte di Giustizia dell'Unione europea – 4. Gli orientamenti delle Corti supreme nazionali: Germania, Paesi Bassi e Austria – 5. La Corte di Cassazione sull'acquisizione probatoria transnazionale: soluzioni annunciate, diritti compromessi – 6. Conclusioni.

1. Premessa

Le innovazioni tecnologiche hanno inciso su molteplici settori e, inevitabilmente, anche sul processo penale, dotandolo di nuovi e potenti mezzi che arricchiscono gli strumenti d'indagine nella disponibilità degli organi investigativi¹. Tra questi, la categoria privilegiata è oggi costituita dalle intercettazioni di comunicazioni disciplinate, sul versante europeo², dalla Direttiva 2014/41/UE sull'ordine europeo di indagine³ e, a livello interno, dagli artt. 266-271 c.p.p., che ne regolano presupposti e limiti di utilizzo. Non va, però, trascurato che questo mezzo di ricerca della prova, per la sua intrusività, mette a rischio numerosi beni giuridici oggetto di tutela nel nostro ordinamento, quali il diritto di difesa⁴ e quello di riservatezza, con riguardo sia ai soggetti direttamente interessati dall'attività di captazione, sia ai terzi incidentalmente coinvolti⁵.

Un esempio delle criticità che possono presentarsi nell'utilizzo dei suddetti strumenti di indagine è rappresentato dalle operazioni di acquisizione probatoria⁶ condotte sulle

* Dottoranda di ricerca in Pluralismi Giuridici. Prospettive Antiche e Attuali – Università degli Studi di Palermo.

¹ C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Revista Brasileira de Direito Processual Penal*, Porto Alegre, 2019, pp. 1168 e 1169.

² Il primo strumento normativo che ha disciplinato la materia delle intercettazioni a livello europeo è rappresentato dalla Convenzione di Bruxelles del 29 maggio 2000 sull'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea. Tale Convenzione è stata attuata in Italia con il D.lgs. 5 aprile 2017, n. 52, emanato in attuazione della legge delega 21 luglio 2016, n. 149.

³ Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale. In Italia, detta direttiva è stata implementata mediante il D.lgs. 21 giugno 2017, n. 108, recante Norme di attuazione della direttiva 2014/41/UE, relativa all'ordine europeo di indagine penale (GU 13.07.2017).

⁴ P. RAUCCI, *L'ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, in *Pen. dir. proc.*, 2025, p. 12 ss.

⁵ R. PRETTATO, *Digitalizzazione e giusto processo: la digital evidence nella giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *DPCE online*, 2024, pp. 721 e 722.

⁶ D. CURTOTTI-V. RIZZI-W. NOCERINO-A.M. RUSSITTO-G. GILIBERTI-G. SCARPA, *Piattaforme criptate e prova penale*, in *Sist. pen.*, 2023, p. 173 ss; M. RAMPIONI, *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, in *Giur. pen. web*, 2023, p. 25.

piattaforme *SkyEcc* ed *EncroChat*, ovvero servizi di messaggistica istantanea che forniscono un *software* sicuro per le comunicazioni private⁷. Tali sistemi consentono agli utenti di comunicare in forma anonima e sicura mediante crittografia *end-to-end*, eliminando ogni possibilità di accesso ai contenuti da parte di terzi, inclusi gli stessi fornitori del servizio. I dispositivi utilizzati presentano misure di sicurezza tecnologicamente avanzate, come un doppio sistema operativo – in modo che il sistema crittografato non sia rilevabile –, l'assenza di associazione tra SIM e *account* utente, la disabilitazione di GPS, microfono e fotocamera, sistemi di cancellazione automatica dei dati e possibilità di eliminazione degli stessi da remoto.

Oltre ai profili tecnici sin qui richiamati, un ulteriore e significativo ostacolo alle attività di accertamento è costituito dal carattere intrinsecamente a-territoriale della *digital evidence*⁸, che rende particolarmente complessa l'opera di inquadramento della competenza relativa alle operazioni di acquisizione⁹. I dati informatici, infatti, possono essere raggiunti tramite la rete *Internet* da qualunque luogo, indipendentemente dalla collocazione “fisica” del *server* che li ospita, rendendo, così, difficile l'individuazione della disciplina applicabile per la raccolta degli stessi (*lex loci* o *lex fori*)¹⁰.

In un contesto caratterizzato dall'utilizzo di tali sofisticati strumenti di protezione delle comunicazioni, capaci di favorire le attività criminose, la Francia – nel 2017 – ha avviato un'attività di indagine, acquisendo, nell'ambito di un procedimento per criminalità organizzata finalizzata al traffico di armi e stupefacenti, diversi dati informatici attraverso un'operazione massiva di *malicious hacking*, condotta, *in primis*, sulla piattaforma *EncroChat*.

Nello specifico, l'*intelligence* francese (DGSI) ha avviato le indagini introducendo nei dispositivi informatici un *trojan horse*¹¹ sotto forma di aggiornamento del sistema operativo, accedendo, così, ai dati presenti nei telefoni compromessi, inclusi i messaggi salvati, le rubriche, le note, le immagini e persino al codice identificativo del dispositivo (IMEI). In una seconda fase, il medesimo *software* è stato impiegato per monitorare le comunicazioni in tempo reale, captando i messaggi in entrata e in uscita e convogliandoli verso un *server* gestito dal Centro nazionale per il contrasto alla criminalità informatica della Gendarmerie francese¹².

Successivamente, tra il 2020 e il 2021, grazie all'impiego di una squadra investigativa comune (SIC), composta dalle autorità giudiziarie e da rappresentanti delle forze di polizia di

⁷ G. GUAGLIARDI, *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?*, in *Giur. pen.*, 2024, pp. 4 e 5.

⁸ M. PITTIRUTI, *L'apprensione all'estero della prova digitale*, in L. LUPÁRIA-L. MARAFIOTI-G. PAOLOZZI (a cura di), *Dimensione tecnologica e prova penale*, 2019, p. 205 ss; F. SIRACUSANO, *La prova digitale transnazionale: un difficile “connubio” tra innovazione e tradizione*, in *Proc. pen. giust.*, 2017, p. 178 ss; G. SOANA, *Catena di Custodia, Prova Digitale e Tecnologia Block Chain*, in *Dir. di Internet*, 2021, pp. 789 e 800; G. SPANGHER, *Servono regole di garanzia per la prova informatica*, in *Pen. Dir. e Proc.*, 2023, p. 425 ss.

⁹ C. PARODI, *L'acquisizione della prova digitale*, in *Il diritto vivente*, 2019, p. 35 ss.

¹⁰ D. CURTOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e “Vecchia Europa”: una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, p. 745 ss; D. CURTOTTI-V. RIZZI-W. NOCERINO-A.M. RUSSITTO-G. GILIBERTI-G. SCARPA, *Piattaforme criptate e prova penale*, cit., p. 175 ss; S. DE FLAMMINEIS, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *Sist. pen.*, 2024, p. 2 ss; G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, in *Pen. dir. proc.*, 2025, p. 2 ss; M. PITTIRUTI, *L'apprensione all'estero della prova digitale*, cit., p. 205 ss.

¹¹ L. MARAFIOTI, *Trojan horse: spiragli di retromarcia legislativa*, in www.questionegiustizia.it, 2023.

