GIURISPRUDENZA PENALE

# 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?

di ***Giulia Guagliardi***

**Sommario. 1.** Introduzione. - **2** Premessa. - **2.1.** I nuovi criptofonini: EncroChat e Sky ECC. - **2.2.** Le operazioni di "intercettazione": *the hack*. - **2.3.** Brevi cenni sulla disciplina dell'Ordine Europeo di Indagine. - **3.** Gli orientamenti della Corte di cassazione. - **3.1.** La tesi che estende la dialettica procedimentale a tutti i segmenti dell'iter di acquisizione della messaggistica. - **3.2.** La tesi che individua nell'art. 234 bis la norma interna applicabile all'acquisizione della messaggistica già decriptata dall'autorità straniera. - **3.3.** La tesi ritiene applicabile alternativamente l'art. 254-bis se riguardante comunicazioni avvenute nella fase "statica" o gli artt. 266 e ss. c.p.p. se avente ad oggetto comunicazioni registrate nella fase "dinamica". - **3.4**. La tesi che ritiene applicabile l'art. 234 c.p.p. - **3.5.** La tesi che ritiene applicabile l'art. 270 c.p.p. - **4.** Le remissioni a Sezioni Unite. - **4.1.** Ordinanza 47798/2023. - **4.2.** Ordinanza 2329/24. - **4.3.** Le motivazioni delle SSUU 29 febbraio 2024. - **5.** Le questioni pendenti dinanzi alle Corti sovranazionali. - **5.1.** La sentenza della CGUE 30 aprile 2024. - **5.2.** I ricorsi pendenti dinanzi alla CEDU.

## 1. Introduzione

Nel 2022 hanno cominciato ad approdare in Cassazione una serie di ricorsi, in sede di impugnazione cautelare, con censure aventi ad oggetto la inutilizzabilità di messaggistica criptata scambiata su piattaforme quali Sky ECC ed EncroChat, acquisita dalle Procure italiane attraverso ordini europei d'indagine da autorità giudiziarie straniere, all'esito di una operazione dell'Europol.

Tali dati informatici erano stati originariamente acquisiti attraverso un'operazione di *malicious hacking* massiva, condotta *in primis* dalla Gendarmeria Francese sulla piattaforma EncroChat (i cui dettagli tecnici non sono stati integralmente divulgati poiché coperti da segreto di stato), e poi da una squadra congiunta di Belgio, Francia e Olanda sulla piattaforma SkyEcc.

Non è certamente la prima volta che la Suprema Corte si trova ad affrontare il dilemma che l'uso della messaggistica criptata pone in tema di bilanciamento tra esigenze investigative e tutela del giusto processo.

Nel precedente caso, relativo alle intercettazioni delle chat Blackberry *pin to pin*[1], le comunicazioni erano state fornite spontaneamente dalla Società Blackberry alle Procure a valle della decriptazione avvenuta in Canada[2]. Una collaborazione spontanea ma non disinteressata, poiché determinata dall'esigenza di non dover cedere le chiavi di cifratura, tanto che le doglianze delle difese - costrette ad un "atto di fede" nel risultato "semi-lavorato" trasmesso dalla Società alla Procura richiedente - si erano concentrate principalmente sulla impossibilità di accedere al dato informatico originale pre-decriptazione (alla cd. stringa informatica) e di individuare eventuali difetti di integrità della cd. *chain of custody*.

La rapida stratificazione di una serie di sentenze emesse in fase cautelare negli anni 2015-2016 (autoalimentata da reciproci richiami alle relative massime) - a fronte di ricorsi che, stante la fase cautelare, non sempre erano dettagliati rispetto agli aspetti tecnico-informatici - ha determinato un giudicato cautelare solidissimo nel quale ha sicuramente pesato di più il "piatto" delle esigenze investigative, legate al contrasto della criminalità organizzata, nazionale e transnazionale[3].

Il Report pubblicato nel 2022 dalla Direzione Investigativa Antimafia, richiamando le parole del Procuratore Giovanni Melillo, rileva che "*i gruppi criminali organizzati, di matrice italiana o allogena, ormai sono strutture che operano costantemente oltre i confini nazionali, determinando "fenomeni e dinamiche criminali complessi, sempre più proiettati su scala transnazionale e perciò bisognosi di un'intensa azione di cooperazione internazionale*".