¹² G. GUAGLIARDI, *Utilizzo nel processo penale di messaggi criptati*, cit., p. 5 ss.

Belgio, Francia e Olanda, con il coordinamento di Europol e la collaborazione di Eurojust¹³, si è giunti alla decriptazione e allo smantellamento di due delle principali piattaforme criptate fino a quel momento conosciute¹⁴: *SkyEcc* e *EncroChat*.

Le informazioni raccolte attraverso queste operazioni hanno avuto un impatto rilevante su una pluralità di ordinamenti. Numerosi Stati membri hanno fatto ricorso ai canali di cooperazione investigativa, in particolare allo strumento dell'ordine europeo di indagine (OEI)¹⁵, al fine di ottenere dati probatori rilevanti nei rispettivi ordinamenti¹⁶. Dette acquisizioni sono state determinanti per l'incriminazione di individui coinvolti in gruppi criminali organizzati, con conseguenze giudiziarie significative che hanno travalicato i confini nazionali, dando luogo ad un acceso dibattito dottrinale e giurisprudenziale.

In primo luogo, si è discusso circa l'individuazione e la conseguente ammissibilità processuale delle prove ottenute mediante attività di *hacking* da parte delle squadre investigative e poi trasmesse alle autorità dei vari Stati membri coinvolti¹⁷. In particolare, si è posto l'interrogativo sulla categoria giuridica entro la quale ricondurre queste attività: se farle rientrare nel paradigma delle intercettazioni (artt. 266 e ss. c.p.p.), dell'acquisizione documentale (art. 234 c.p.p.), della corrispondenza (artt. 254 e 353 c.p.p.)¹⁸ o, più propriamente, delle prove informatiche (art. 234 *bis* e 244, comma 2, c.p.p.). La scelta sulla qualificazione giuridica risulta determinante poiché influisce direttamente sul regime applicabile e sulla definizione delle garanzie processuali da riconoscere.

In secondo luogo, sono state sollevate criticità riguardanti le modalità concrete di ottenimento delle prove, in quanto la Francia, invocando il segreto di Stato¹⁹, ha sottratto trasparenza al meccanismo di acquisizione dei dati, con conseguenti limitazioni per la difesa nel controllo sull'integrità e sull'origine del materiale probatorio, con inevitabili ripercussioni sul principio del contraddittorio e del giusto processo²⁰.

Infine, questo genere di attività investigative ha posto rilevanti questioni anche con riferimento alla posizione dei c.d. soggetti terzi, i quali, pur essendo estranei alla vicenda

¹³ 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 *Sist. Pen.*, 2024, p. 207.

¹⁴ P. TROISI, *I canali di ingresso delle intercettazioni assunte e decrittate all'estero*, in *Proc. pen. giust.*, 2024, p. 1591; O. MURRO - W. NOCERINO, *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, in *Pen. dir. proc.*, 2024, p. 4 ss.

¹⁵ T. BENE - L. LUPARIA - L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2016, p. 9 ss; M. DANIELE, *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite*, in *Sist. Pen.*, 2023, pp. 1 e 2; 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*, 2014, p. 113 ss; M. RAMPIONI, *I limiti di utilizzabilità della messaggistica criptata*, cit., p. 25; T. RUSSO, *Ancora in materia di esecuzione dell'ordine europeo d'indagine (OEI) tra formazione della prova e sorveglianza di massa: due questioni aperte*, in *Sist. Pen.*, 2025, p. 27 ss.

¹⁶ M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in A. CADOPPI-S. CANESTRARI-A. MANNA-M. PAPA (a cura di), *Cybercrime. Diritto e procedura penale dell'informatica*, Milano, 2018, p. 1621 ss; G. DI PAOLO, *La circolazione transfrontaliera delle prove elettroniche*, cit., p. 3 ss. D. TRIPICCIÓN, *Il regime di utilizzabilità della prova digitale formata all'estero ed acquisita tramite ordine europeo di indagine*, in *Cass. pen.*, 2024, p. 692 ss.

¹⁷ F. SIRACUSANO, *La prova digitale transnazionale*, cit., p. 180 ss.

¹⁸ M. BORGABELLO, *Il concetto di corrispondenza nella sentenza 170 del 2023 della Corte costituzionale*, in *Giur. pen. web*, 2023.

¹⁹ G. GUAGLIARDI, *Utilizzo nel processo penale di messaggi criptati*, cit., p. 17 ss.

²⁰ A. GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *Arch. pen.*, 2024, p. 3 ss; L. MASSARI, *Il diritto di difesa, questo sconosciuto: il caso dei criptofonini e degli ordini europei di indagine*, in *Dir. dif.*, 2024; P. RAUCCI, *L'ordine europeo di indagine e prove digitali*, cit., p. 21 ss.

oggetto di indagine, si sono trovati coinvolti nelle operazioni di *hacking* massivo, attraverso una forma di intercettazione indiretta che ha portato alla raccolta dei loro dati personali poi confluiti nei *server*, unitamente a quelli relativi ai destinatari delle operazioni di captazione informatica. Questo coinvolgimento, astrattamente solo “indiretto”, si ripercuote comunque sulla tutela della riservatezza e sulla protezione dei dati personali dei terzi, privi peraltro di specifici strumenti processuali atti a tutelare la loro posizione²¹.

In definitiva, è evidente come tale vicenda abbia sollevato molteplici interrogativi sui quali sono state chiamate a rispondere sia le corti “europee” – Corte europea dei diritti dell’uomo e Corte di Giustizia – sia quelle nazionali. Le decisioni intervenute, pur nella diversità degli approcci, hanno contribuito a delineare un primo perimetro interpretativo, evidenziando la necessità di un difficile equilibrio tra esigenze procedimentali e tutela dei diritti inviolabili della persona.

2. La giurisprudenza della Corte EDU sull’uso di strumenti tecnologici investigativi e la tutela delle garanzie convenzionali

Come accennato, la Corte di Strasburgo è stata chiamata a pronunciarsi sul rispetto delle garanzie convenzionali di tecniche investigative fondate sull’impiego di strumenti di sorveglianza tecnologicamente avanzati e, in particolare, di operazioni di *hacking* a carattere massivo.

Un primo significativo riferimento giurisprudenziale è rappresentato dal caso A.L. ed E.J. c. Francia²², relativo alle indagini condotte dalle autorità francesi sulla piattaforma *EncroChat*. Nello specifico, due cittadini britannici detenuti nel Regno Unito deducevano la violazione dell’art. 8 CEDU, atteso che le autorità francesi avevano disposto l’acquisizione generalizzata dei dati contenuti nella piattaforma *EncroChat* e successivamente trasmessi al Regno Unito. A ciò si aggiungeva, secondo i ricorrenti, la violazione degli artt. 6 e 13 CEDU, per la mancanza di rimedi effettivi volti a contestare nell’ordinamento inglese l’ottenimento e l’utilizzazione delle informazioni così raccolte²³.

La Corte di Strasburgo si è concentrata sull’adempimento della condizione di ammissibilità prevista dall’art. 35 CEDU, ossia l’esaurimento dei rimedi interni, riaffermando il carattere sussidiario del meccanismo di tutela predisposto dalla CEDU.