Dai dati di analisi di Europol e delle principali Agenzie di *Law Enforcement*, è unanimemente riconosciuta la resilienza della criminalità organizzata e la capacità di saper cogliere celermente le trasformazioni tecnologiche.

---

[1] A. Testaguzza, *Intercettazioni BlackBerry - "Pin to pin"*, Archivio Penale, 2016 n. 1; S. Fùrfaro, *Le intercettazioni "pin to pin" del sistema blackberry, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche*, Archivio Penale, 2016 n. 1. Cass., Sez. VI, 20.4.2021, n. 18907; Cass., Sez. III, 9.5.2019, n. 36381; Cass., Sez. III, 26.9.2019, n. 47557; Cass., Sez. IV, 8.4.2016, n. 16670; Cass., Sez. III, 10.11.2015, n. 5818.

[2] Si tenga presente che il sistema di comunicazione di EncroChat e Sky-ECC non è basato sulla tecnologia *Pin to Pin* tipo Blackberry, vale a dire su un sistema crittografico dove le chiavi di cifratura sono collocate in un server, bensì sul sistema *end to end* che prevede la cifratura delle conversazioni mediante l'utilizzo di chiavi depositate esclusivamente sui dispositivi che colloquiano, sicché, in questa modalità, neanche il gestore del servizio è in grado di conoscere le chiavi utilizzate e di conseguenza il contenuto delle comunicazioni (Cass. I ud. 13 ottobre 2022, dep 15 febbraio 2023, n. 6363).

[3] Sul punto si veda S. Fùrfaro, *Le intercettazioni "pin to pin" del sistema blackberry, ovvero: quando il vizio di informazione tecnica porta a conclusioni equivoche*, in Archivio Penale 2016, n. 1

Non a caso, Europol nel 2017 ha avviato un progetto denominato SIRIUS, finanziato dall'UE, per approfondire la complessità delle indagini transfrontaliere che interessano le prove digitali, frutto di un'attività congiunta con Eurojust e il Network della Giustizia Europea.
In questo scenario, nel quale il progresso tecnologico procede con un ritmo incalzante, assistiamo da un lato ad una costante rincorsa delle forze di polizia all'individuazione di tecniche investigative sempre più invasive e dall'altro ad una straordinaria capacità di adattamento delle organizzazioni criminali tramite la ricerca di nuove modalità di elusione delle captazioni. Quanto più velocemente progrediscono le prime, tanto più velocemente accelerano le seconde. È necessario però chiedersi se, per colmare questa lunghezza di vantaggio, si possano sacrificare principi fondamentali del giusto processo.
Da più parti, anche oltre confine, si alza forte il coro che chiede una migliore regolamentazione a livello europeo, unitaria e puntale, delle modalità di acquisizione delle prove digitali, soprattutto nel caso di indagini transfrontaliere ove si assiste alla "libera circolazione" (favorita dai nuovi strumenti di cooperazione giudiziaria) di prove acquisite in Paesi con diverse legislazioni in termini di regime di utilizzabilità e garanzie difensive. Un dibattito che si è acuito di recente, allorquando in Europa sono stati eseguiti migliaia di arresti e sequestri sulla base di messaggi criptati, originariamente acquisiti attraverso un'operazione di hacking della quale non si conoscono tutti i dettagli, e poi diffusi tramite Europol a moltissime Procure europee, tra cui quelle italiane.
Sul punto, a valle di numerose pronunce di rigetto e della formazione di un contrasto giurisprudenziale, sono state rimesse due questioni alle Sezioni Unite della Cassazione in data 3 novembre 2023 dalla sezione III ed in data 15 gennaio 2024 dalla sezione VI.
La Cassazione a Sezioni Unite si è pronunciata, su entrambe, in data 29 febbraio 2024 rigettando tuttavia i ricorsi.
Il capitolo non può però dirsi definitivamente chiuso data la pendenza di procedimenti dinanzi alla Corte Europea dei Diritti dell'Uomo, nonché l'esistenza di una pronuncia della Corte di Giustizia UE che ha restituito gli atti al giudice *a quo* fissando una serie di principi ora rimessi ad una nuova decisione del Tribunale Regionale di Berlino circa l'ammissibilità delle prove.

## 2. Premessa

### 2.1. I nuovi criptofonini: EncroChat e Sky ECC

EncroChat (ormai in disuso) era una rete di comunicazioni e un fornitore di servizi con sede in Europa che consentiva lo scambio di comunicazioni criptate attraverso smartphone (cc.dd. criptofonini) dotati di doppio sistema operativo, uno ordinario (Android OS) ed uno nascosto (EncroChat OS) al fine di garantire l'anonimato e l'inviolabilità sia dell'interfaccia crittografata che del dispositivo stesso.

La piattaforma aveva preso piede tra il 2015[4] e il 2016 presentandosi come valido sostituto di un servizio di crittografia end-to-end precedentemente disabilitato, garantendo la possibilità di mandare messaggi criptati (EncroChat), effettuare chiamate criptate (EncroTalk) e scrivere note private criptate (EncroNotes), attraverso un server centrale con sede in Francia.
I documenti trapelati e ottenuti da Motherboard (Tech by VICE) nel 2020 hanno rivelato che i telefoni di EncroChat erano dispositivi con hardware modificati ai quali venivano disabilitati fotocamera, microfono, GPS e porta USB (che rimaneva solo in funzione di carica batteria), lasciando attive le chiamate vocali basate sul metodo ZRTP[5], quindi senza l'uso della rete GSM, e la messaggistica, ma con applicazioni proprietarie e crittografate (al fine di garantire la cd. *Zero-attack surface*).
Inoltre, gli utenti attraverso l'inserimento di un codice PIN (cd. *panic code*) potevano eliminare immediatamente la memoria del dispositivo; era prevista l'opzione di autodistruzione del messaggio nel dispositivo di un altro utente attraverso un *timer countdown* ed un sistema di protezione con password multiple, ciascuna impostata per attivare una procedura di distruzione in caso di errore per un numero consecutivo di tentativi.
EncroChat aveva rapidamente raggiunto circa 60.000 abbonati, nonostante il costo elevato per l'acquisto del *device* e dell'abbonamento mensile, grazie ad una sistematica campagna di marketing, che pubblicizzava tali prodotti come capaci di resistere ai tentativi esterni di ottenere l'accesso ai loro contenuti, anche grazie alla possibilità di segnalare la presenza di sistemi di individuazione (cd. *Imsi Catcher*) o di tentativi di intromissione da parte di agenti esterni.
Sky ECC, similmente ad EncroChat, era una piattaforma di messaggistica criptata che inizialmente usava l'hardware Blackberry, passando successivamente a modificare anche dispositivi Android e IPhone, sui quali la fotocamera, il microfono e il GPS venivano completamente disattivati ed i messaggi venivano crittografati ed eliminati automaticamente dopo trenta secondi.

[4] La prima versione del sito web dell'azienda archiviata dalla Wayback Machine risale al 23 settembre 2015.

[5] Il metodo di anti intercettazione telefonica noto come "metodo Zimmermann" o "ZRTP" storicamente è stato il primo standard di sicurezza per la comunicazione telefonica. L'autore del protocollo, Philip Zimmermann, ha creato uno dei primi software per la cifratura digitale della voce nel quale agli interlocutori viene richiesto di verificare verbalmente un codice di sicurezza della chiamata. Dopo che gli interlocutori hanno verificato questo codice di sicurezza (Short authentication string), la chiamata telefonica viene cifrata con lo standard di sicurezza SRTP (Secure Real Time Transport), che è in grado di rendere sicure anche le comunicazioni telefoniche tramite VoIP e anche di messaggistica.

L'applicazione di messaggistica, di proprietà della Sky Global (fornitore di servizi con sede a Vancouver, in Canada), era utilizzata da oltre 170.000 persone in tutto il mondo, con server negli Stati Uniti, in Canada e in Europa, sui quali ogni giorno venivano scambiati milioni di messaggi. Oltre il 20% della base utenti di Sky ECC era costituita da clienti con sede in Belgio e nei Paesi Bassi.
Sin dal 2016, le forze dell'ordine dei Paesi europei hanno sospettato che tali piattaforme criptate fossero utilizzate per scambiare comunicazioni relative ad attività criminale organizzata.