Infatti, esaminata la normativa nazionale, la Corte ha concluso che, ai sensi dell’art. 694-41 del codice di procedura penale francese²⁴, i ricorrenti, seppur di nazionalità britannica, avevano a disposizione strumenti giuridici idonei a contestare la legittimità e la proporzionalità della misura di raccolta dei dati. In particolare, essi avrebbero potuto richiedere l’esclusione delle prove acquisite mediante l’ordine europeo di indagine, alle stesse condizioni e secondo le medesime procedure riconosciute a un soggetto sottoposto ad indagine in Francia²⁵. Orbene, la scelta dei ricorrenti di non sottoporsi alla legislazione dello

²¹ G. SPANGHER, *Criptofonini: sono “in gioco” diritti fondamentali*, in *Cass. pen.*, 2024, p. 173 ss.

²² Corte Europea dei Diritti dell’Uomo, Quinta Sezione, A.L. c. France e E.J. c. France, ricorsi nn. 44715/20 e 47930/21, del 24 settembre 2024, in <https://hudoc.echr.coe.int/eng?i=002-14395>.

²³ T. ZAPPÀ, *La sorte del diritto di difesa nel complicato rapporto tra evoluzione tecnologica ed esigenze investigative*, in *Il diritto vivente*, 2025.

²⁴ <https://hudoc.echr.coe.int/eng?i=002-14395>, cit.

²⁵ T. ZAPPÀ, *La sorte del diritto di difesa*, cit.

Stato convenuto non li ha esonerati dal loro obbligo di esperire i mezzi di ricorso interni disponibili in tale Stato.

Di conseguenza, difettando il requisito di cui all'art. 35 CEDU, la Corte europea ha dichiarato inammissibili i ricorsi, senza pronunciarsi nel merito delle questioni sollevate e lasciando, così, irrisolti profili di grande rilievo. È, infatti, evidente come i giudici di Strasburgo abbiano scelto di non esporsi, trincerandosi dietro la, pur doverosa, declaratoria di inammissibilità e liquidando – forse con eccessiva rapidità – un caso che sollevava interrogativi di primaria rilevanza circa il rapporto tra esigenze investigative (transnazionali) e tutela dei diritti fondamentali.

È evidente che, all'esito di questa decisione, la Corte non ha offerto un adeguato scrutinio sul rispetto delle garanzie convenzionali e, in particolare, sui diritti di difesa e sul diritto a un equo processo, che avrebbero richiesto una valutazione approfondita, in virtù della natura intrusiva delle operazioni di *hacking* e della successiva circolazione dei dati personali tra le autorità di diversi Stati membri.

Un diverso approccio si rinviene nella sentenza della Grande Camera della Corte EDU del 26 settembre 2023, *Yüksel Yalçinkaya c. Turchia*²⁶, che, pur trattando una vicenda del tutto distinta rispetto a quella relativa ad *Encrochat* e *SkyEcc*, ha affrontato problematiche affini sotto il profilo delle garanzie processuali. In particolare, questo caso riguardava la condanna del ricorrente per appartenenza a un'organizzazione terroristica armata, c.d. *FETÖ/PDY* (in precedenza nota come “Movimento *Gülen*”), ritenuta dalle autorità turche responsabile del tentato colpo di Stato.

Elemento centrale della condanna era rappresentato dall'utilizzo, da parte dell'interessato, dell'applicazione di messaggistica crittografata denominata *ByLock*, che i giudici nazionali, alla luce delle attività investigative consistite nell'accesso ai *server* principali dell'applicazione e all'acquisizione dei dati ivi contenuti, avevano considerato come uno strumento concepito, in via esclusiva, per i membri del movimento e, dunque, indicativo di per sé dell'appartenenza all'organizzazione²⁷.

Orbene, nell'ambito del processo svolto dinanzi alle autorità turche non era stata riconosciuta al ricorrente la possibilità di accedere ai dati “grezzi” di *ByLock*, secretati dai servizi di *intelligence*, né quella di conoscere e contestare il materiale decriptato che lo riguardava. Inoltre, i giudici nazionali avevano omesso di considerare una serie di argomentazioni difensive che sollevavano dubbi sull'affidabilità delle modalità di acquisizione della prova²⁸, quali le incongruenze tra i diversi elenchi di utenti redatti dai servizi, le discrepanze tra il numero dei *download* e quello degli utilizzatori effettivamente perseguiti, nonché il dato – non contestato – per cui l'applicazione era stata liberamente accessibile al pubblico fino al 2016, senza alcuna restrizione di utilizzo²⁹. Elemento, quest'ultimo che smentiva la teoria dell'utilizzo esclusivo del suddetto *software* da soggetti appartenenti alle organizzazioni criminali, posta alla base della condanna.

²⁶ Corte Europea dei Diritti dell'Uomo, Grande Camera, *Yüksel Yalçinkaya c. Turchia*, ricorso n. 15669/20, del 26 settembre 2023.

²⁷ R. PRETTATO, *Digitalizzazione e giusto processo*, cit., p. 723 ss.

²⁸ J.J. OERLEMANS-D.A.G. VAN TOOR, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in *Eur. Journ. Crime Crim. Law Crim Just.*, 2022, p. 321 ss.

²⁹ T. ZAPPÀ, *La sorte del diritto di difesa*, cit.

Tenuto conto di tali carenze, la Corte EDU ha ritenuto che al ricorrente non fosse stato assicurato un effettivo diritto di difesa³⁰, con conseguente violazione delle garanzie processuali sancite dall'art. 6 CEDU.

Allo stesso tempo, i giudici sovranazionali hanno preso atto delle difficoltà tecniche e delle sfide pratiche connesse alla gestione della *digital evidence*³¹, chiarendo tuttavia che detti elementi non giustificano in alcun modo un'applicazione, per così dire, 'affievolita' delle garanzie convenzionali, riconoscendo la necessità di adottare i tradizionali *standard* procedurali per assicurare che il principio del giusto processo venga effettivamente rispettato, anche in presenza di strumenti investigativi tecnologicamente avanzati.

Ciò nondimeno, occorre rilevare come la Corte di Strasburgo, pur mostrando una crescente sensibilità rispetto alle questioni sollevate dalla *digital evidence*, continua a muoversi con estrema cautela, senza mai oltrepassare una soglia di intervento che possa dirsi realmente innovativa. È come se i giudici europei procedessero per gradi minimi, rimanendo entro una sorta di "*comfort zone* interpretativa". Dinanzi a problematiche ormai ricorrenti e più volte sottoposte al suo esame, la Corte avrebbe potuto cogliere l'occasione per delineare orientamenti di carattere generale o vere e proprie linee guida sull'utilizzo della prova digitale, offrendo agli Stati contraenti uno schema comune di riferimento. Questo avrebbe consentito non soltanto di fornire maggiore certezza agli operatori del diritto, ma anche di favorire un'applicazione uniforme delle garanzie convenzionali nell'ambito, estremamente delicato, della prova tecnologica.

3. L'interpretazione della Corte di Giustizia dell'Unione europea

Un'analisi più approfondita sul tema in questione è stata offerta dalla Corte di Giustizia dell'Unione europea, la quale, con la sentenza del 30 aprile 2024³², si è pronunciata sul caso *EncroChat*, chiarendo i presupposti di legittimità relativi alla trasmissione e all'utilizzo delle prove nei procedimenti penali transnazionali attraverso lo strumento dell'ordine europeo di indagine³³.