### *2.2.* Le operazioni di "intercettazione": *the hack*

La gendarmeria francese sin dal 2017 aveva avviato un'operazione investigativa (denominata *Emma 95*) sui telefoni dotati di sistema EncroChat (sequestrati in occasione di alcune retate dalla polizia).
Data la diffusione dei criptofonini EncroChat in tutto il mondo, le autorità francesi già nel 2019 avevano aperto un caso presso Eurojust. In un primo momento, i dati sono stati condivisi con i Paesi Bassi (ove era in corso un'operazione analoga denominata *Lemont 26*), attraverso la creazione di una squadra investigativa congiunta (*joint investigation team* - JIT).
Il 9 marzo 2020 Eurojust ha organizzato una videoconferenza con rappresentanti delle autorità della Francia, dei Paesi Bassi, del Regno Unito e della Germania. Nel corso di tale conferenza, i rappresentanti delle autorità della Francia e dei Paesi Bassi hanno informato i rappresentanti delle autorità degli altri Stati membri dell'indagine da essi condotta nei confronti della società di gestione dei criptofonini e della misura di intercettazione dei dati che essi avevano preso in considerazione, ossia l'installazione di un trojan[6].
Una volta appreso che i dati transitavano su server OVH SAS in Francia (Roubaix) gli investigatori sono riusciti nell'aprile 2020 ad hackerare il sistema ed ottenere le comunicazioni EncroChat (e altri dati)[7].
In una prima fase, l'agenzia di intelligence francese DGSI ha inviato ai telefoni un software trojan sotto forma di aggiornamento, che ha raccolto dati storici dalla memoria dei telefoni infettati, compresi i messaggi di chat memorizzati, le rubriche, le note e il numero IMEI univoco di ciascun telefono.

---

[6] CGUE Sentenza (Grande Sezione) del 30 aprile 2024, nella causa C-670/22, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Landgericht Berlin (Tribunale del Land, Berlino, Germania), paragrafo 21.

[7] https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.
R. Stoykova, *EncroChat: The hacker with a warrant and fair trials?,* Forensic Science International: Digital Investigation, Volume 46, September 2023, 301602

Nella seconda fase, il trojan ha intercettato i messaggi di chat in entrata e in uscita trasmettendoli ad un server gestito dal Centro per la lotta al crimine digitale (C3N) della Gendarmeria a Pontoise, utilizzando in entrambe le fasi un *load balancer* (un servizio che distribuisce il carico di lavoro di un gruppo di server) compromesso nel *data center* di Roubaix.
Dal 1° aprile 2020 i dati sono stati raccolti e trasmessi ad un *data hub* controllato dalla Gendarmeria francese. Su 64.134 utenti registrati ne sono stati intercettati 32.477 provenienti da 122 Paesi. Tra aprile e giugno 2020 le autorità francesi sono riuscite a ottenere l'IMEI dei dispositivi, gli indirizzi email degli utenti, la data e l'orario delle comunicazioni, l'ubicazione delle antenne attraverso le quali è avvenuto l'accesso, nonché testi e immagini trasmessi nelle chat in corso. Inoltre, hanno avuto accesso alla memoria completa dei dispositivi intercettati, accedendo anche alle chat di periodi precedenti alle indagini che non erano state ancora cancellate. L'attività di intercettazione si è interrotta il 13 giugno 2020, quando la società si è accorta della violazione dei sistemi da parte delle autorità e ha immediatamente inviato un messaggio di allarme a tutti gli utenti.
Presso la sede di Europol è stata istituita una task force operativa, nota come "OTF EMMA" che ha riunito investigatori ed esperti di Europol, Stati membri e paesi terzi per lavorare congiuntamente sui dati EncroChat. Da allora Europol ha organizzato il trattamento e il trasferimento dei dati alle forze dell'ordine competenti in tutta Europa attraverso i meccanismi di cooperazione giudiziaria e sostenuto le indagini *spin-off* avviate in tutto il mondo[8].
Le indagini hanno riguardato principalmente il traffico di droga su larga scala, omicidi e altri gravi crimini violenti, corruzione, riciclaggio di denaro e crimini informatici.
Il 27 giugno 2023 le autorità giudiziarie e di polizia francesi e olandesi hanno presentato una prima panoramica dei risultati. Sulla base delle informazioni recuperate, gli investigatori sono riusciti a intercettare, condividere e analizzare oltre 115 milioni di conversazioni che coinvolgono un numero stimato di oltre 60.000 utenti in tutto il mondo. Ciò ha dato il via ad un numero significativo di indagini e determinato oltre 6.500 arresti e quasi 900 milioni di euro di fondi criminali sequestrati.
Secondo Europol, molti utenti EncroChat sono passati alla piattaforma Sky ECC dopo che la prima è stata rimossa. Pertanto, le autorità di Belgio, Francia e Olanda hanno collaborato ad un'operazione (denominata *Argus*) per infiltrarsi, dal febbraio/marzo 2021, nella rete protetta Sky ECC riuscendo a decrittografare centinaia di milioni di messaggi di almeno 70.000 utenti, che la Cooperazione internazionale guidata da Europol ha permesso di rendere

[8] Ad esempio l'Operazione Venetic nel Regno Unito che ha portato ad oltre 1.550 arresti, o l'Operazione Eureka in Italia con 108 arresti e 150 perquisizioni in otto Paesi Ue.

disponibili in favore di autorità giudiziarie comunitarie, tramite Eurojust e l'emissione di appositi ordini d'indagine europei.
Dunque, la portata del materiale raccolto dalla rete Sky ECC, attraverso un'operazione investigativa i cui dettagli non sono integralmente noti, sembra essere di gran lunga maggiore rispetto a quello estratto da EncroChat.
Il 9 marzo 2021 la polizia belga ha dato esecuzione ad una maxi operazione su base internazionale, così rendendo pubblica l'avvenuta violazione del sistema criptato Sky ECC[9].

### 2.3. Brevi cenni sulla disciplina dell'Ordine Europeo di Indagine (O.E.I.)

L'art. 82, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE) stabilisce che la cooperazione giudiziaria in materia penale deve fondarsi sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie, comunemente considerato "una pietra angolare" della cooperazione giudiziaria in un sistema europeo integrato di raccolta e circolazione delle prove, per come ribadito nel Considerando 19 della Direttiva 2014/41/UE ("*La creazione di uno spazio di libertà, di sicurezza e di giustizia nell'Unione si fonda sulla fiducia reciproca e su una presunzione di conformità, da parte di tutti gli Stati membri, al diritto dell'Unione e, in particolare, ai diritti fondamentali*").
L'art. 4, par. 3, primo comma, del Trattato sull'Unione europea (TUE) stabilisce il principio di leale collaborazione, ovverosia la fiducia reciproca e la presunzione relativa che gli altri Stati membri rispettino il diritto dell'Unione e, in particolare, i diritti fondamentali nei loro rispettivi territori, tra i quali rientra ovviamente anche il diritto di difesa nei procedimenti penali.
Secondo l'art. 82, par. 2, TFUE è possibile adottare, attraverso la procedura legislativa ordinaria, direttive volte a stilare "*norme minime*" anche in tema di ammissibilità reciproca delle prove fra gli Stati membri. Su tale presupposto si è innestato l'intervento del Consiglio europeo ed il Programma di Stoccolma del 2009 con cui si è inteso invitare la Commissione a proporre "*un sistema generale di acquisizione delle prove nelle cause aventi dimensione transfrontaliera, basato sul principio del riconoscimento reciproco*" fondato su una "*solida base procedurale comune*".
Tuttavia, il tenore della proposta di Direttiva O.E.I., avanzata su iniziativa di alcuni Stati membri nel 2010, ha confermato, ancora una volta, le resistenze a cedere porzioni di sovranità nazionale in un settore, come quello delle prove, espressione di tradizioni giuridiche e culturali tipiche di ciascun ordinamento,

[9] https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

accantonando il più ambizioso progetto di edificare regole comuni – o, quantomeno armoniche – di ammissione reciproca delle prove[10].
La Direttiva 2014/41/UE, pur collocandosi sostanzialmente al di fuori del circuito degli interventi normativi finalizzati ad armonizzare le regole nazionali, è comunque considerata un cardine "evoluto" della cooperazione giudiziaria in materia penale nell'Unione europea, improntata a rapidità e tendenziale automaticità delle procedure, emancipate dal preventivo vaglio politico[11], sebbene non privo di insidie.
A partire dal 22 maggio 2017, la Direttiva sostituisce la maggior parte delle leggi esistenti in materia di trasferimento delle prove tra Stati membri nei procedimenti penali attraverso una *reductio ad unum* dei modelli esistenti (cfr. considerando n. 6 della Direttiva 2014/41), al fine di incrementare e velocizzare i meccanismi di cooperazione tra Stati dell'U.E., soprattutto in materia di criminalità transfrontaliera. Ad indicare il cambio di sistema la scelta del termine "ordinanza" e il riferimento agli Stati "di emissione" e "di esecuzione", in luogo di Stati "richiedente" e "richiesto".
Il 13 Luglio 2017 è stato pubblicato, sulla Gazzetta Ufficiale serie generale n. 162, il decreto legislativo n. 108 del 21 giugno 2017, entrato in vigore il 28 luglio 2017, che contiene le norme per la trasposizione nell'ordinamento italiano della Direttiva europea.
L'art. 1 d.lgs. 108/2017 precisa che l'attuazione della Direttiva deve assicurare il rispetto dei principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione europea in tema di diritti fondamentali, nonché in tema di diritti di libertà e di giusto processo.
L'art. 2 d.lgs. 108/2017, in linea con l'art. 1 della Direttiva 2014/41, definisce Ordine Europeo di Indagine "*il provvedimento emesso dalla autorità giudiziaria o dalla autorità amministrativa e convalidato dall'autorità giudiziaria di uno Stato membro dell'Unione europea, per compiere atti di indagine o di assunzione probatoria*[12] *che hanno ad oggetto persone o cose che si trovano nel territorio*