La decisione trae origine da una questione pregiudiziale sollevata dal Tribunale di Berlino (*Landgericht Berlin*), chiamato a valutare la legittimità di tre ordini europei di indagine emessi dalla Procura generale di Francoforte (*Generalstaatsanwaltschaft Frankfurt am Main*) nell'ambito di un procedimento penale relativo a un traffico di sostanze stupefacenti³⁴.

Le questioni sottoposte ai giudici di Lussemburgo erano molteplici.

La prima ha riguardato la legittimità dell'OEI emesso dalla Procura di Francoforte al fine di ottenere prove già nella disponibilità delle autorità francesi³⁵.

³⁰ M. DANIELE, *Oei e messaggi digitali già acquisiti all'estero*, in *Sist. Pen.*, 2025, p. 29.

³¹ R. PRETTATO, *Digitalizzazione e giusto processo*, cit., p. 729 ss.

³² Corte di Giustizia dell'Unione Europea, Grande Sezione, sent. C-670/22, del 30 aprile 2024.

³³ N. GALLO, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, in *Arch. pen.*, 2023, p. 8 ss; L. GIORDANO, *La Corte di giustizia dell'UE sui criptofonini*, in *Ius Giusfrè*, 2024; E. LORENZETTO, *Il caso Encrochat e l'ordine europeo di indagine penale nel la staffetta fra Corte di giustizia e diritto dello Stato di emissione*, in *Cass. pen.*, 2024, p. 2887; G. SPANGHER, *La Corte di Giustizia e i criptofonini*, in *Giustizia insieme*, 2024.

³⁴ R. BELFIORE, *L'ordine europeo di indagine nella sentenza "encrochat" della Corte di Giustizia UE*, in *Dir. e proc. pen.*, 2024, p. 1264; A. GAUDIERI, *OEI: la decisione della CGUE sul caso dei criptofonini*, in *Pen. dir. e proc.*, 2024, p. 2.

³⁵ S. RAGAZZI - F. SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate*, cit., p. 218.

La Corte, innanzitutto, ha rilevato che, ai sensi dell'art. 1, par. 1, della direttiva 2014/41, l'OEI può riguardare sia il compimento di specifici atti volti all'acquisizione di prove, sia l'ottenimento di prove già in possesso delle autorità competenti dello Stato di esecuzione. Inoltre, ha chiarito che un simile ordine può essere emesso dal pubblico ministero senza la necessità di una convalida giudiziale, purché siano rispettate le stesse condizioni che regolerebbero la trasmissione di prove analoghe in un contesto puramente interno³⁶.

A questo proposito, è stato richiamato l'art. 6, par. 1, della direttiva 2014/41, che impone all'autorità di emissione un duplice vaglio³⁷: da un lato, quello di necessità e proporzionalità dell'OEI rispetto al procedimento in corso, con particolare attenzione ai diritti della persona indagata o imputata; dall'altro, quello di conformità dell'atto di indagine richiesto alle condizioni previste dal proprio diritto nazionale³⁸.

Questo approccio, secondo la Corte, contribuisce ad evitare forme di abuso nell'utilizzo dell'OEI, preservandone la funzione di strumento eccezionale e circoscritto a situazioni giustificate da esigenze investigative concrete e proporzionate³⁹. Tuttavia, è opportuno evidenziare come la raccolta delle prove avvenuta mediante intercettazioni di massa su piattaforme criptate, unitamente al mancato accesso all'algoritmo di decrittazione, non scongiuri il rischio di elusione della normativa dello Stato di emissione.

La seconda questione ha avuto ad oggetto la qualificazione giuridica delle attività svolte dalle autorità francesi, belghe e olandesi con il supporto di Eurojust ed Europol, la definizione di intercettazione e la portata dell'obbligo di notifica agli Stati interessati⁴⁰.

Preliminarmente, l'organo di giustizia ha ricondotto tali operazioni alla nozione di intercettazione, quantomeno ai fini dell'ordine europeo di indagine⁴¹. In particolare, ha precisato che rientra in questa categoria l'utilizzo di un captatore installato su apparecchi terminali, diretto a estrarre dati relativi al traffico, all'ubicazione e alle comunicazioni di un servizio basato su *internet*, fornendo così una definizione ad ampio spettro, che consente di ricomprendervi non soltanto la captazione "in tempo reale", ma anche i contenuti già memorizzati sui dispositivi⁴².

Inoltre, la Corte ha ribadito che siffatte attività determinano un'ingerenza particolarmente significativa nel diritto al rispetto della vita privata e delle comunicazioni, sancito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea. Ne consegue che gli Stati membri sono tenuti a garantire che, nell'ambito di un procedimento penale, siano rispettati i diritti di difesa e le garanzie di un equo processo nella valutazione delle prove ottenute tramite OEI; in mancanza di tali presupposti, le prove devono essere escluse.

³⁶ Secondo quanto stabilito dall'art. 2 della direttiva 2014/41 relativa all'ordine europeo di indagine penale, il pubblico ministero figura espressamente tra le autorità giudiziarie che, al pari del giudice, dell'organo giurisdizionale o del magistrato inquirente, sono intese come «autorità di emissione». Cfr. Corte di giustizia dell'Unione Europea, Sezione seconda, sent. C-635/23, del 10 luglio 2025. T. RUSSO, *Ancora in materia di esecuzione dell'ordine europeo d'indagine*, cit., p. 36 ss; V. TONDI, *La Corte di Giustizia sul caso encrochat: le importanti indicazioni della grande sezione sulla circolazione dei dati mediante ordine europeo di indagine*, in *Proc. pen. giust.*, 2024, p. 837;

³⁷ T. ZAPPÀ, *La sorte del diritto di difesa*, cit.

³⁸ G. SPANGHER, *La Corte di Giustizia e i criptofonimi*, cit.; P. TROISI, *I canali di ingresso delle intercettazioni*, cit. pp. 1594 e 1595.

³⁹ R. BELFIORE, *L'ordine europeo di indagine*, cit., p. 1266.

⁴⁰ S. RAGAZZI - F. SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate*, cit., p. 219; V. TONDI, *La Corte di Giustizia sul caso encrochat*, cit., p. 838 ss.

⁴¹ M. DANIELE, *Oei e messaggi digitali già acquisiti all'estero*, cit., p. 13.

⁴² F. NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in *Sist. pen.*, 2024, p. 201; P. TROISI, *I canali di ingresso delle intercettazioni*, cit. p. 1603.

Dopodiché, muovendo dalla suddetta qualificazione, i giudici europei hanno aggiunto che le misure di intercettazione devono essere notificate allo Stato membro nel quale si trova il soggetto interessato, riconoscendo all'autorità destinataria la possibilità di opporsi⁴³ o interrompere l'attività qualora essa non sarebbe stata autorizzata in un procedimento interno analogo⁴⁴.