[10] F. Siracusano, *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in Archivio Penale, 2017, fascicolo 2, pp. 675-691

[11] Da ricordare che i primi strumenti ispirati al principio di reciproco riconoscimento per l'acquisizione delle prove sono la decisione-quadro 2003/577/GAI del Consiglio per l'esecuzione, nell'Unione europea, di provvedimenti di blocco dei beni o di sequestro probatorio e la decisione-quadro 2008/978/GAI del Consiglio disciplinante il mandato europeo di ricerca delle prove (c.d. m.e.r.) che si applica solo alle prove preesistenti (oggetti, documenti e dati presenti sul territorio dello Stato di esecuzione), rivelatasi deludente proprio per il ristretto ambito applicativo (entrata in vigore il 19 gennaio 2009 ma non è mai stata recepita dall'Italia).

[12] Rientrano nell'ambito di applicazione della direttiva, da un lato, i mezzi di ricerca della prova, come le intercettazioni e il sequestro, dall'altro, le prove in senso stretto, quali i documenti o le prove dichiarative.

*dello Stato o di un altro Stato membro dell'Unione ovvero per acquisire informazioni o prove che sono già disponibili"*.
Ai sensi dell'art. 6 della Direttiva 2014/41, l'autorità di emissione può emettere un O.E.I. solamente quando l'emissione è necessaria (cioè funzionale al procedimento all'interno del quale si innesta e capace di raggiungere il risultato cercato) e proporzionata ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata; nonché – in virtù del principio di equivalenza - solo se l'atto o gli atti di indagine richiesti nell'O.E.I. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo (così da evitare che la ricerca di una prova all'estero si trasformi nell'escamotage per eludere la corrispondente normativa nazionale[13]).
Nel d.lgs. 108/2017 non troviamo una trasposizione pedissequa delle suddette condizioni bensì solo il riferimento alla proporzione ex artt. 7 e 9, con la specifica che il legislatore italiano ha preferito operare a contrario indicando in quali casi la condizione in esame non è integrata, ossia nell'ipotesi in cui il sacrificio dei diritti dell'individuo non sia controbilanciato da idonee esigenze investigative e/o dalla gravità del reato.
Tale opzione appare solo in parte in linea con il disposto della Direttiva, che pare invece sollecitare un giudizio di necessità e proporzionalità *tout court*, anche laddove non si registrino particolari ricadute sulla sfera dei diritti dell'individuo[14].
La prevalenza del modello del mutuo riconoscimento, rispetto al modello della mutua assistenza giudiziaria, è tanto più elevata laddove si tratti di acquisire prove precostituite ossia già esistenti nello Stato di esecuzione rispetto alle quali l'autorità di emissione non fornisce "indicazioni" formali e procedurali affidandosi alla *lex loci,* in una Europa che tuttavia presenta garanzie procedurali a geometria variabile.
Tuttavia, solo un elevato grado di armonizzazione delle norme procedurali relative alla raccolta e all'ammissibilità delle prove nei paesi europei può

[13] F. Siracusano, *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in Archivio Penale, 2017, fascicolo 2, pp. 675-691