In questa prospettiva, la Corte ha sottolineato che l'obbligo di notifica non risponde soltanto alla necessità di preservare la sovranità dello Stato membro interessato, ma persegue anche l'obiettivo di garantire che il livello di tutela riconosciuto nell'ordinamento nazionale in materia di intercettazioni non venga compromesso. Un simile meccanismo, infatti, è funzionale a proteggere i diritti delle persone terze coinvolte, estendendosi, altresì, all'utilizzazione dei dati ai fini dell'esercizio dell'azione penale nello Stato membro destinatario della notifica⁴⁵.

La terza questione ha riguardato il principio di effettività e, in particolare, le conseguenze giuridiche derivanti dall'acquisizione di prove in violazione del diritto dell'Unione europea. Sul punto, si è precisato che i giudici nazionali sono tenuti a escludere dal processo le prove rispetto alle quali le parti non abbiano avuto la possibilità concreta di formulare osservazioni efficaci, soprattutto quando esse siano idonee a incidere in modo determinante sulla ricostruzione dei fatti.

È evidente, dunque, la centralità attribuita al contraddittorio e al pieno esercizio del diritto di difesa, che rischierebbero di essere gravemente compromessi qualora non fosse garantito all'imputato il diritto di confrontarsi con il materiale probatorio posto a suo carico. Ciononostante, va osservato come questo principio, pur affermato con chiarezza dalla Corte, non abbia sempre trovato una coerente applicazione nelle giurisprudenze nazionali che, in più occasioni, hanno ammesso all'interno dei processi prove acquisite tramite l'ordine d'indagine europeo senza garantire alla difesa una reale possibilità di contestazione.

Inoltre, nella motivazione della sentenza sono stati ribaditi alcuni principi generali destinati a orientare lo svolgimento delle indagini transnazionali. Da un lato, la Corte ha sottolineato il rilievo del principio di fiducia reciproca tra Stati membri, particolarmente significativo nel contesto delle squadre investigative comuni; dall'altro, ha richiamato la necessità di preservare la sovranità statale, chiarendo che l'art. 31 della direttiva OEI⁴⁶ non si

⁴³ C. DE LUCA, *L'opposizione al riconoscimento dell'ordine europeo d'indagine (OEI) proveniente dall'estero: verso un mutamento di prospettiva?*, in *Cass. pen.*, 2024, p. 2376.

⁴⁴ G. SPANGHER, *La Corte di Giustizia e i criptofofoni*, cit.

⁴⁵ M. DANIELE, *La sfera d'uso delle prove raccolte*, in M. DANIELE-R.E. KOSTORIS (a cura di), *L'ordine europeo d'indagine penale*, Torino, 2018, p. 186; A. DIDDÌ, *Specifici atti di indagine*, in F. RUGGIERI (a cura di), *Processo penale e regole europee. Atti, diritti, soggetti e decisioni*, Torino, 2018, p. 99; T. RUSSO, *Ancora in materia di esecuzione dell'ordine europeo d'indagine*, cit., p. 38; P. TROISI, *I canali di ingresso delle intercettazioni*, cit. p. 1599.

⁴⁶ Articolo 31: Notifica allo Stato membro nel quale si trova la persona soggetta a intercettazione e la cui assistenza tecnica non è necessaria - 1. Se, ai fini del compimento di un atto di indagine, l'intercettazione di telecomunicazioni è autorizzata dall'autorità competente di uno Stato membro (lo «Stato membro di intercettazione») e l'indirizzo di comunicazione della persona soggetta a intercettazione indicata nell'ordine di intercettazione è utilizzato sul territorio di un altro Stato membro (lo «Stato membro notificato») la cui assistenza tecnica non è necessaria per effettuare l'intercettazione, lo Stato membro di intercettazione ne dà notifica all'autorità competente dello Stato membro notificato dell'intercettazione: a) prima dell'intercettazione, qualora l'autorità competente dello Stato membro di intercettazione sappia, al momento di ordinare l'intercettazione, che la persona soggetta a intercettazione e si trova o si troverà sul territorio dello Stato membro notificato; b) durante l'intercettazione o ad intercettazione effettuata, non appena venga a conoscenza del fatto che la persona soggetta a intercettazione si trova, o si trovava durante l'intercettazione, sul territorio dello Stato membro notificato. 2. La notifica di cui al paragrafo 1 è effettuata utilizzando il modulo di cui all'allegato C. 3.

limita a tutelare la competenza dello Stato notificato, ma mira anche a garantire la protezione dei diritti delle persone coinvolte.

Parallelamente, ha evidenziato che l'autonomia procedurale degli Stati membri incontra limiti precisi fissati dal principio di equivalenza, con il quale si vieta di adottare regole meno favorevoli rispetto a quelle previste per situazioni interne analoghe, e dal principio di effettività, che osta all'operatività di discipline tali da rendere impossibile o eccessivamente gravoso l'esercizio dei diritti riconosciuti dal diritto dell'Unione.

Infine, la quarta questione ha riguardato il principio della trasparenza, strettamente connesso alla necessità di garantire il rispetto dei diritti della difesa e di un giusto processo⁴⁷. In particolare, la Corte, nella sentenza in esame, ha chiarito che la verifica dell'integrità dei dati acquisiti non può avvenire nella fase di emissione dell'ordine europeo di indagine, ma soltanto nel momento in cui le prove divengono effettivamente disponibili alle autorità competenti e vengono introdotte nel procedimento penale⁴⁸. È, dunque, nella sede del contraddittorio sulla loro utilizzabilità, o al più tardi in quella della valutazione probatoria, che l'eventuale opacità delle modalità di acquisizione assume rilevanza giuridica, soprattutto quando si tratti di elementi decisivi ai fini della ricostruzione dei fatti⁴⁹.

In conclusione, è stata ribadita l'esigenza di mantenere un costante equilibrio tra l'interesse pubblico alla repressione dei reati e la tutela dei diritti fondamentali degli individui, ricordando che tali garanzie si estendono non soltanto agli indagati, ma anche ai terzi, la cui vita privata può essere compromessa dallo svolgimento indagini invasive mediante l'utilizzo di strumenti tecnologicamente sofisticati⁵⁰.

La portata della sentenza, pertanto, non si esaurisce nel caso specifico, ma assume un rilievo sistematico: essa fissa principi di diritto destinati a orientare le giurisprudenze nazionali nell'utilizzo delle prove digitali acquisite all'estero, imponendo alle corti degli Stati membri un adeguamento costante e coerente con i parametri stabiliti dalla Corte di Giustizia.

4. Gli orientamenti delle Corti supreme nazionali: Germania, Paesi Bassi e Austria

Sul piano nazionale, meritano attenzione le pronunce delle Corti tedesca, olandese e austriaca che offrono approcci diversi sull'utilizzo della prova digitale entro i confini domestici.

Qualora l'intercettazione non sia ammessa in un caso interno analogo, l'autorità competente dello Stato membro notificato può, senza ritardo e al più tardi entro 96 ore dalla ricezione della notifica di cui al paragrafo 1, notificare all'autorità competente dello Stato membro di intercettazione che: a) l'intercettazione non può essere effettuata o si pone fine alla medesima; e b) se necessario, gli eventuali risultati dell'intercettazione già ottenuti mentre la persona soggetta ad intercettazione si trovava sul suo territorio non possono essere utilizzati o possono essere utilizzati solo alle condizioni da essa specificate. L'autorità competente dello Stato membro notificato informa l'autorità competente dello Stato membro di intercettazione dei motivi di tali condizioni. 4. L'articolo 5, paragrafo 2, si applica, *mutatis mutandis*, alla notifica di cui al paragrafo 2.