[14] Nella relazione illustrativa, allegata allo Schema di D.Lgs. recante norme di attuazione della direttiva 2014/41/UE, p. 18 si legge che "*Non si è inteso positivizzare con riguardo alle richieste di giudici e pubblici ministeri in fase attiva il principio di proporzione dal momento che l'ordinamento interno disciplina atti di indagine tipici per i quali rispetto al singolo scopo investigativo la proporzione è presunta per legge. L'art. 326 del codice di procedura penale stabilisce, infatti, che il pubblico ministero svolge le indagini "necessarie" per le determinazioni inerenti l'esercizio dell'azione penale. Le norme in materia di prova rinviano ai concetti di irrilevanza e superfluità della prova. Vale a dire cioè che il principio di proporzione è immanente al sistema interno relativo ai mezzi di prova e di ricerca della prova, calibrato anche in relazione alla gravità dei reati per cui si procede (si pensi significativamente alla materia delle intercettazioni)"*.

garantire una solida base su cui costruire quell'approccio fideistico che alimenta il principio del reciproco riconoscimento e garantire la "portabilità" di un elemento di prova *ultra fines*, senza diminuire gli standard di tutela del giusto processo e senza lasciare all'interprete spazi eccessivi che possano sconfinare nella creatività e nell'arbitrio[15].
Altrimenti il rischio è che una prova acquisita eludendo gli standard di tutela previsti nello Stato di emissione, diventi ivi importabile solo perché battezzata come "prova europea", assegnando al risultato conoscitivo acquisito un valore preponderante rispetto al metodo probatorio, quasi declassato a mero formalismo d'ostacolo alla realizzazione della pretesa punitiva dello Stato rispetto a reati di particolare allarme sociale.
Il fine del processo non è soltanto la scoperta del vero o la difesa della società, ma è anche e soprattutto il fatto che la lotta contro il crimine sia condotta "*in un certo modo, secondo un certo rito, con l'osservanza di certe regole*"[16].

## 3. Gli orientamenti della Corte di cassazione

### 3.1. La tesi che estende la dialettica procedimentale a tutti i segmenti dell'iter di acquisizione della messaggistica

La prima pronuncia degna di nota sull'uso di messaggistica criptata Sky ECC presenta un approccio sorprendentemente garantista (Cass. IV, 15 luglio 2022, dep. 7 settembre 2022, n. 32915, Lori).
La difesa infatti aveva richiesto al PM di mettere a disposizione la "*documentazione (comprensiva dei file) consegnata da Europol nel mese di marzo 2021, a seguito dell'accesso ai server di Sky ECC, con indicazione delle modalità di acquisizione da parte della stessa Europol dei dati in oggetto dai server, con annessi verbali; i verbali delle attività compiute dal R.O.N.I. dei Carabinieri Lazio per fini di polizia di cui alla dichiarata analisi preliminare*".
Istanza rigettata dal PM sulla base del rilievo che "*gli atti richiesti dalla difesa non sono contenuti nel fascicolo processuale, trattandosi di scambi informativi tra forze di polizia di paesi diversi che in quanto tali non sono processualmente utilizzabili*".
La Cassazione, nell'annullare con rinvio l'ordinanza del Tribunale del Riesame di Roma, ha affermato che "*il principio del contraddittorio implica che la dialettica procedimentale non si esplichi soltanto relativamente al vaglio del materiale acquisito ma si estenda alle modalità di acquisizione del predetto materiale. Ciò è funzionale al controllo della legittimità del procedimento*

[15] Critica sulla creatività della giurisprudenza, M. Siracusa, *Il Giano bifronte: autorità e libertà nella data retention. A proposito di una recente pronuncia della Cassazione*, p. 8, in Archivio Penale 2023, n. 2.
[16] Così NOBILI, *Il principio del libero convincimento del giudice*, Milano, 1974, 24, citato in F. Dinacci, *L'inutilizzabilità e il male captum bene retentum: vecchie superstizioni e nuove consapevolezze*, Archivio Penale 2023, n. 2.