⁴⁷ L. BERNARDINI, *On Encrypted Messages and Clear Verdicts – the Encro Chat Case before the Court of Justice (Case C-670/22, MN)*, in *EU Law Live*, 2024.

⁴⁸ R. BELFIORE, *Immediatezza e prova transnazionale*, in *Cass. pen.*, 2021, p. 2197; M. DANIELE, *Oei e messaggi digitali già acquisiti all'estero*, cit., p. 14 ss.

⁴⁹ A. GAITO, *Comunicazioni criptate ed esigenze difensive*, cit., p. 8 ss.; E. LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale*, in *Cass. pen.*, 2024, p. 185 ss.

⁵⁰ T. RUSSO, *Ancora in materia di esecuzione dell'ordine europeo d'indagine*, cit., p. 40.

La Corte di giustizia federale tedesca (*Bundesgerichtshof*), con decisione del 2 marzo 2022⁵¹, ha riconosciuto la piena utilizzabilità delle conversazioni ottenute dalle autorità tedesche attraverso un OEI rivolto alla Francia. Innanzitutto, i giudici hanno chiarito che gli atti di indagine compiuti dalle autorità francesi non possono essere sottoposti a verifica secondo i parametri del diritto tedesco. Quindi, secondo questa impostazione, non risulta decisivo stabilire se una misura analoga sarebbe stata autorizzabile in Germania, poiché il riesame della questione, alla luce del diritto straniero, non costituisce condizione necessaria per il trasferimento e l'utilizzo delle prove raccolte in conformità al diritto dello Stato di origine⁵².

Inoltre, le differenze esistenti tra i presupposti richiesti in Francia e quelli previsti in Germania per l'adozione di determinate attività investigative trovano adeguato contemperamento nel § 261 del codice di procedura penale tedesco, che sancisce il principio del libero convincimento del giudice nella valutazione della prova. Conseguentemente, la Corte ha escluso la sussistenza di una violazione dei diritti fondamentali e dei principi sanciti dal diritto europeo, sottolineando come l'operato delle autorità francesi non rappresentasse una forma di "sorveglianza di massa" su un numero indefinito di utenti, ma avesse piuttosto avuto ad oggetto una precisa piattaforma – *EncroChat* – progettata e utilizzata prevalentemente quale strumento di supporto ad attività criminali. A conferma di ciò, rileva la circostanza che i dispositivi sui quali era installato il suddetto *software* – ossia i criptofonini – non fossero reperibili attraverso i canali ordinari di distribuzione e comportassero costi particolarmente elevati, tali da renderne l'impiego circoscritto a contesti criminali caratterizzati da un alto livello di organizzazione.

Infine, i giudici tedeschi hanno ritenuto legittima anche l'acquisizione preventiva di detti elementi investigativi mediante trasferimenti effettuati dai servizi di *intelligence* prima dell'emissione dell'ordine europeo di indagine, richiamando sul punto il principio sovranazionale che consente la trasmissione di informazioni tra autorità di polizia di diversi Stati membri⁵³.

Questa pronuncia non ha eliminato le perplessità sulla reale affidabilità del materiale probatorio, dal momento che l'integrità dei dati trasmessi non può essere verificata a causa del segreto di Stato opposto dalle autorità francesi. È quindi evidente che, nel bilanciamento tra diritti fondamentali dell'individuo ed esigenze investigative e di sicurezza pubblica, la Corte tedesca abbia privilegiato in modo marcato queste ultime, riducendo così lo spazio di tutela delle garanzie difensive.

Una soluzione diversa è stata adottata dalla Corte Suprema dei Paesi Bassi (*Hoge Raad*), con la decisione del 13 giugno 2023⁵⁴ su domanda pregiudiziale della Corte distrettuale dei Paesi Bassi Settentrionali.

Il caso in questione presenta profili peculiari rispetto agli altri, in quanto le autorità olandesi, facendo parte delle SIC, hanno partecipato attivamente alle attività di indagine, le quali sono state autorizzate mediante appositi provvedimenti emessi dal giudice competente.

Orbene, la Corte olandese, pur trovandosi in una situazione di favore rispetto alle altre corti nazionali, poiché nei procedimenti sottoposti al suo esame non emergevano particolari criticità in ordine all'acquisizione probatoria, ha ritenuto opportuno formulare delle conclusioni di portata più ampia.

⁵¹ <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html>.

⁵² T. ZAPPÀ, *La sorte del diritto di difesa*, cit.

⁵³ S. RAGAZZI - F. SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate*, cit., p. 210 ss.

⁵⁴ <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2023:913>.

In primo luogo, ha chiarito che, quando le indagini vengono condotte da autorità straniere, si applicano i requisiti previsti dal diritto olandese per l'adozione della misura investigativa solo se l'iniziativa è della stessa autorità olandese. Invece, l'autorizzazione preventiva del giudice nazionale non è necessaria nel caso in cui le indagini si svolgano o siano già state svolte dalle autorità straniere, e queste rendano disponibili i risultati delle investigazioni. Opera, così, una presunzione di legittimità della raccolta dei dati esteri, potendo questa essere sindacata dal giudice olandese unicamente quando emergano evidenti segnali di inaffidabilità dei dati o di illegittimità del metodo di raccolta degli stessi.

In secondo luogo, ha stabilito che in caso di acquisizione di materiale probatorio da un altro Stato, il giudice nazionale deve partire dall'assunto che la raccolta dei dati sia avvenuta in maniera affidabile, mentre è tenuto a esercitare un vaglio di affidabilità solo quando emergano concrete indicazioni di inaffidabilità o laddove le modalità di acquisizione siano rilevanti per la valutazione della prova ai fini del rispetto delle garanzie del giusto processo.

In terzo luogo, la Corte ha sottolineato che, pur non essendo previsto dal codice di rito olandese, il pubblico ministero può comunque richiedere un'autorizzazione preventiva al giudice per lo svolgimento di attività investigative particolarmente invasive o non disciplinate dall'ordinamento nazionale⁵⁵.

La decisione della Corte Suprema olandese evidenzia, quindi, una chiara distinzione tra la responsabilità delle autorità straniere che conducono le indagini e il ruolo del giudice nazionale nella valutazione della legittimità (*ex ante* e/o *ex post*) e dell'utilizzabilità delle prove.

Infine, risulta più restrittivo l'orientamento della Corte Suprema austriaca⁵⁶. Quest'ultima, richiamandosi alla giurisprudenza della Corte di Giustizia⁵⁷, ha affermato, in maniera netta, che le prove raccolte da autorità investigative straniere su dispositivi mobili situati in Austria non possono essere utilizzate quando i metodi impiegati non siano consentiti dal diritto nazionale.

La pronuncia si distingue dalle altre perché compie un passo ulteriore rispetto alla giurisprudenza tedesca e olandese: la Corte, infatti, ha sottolineato che l'autorità emittente l'OEI deve fornire al pubblico ministero austriaco informazioni sufficienti per consentirgli di valutare in concreto le modalità di raccolta dei dati e, conseguentemente, la loro utilizzabilità processuale. Inoltre, ha precisato che la legge austriaca non concede al pubblico ministero alcuna discrezionalità nell'autorizzare provvedimenti investigativi. Infatti, qualora questi ultimi non risultino compatibili con l'ordinamento austriaco, l'utilizzo delle prove deve essere categoricamente escluso, evitando così che le garanzie interne possano essere aggirate mediante il ricorso a canali investigativi esteri⁵⁸.

In definitiva, il criterio dirimente individuato dalla Corte Suprema austriaca consiste nell'accertare se la misura investigativa sarebbe stata legittima anche secondo la *lex fori* dell'ordinamento in cui i dati vengono utilizzati, riaffermando così la centralità del principio di legalità e la non sacrificabilità delle tutele difensive.

La rilevanza di tale pronuncia può essere apprezzata oltre i ristretti confini nazionali, poiché sancisce con fermezza la non elusività delle garanzie legali interne a fronte di misure

⁵⁵ S. RAGAZZI - F. SPIEZIA, *Decifrare, acquisire e utilizzare le comunicazioni criptate*, cit., p. 211 ss.

⁵⁶ Suprema Corte austriaca (OGH *Entscheidung*), sent. n. 14Os107, del 5 novembre, 2024; Suprema Corte austriaca (OGH *Entscheidung*), sent. n. 11Os129, del 13 novembre, 2024.

⁵⁷ Corte di Giustizia dell'Unione Europea, Grande Sezione, sent. C-670/22, del 30 aprile 2024, cit.

⁵⁸ C. LÖDDEN, *Austrian Supreme Court Rules on the Use of SkyECC-Evidence Collected by Foreign Authorities*, in *Joint defense team*, 2025.

investigative segrete idonee adottate da autorità straniera e idonee a incidere sui diritti fondamentali.

In conclusione, dal confronto tra le pronunce esaminate emerge un quadro europeo eterogeneo: la Germania tende a privilegiare le esigenze investigative, l'Austria adotta un rigoroso rispetto delle garanzie interne, mentre i Paesi Bassi seguono una posizione intermedia, riconoscendo la legittimità dei dati esteri, ma prevedendo verifiche di affidabilità qualora ciò sia necessario a garantire il rispetto del giusto processo. Tali differenze evidenziano la significativa variabilità nel trattamento delle prove digitali e sottolineano l'importanza di un continuo dialogo giurisprudenziale a livello europeo finalizzato a bilanciare efficacia investigativa e tutela dei diritti fondamentali.

5. *La Corte di Cassazione sull'acquisizione probatoria transnazionale: soluzioni annunciate, diritti compromessi*

Nel panorama nazionale italiano, assumono particolare rilievo le due sentenze c.d. gemelle⁵⁹ della Corte di Cassazione a Sezioni Unite, chiamata a pronunciarsi sulla questione in esame nel tentativo di fornire un orientamento unitario. Il tema, infatti, era stato già più volte sottoposto all'attenzione delle sezioni semplici, le quali avevano adottato soluzioni tra loro difformi, dando luogo a significative oscillazioni giurisprudenziali⁶⁰.

Le Sezioni Unite sono state chiamate a pronunciarsi su due questioni. La prima ha riguardato la qualificazione giuridica degli atti trasmessi dalla Francia e, successivamente, acquisiti dal pubblico ministero italiano tramite ordine europeo di indagine.

A tal proposito, la Corte ha ricondotto tale attività nell'ambito delle intercettazioni, ritenendo applicabile l'art. 270 c.p.p. e riconoscendo al pubblico ministero la possibilità di acquisire i dati in parola senza necessità di una preventiva autorizzazione da parte del giudice competente per il nuovo procedimento⁶¹.

La Cassazione ha fondato la sua conclusione sul principio, consolidato a livello interno, secondo cui il pubblico ministero può chiedere e ottenere la disponibilità di prove già formate in un determinato processo per produrle in un altro, anche se originariamente soggette ad autorizzazione del giudice. Secondo questa impostazione, dunque, gli atti oggetto di ordine europeo d'indagine, in quanto prove già in possesso delle autorità competenti dello Stato di esecuzione, possono essere legittimamente richiesti e acquisiti dal pubblico ministero italiano, anche se l'attività acquisitiva svolta in un altro stato è avvenuta senza alcuna preventiva autorizzazione giudiziale.

È evidente, però, che le garanzie riconosciute dal nostro ordinamento potrebbero non essere previste con la stessa intensità in altri ordinamenti, nei quali l'accesso ai dati può avvenire secondo procedure meno rigorose, con conseguente rischio di un abbassamento del livello di tutela interno qualora dette tipologie di prove fossero automaticamente utilizzabili nel processo penale italiano.

⁵⁹ Cass., Sez. Un., 29 febbraio 2024, n. 23755, in *Cass. Pen.*, 2024, p. 2553 ss.; Cass., Sez. Un., 29 febbraio 2024, n. 23756, *ivi*, p. 2575 ss.; M. DANIELE, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, in *Sist. pen.*, 2024, p. 1.

⁶⁰ L. FILIPPI, *Criptofonini Sky-Ecc e messaggi criptati: la Corte di Cassazione attua i principi di diritto enunciati dalle Sezioni Unite*, in *Pen. dir. proc.*, 2024, p. 2 ss.; F. GIUNCHEDI, *Sezioni unite e acquisizione di dati dalla piattaforma Sky ECC: soluzioni formalmente ineccepibili, ma lesive dei diritti di difesa e del contraddittorio tecnico*, in *Proc. pen. giust.*, 2025, p. 91; G. GUAGLIARDI, *Utilizzo nel processo penale di messaggi criptati*, *cit.*, p. 32; L. PELLI, *Sezioni Unite*, in *Proc. pen. giust.*, 2024, p. 1084 ss.; T. ZAPPÀ, *La sorte del diritto di difesa*, *cit.*

⁶¹ F. GIUNCHEDI, *Sezioni unite e acquisizione di dati dalla piattaforma Sky ECC*, *cit.*, p. 93; L. PELLI, *Sezioni Unite*, *cit.*, p. 1086.

Un'ipotesi ancor più controversa è rappresentata dall'eventualità in cui – mediante l'utilizzo dell'OEI quale strumento volto a eludere le garanzie interne – il pubblico ministero deleghi all'autorità estera lo svolgimento di attività probatorie che, nell'ordinamento italiano, presupporrebbero un provvedimento autorizzativo del giudice, che verrebbe così evitato. In questa prospettiva, il ricorso all'OEI rischierebbe di tradursi in una vera e propria “scorciatoia probatoria”⁶², suscettibile di sacrificare in modo sproporzionato, per esigenze di natura investigativa, la protezione dei diritti fondamentali, soprattutto in una fase storica caratterizzata dal crescente impiego di strumenti tecnologicamente sofisticati e altamente invasivi.

La seconda questione ha riguardato il rispetto delle garanzie difensive. Sul punto, le Sezioni Unite hanno ritenuto non necessario rendere accessibile alla difesa l'algoritmo utilizzato per la decrittazione, escludendo qualsiasi rischio di alterazione dei dati, in quanto l'eventuale utilizzo di una chiave errata avrebbe determinato una mancata decrittazione, e non già una decrittazione inesatta.

Non del tutto convincente si rivela l'impostazione seguita dalla Cassazione nella parte in cui esclude la possibilità per la difesa di esercitare un controllo tecnico sulla prova digitale, realizzando, in questo modo, quella che è stata efficacemente definita una “tirannia tecnologica”⁶³, in cui non sono tanto i principi giuridici a determinare le modalità di acquisizione e utilizzazione della prova, quanto piuttosto la concreta conformazione tecnica del dato digitale, che finisce per condizionare in maniera irreversibile la realtà processuale⁶⁴.

Questo assunto si traduce inevitabilmente in una compressione del principio del giusto processo, poiché l'impossibilità di accesso ai dati non consente alla difesa neppure di nominare consulenti di parte e di instaurare un contraddittorio effettivo, indispensabile per la corretta valutazione probatoria.

In definitiva, pare che le Sezioni Unite della Corte di Cassazione abbiano affrontato con eccessiva rapidità una questione di particolare delicatezza, che avrebbe invece richiesto probabilmente un'analisi più attenta. Colpisce, in particolare, la mancata valorizzazione dei principi enunciati dalla Corte di Giustizia nella sentenza *EncroChat*, ove è stato affermato che il diritto di difesa postula la possibilità per le parti di formulare efficacemente le proprie osservazioni sulle prove potenzialmente decisive, elevando tale garanzia a condizione stessa di utilizzabilità.

L'intervento della Cassazione, così configurato, non appare pertanto idoneo ad assicurare il pieno rispetto dei diritti fondamentali che costituiscono l'architettura del processo penale: il diritto di difesa (art. 24 Cost.), il diritto al giusto processo (art. 111 Cost.) e la tutela della vita privata (art. 8 CEDU). L'approccio adottato rischia, infatti, di compromettere non solo le garanzie degli imputati, ma anche quelle dei soggetti terzi, le cui comunicazioni possano risultare, sia pure in via mediata, oggetto di attività investigative⁶⁵.

⁶² L'espressione è di L. MARAFIOTI, *Sezioni Unite e tirannie tecnologiche*, cit., pp. 8 e 9.

⁶³ L. MARAFIOTI, *Sezioni Unite e tirannie tecnologiche*, cit., p. 11.

⁶⁴ A. BARBIERI, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*, in *Giur. pen.*, 2023, p. 4 ss.

⁶⁵ Corte Europea dei Diritti dell'Uomo, Sez. I, Contrada c. Italia, ricorso n. 2507/19, del 23 maggio 2024, in *Cass. Pen.*, 2024, p. 2828 ss. Cfr. T. BENE, *Le garanzie procedurali a tutela della posizione del soggetto terzo in procedure di ablazione del diritto di proprietà*, in *Proc. pen. giust.*, 2025, p. 995 ss; S. LORUSSO, *Nessun dubbio (per la CEDU) sull'uso distorto delle intercettazioni lesivo dei terzi estranei al procedimento*, in <https://www.la-legislazione-penale.eu/nessun-dubbio-per-la-cedu-sulluso-distorto-delle-intercettazioni-lesivo-dei-terzi-estranei-al-procedimento-sergio-lorusso/>, 2025; E. SCORZA, *Diritto al rispetto della vita privata, procedimento penale e mezzi di ricerca della prova: la Corte EDU si pronuncia sulla tutela dei terzi*, in *Cass. Pen.*, 2024, p. 2840.

7. Conclusioni

L'analisi sin qui condotta evidenzia un panorama giurisprudenziale estremamente complesso e articolato, in cui le operazioni di *hacking* di massa sulle piattaforme criptate hanno rappresentato un banco di prova cruciale per i sistemi processuali nazionali, chiamati a confrontarsi con le sfide derivanti dalla digitalizzazione delle indagini.

La cooperazione giudiziaria e investigativa a livello europeo ha consentito un contrasto efficace alle reti criminali di rilevanza internazionale, trovando nell'utilizzo dell'OEI uno strumento indispensabile per rendere più incisiva la collaborazione tra le autorità di diversi paesi. Tuttavia, la questione relativa all'ammissibilità delle prove acquisite mediante tecniche investigative tecnologicamente avanzate rimane uno dei nodi più problematici del processo penale contemporaneo, anche alla luce delle ricadute che l'utilizzo di tali strumenti produce sulla tutela dell'indagato, incidendo in modo significativo sul diritto di difesa e dei terzi.

In questo contesto, infatti, sono stati acquisiti e resi utilizzabili – anche nei confronti di autorità straniere – dati e comunicazioni riferibili a soggetti estranei alle attività illecite oggetto di indagine, ai quali non è stata riconosciuta alcuna facoltà di opporsi all'uso delle informazioni raccolte, né tantomeno di chiederne la cancellazione, anche nelle ipotesi in cui tali dati si sono rivelati ininfluenti per lo svolgimento delle indagini.

Le soluzioni proposte dalle varie corti, nazionali e sovranazionali, si sono rivelate poco incisive e non pienamente idonee a garantire un equilibrio tra esigenze investigative e rispetto delle garanzie processuali. Risulta, dunque, necessario un ripensamento dell'approccio adottato dalla giurisprudenza, volto a riaffermare il valore dei principi costituzionali e sovranazionali in tema di giusto processo.

In una prospettiva *de jure condendo*, se l'adozione di un codice di procedura penale europeo appare al momento un obiettivo ambizioso e di difficile realizzazione, risulta auspicabile il raggiungimento di un maggiore grado di armonizzazione delle norme procedurali relative alla raccolta e all'utilizzabilità delle prove tra i diversi ordinamenti nazionali. Ciò consentirebbe di agevolare la circolazione tra Stati membri senza pregiudicare gli *standard* di tutela del giusto processo né lasciare eccessivi spazi di discrezionalità suscettibili di tradursi in forme di arbitrio interpretativo.

Intanto, *de jure condito*, è essenziale che i tribunali nazionali, nella valutazione dell'ammissibilità delle prove, esercitino un controllo rigoroso sul rispetto dei diritti fondamentali, assicurando che le acquisizioni probatorie avvengano nel pieno rispetto delle norme procedurali e delle garanzie difensive, anche dei soggetti terzi eventualmente coinvolti.

ABSTRACT: *Evidence Gathering in Transnational Investigations: Judicial Cooperation and Defensive Guarantees*

The use of encrypted messaging services such as Ecrochat and SkyEcc by organized crime has posed new challenges in terms of privacy protection and procedural guarantees. The investigations, launched by the French Gendarmerie and culminating in the decryption of thousands of conversations through hacking, have raised sensitive questions about the admissibility and legitimacy of the evidence obtained. This article analyzes the issue, starting with the supranational level, where it examines the guidelines of the European Court of Human Rights and the Court of Justice of the European Union, which, despite reaching

different conclusions, show a gradual adaptation of conventional guarantees to digital evidence. Secondly, the analysis focuses on the national level and, in particular, on the rulings of the Supreme Courts of some of the states involved, such as Germany, the Netherlands, Austria, and, most recently, Italy, where the Court of Cassation has adopted an approach that is not fully in line with the respect for defense guarantees. The issues addressed highlight the complexity of balancing investigative needs and fundamental rights, highlighting the need for harmonized regulatory intervention at the European level.