*acquisitivo, anche nell'ottica delineata dall'art. 191 cod. proc. pen.* (…) *a condizione, naturalmente, che, come nel caso di specie, risulti l'effettiva incidenza dell'elemento dimostrativo in disamina sul convincimento del giudice*". Posto che la modalità di acquisizione rileva ai fini della verifica della corrispondenza della testualità di tale messaggistica al tenore letterale dei messaggi originariamente inviati e ricevuti, nonché delle utenze dei mittenti e dei destinatari individuati con quelli effettivi, ciò comporta imprescindibilmente la necessità di conoscere le modalità di svolgimento dell'attività investigativa svolta onde consentire la piena esplicazione del diritto di difesa.
Come si evince dalla successiva sentenza di Cassazione sul medesimo caso (sez. III, 9 gennaio 2023, n. 17794), il Tribunale del Riesame, pronunciandosi in sede di rinvio, con ordinanza del 28 settembre 2022 ha parzialmente riformato l'ordinanza del Giudice per le indagini preliminari del Tribunale di Roma sostituendo la misura della custodia cautelare in carcere con gli arresti domiciliari, relativamente al reato di cui all'art. 74, T.U. stup.
Tuttavia, dalla suddetta sentenza non è dato rilevare se il Tribunale abbia colmato la lacuna motivazionale evidenziata nel pronunciamento rescindente della Cassazione che imponeva di "*chiarire, nel contraddittorio delle parti, tutti i segmenti dell'iter di acquisizione della messaggistica*".
Vero è che in altra sentenza della Cassazione n. 19082/2023, il ricorrente, con riferimento alla sentenza Lori, ha dedotto che "*all'esito del rinvio originato dall'annullamento da essa pronunciato, è stata affermata l'inutilizzabilità del dato probatorio per la mancata realizzazione del richiesto contraddittorio*".
Ogni successivo tentativo di invocare il principio espresso dalla sentenza Lori è stato negato in virtù della mancata sovrapponibilità tra le fattispecie in esame.

### 3.2. La tesi che individua nell'art. 234 bis la norma interna applicabile all'acquisizione della messaggistica già decriptata dall'autorità straniera

Numerose sentenze della Corte di Cassazione hanno ritenuto utilizzabili i messaggi acquisiti mediante O.E.I. individuando nell'art. 234-bis c.p.p. la norma interna di riferimento alla stregua della quale l'atto di indagine avrebbe potuto essere emesso in un caso analogo interno[17].

[17] Cass. I, 1 luglio 2022, dep. 15 settembre 2022, n. 34059; Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363; Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6364; Cass, VI, 25 ottobre 2022, dep. 20 dicembre 2022, n. 48330; Cass. I, 13 gennaio 2023, dep. 5 maggio 2023, n. 19082; Cass. I, 13 gennaio 2023, dep. 5 maggio 2023, n. 19083; Cass. I, 8 febbraio 2023, dep. 8 maggio 2023, n. 19155; Cass. I, 16 febbraio 2023, dep. 27 aprile 2023, n. 17529; Cass. IV, 28 marzo 2023, dep. 28 aprile 2023, n. 17647; Cass. IV, 28 marzo 2023, dep. 10 maggio 2023, n. 19623, Cass. IV, 4 aprile 2023, dep. 4 maggio 2023, n. 18511, Cass. I, 5 aprile 2023, dep. 18 aprile 2023, n. 16347; Cass. IV, 28

Nei suddetti casi, la Corte ha richiamato innanzitutto la giurisprudenza che distingue, da un lato, le operazioni di captazione e registrazione di messaggi "in transito" dal mittente al destinatario e, dall'altro, le operazioni di decriptazione del messaggio per trasformare mere stringhe informatiche in dati intellegibili, laddove solo alle prime si applica la disciplina dell'art. 266 bis c.p.p.[18]

La Corte ha escluso l'applicazione di suddetta norma ritenendo che la messaggistica "*non è stata acquisita mediante operazioni di intercettazioni di comunicazioni telematiche ma attraverso la richiesta ad uno Stato estero, la Francia, con ordine di indagine europeo di trasmettere, in applicazione dell'art. 234 bis cod. proc. pen., previa decriptazione, messaggi di comunicazioni già avvenuti e conservati presso il server della società che gestisce il servizio di messaggistica ed acquisiti nell'osservanza dell'ordinamento interno francese*" (Cass. I, 1 luglio 2022, dep. 15 settembre 2022, n. 34059). Ciò sarebbe confermato dal fatto che l'autorità italiana non ha compilato la sezione H7 dell'O.E.I. (relativa ad attività di intercettazione telefonica/telematica), né la sezione H5 (relativa ad atti d'indagine implicanti l'acquisizione di prove in tempo reale, in modo continuo e per un determinato periodo di tempo), formulando unicamente richiesta di trasmissione di copia dei messaggi riferibili ai PIN di interesse (Cass. I ud. 13 ottobre 2022, dep 15 febbraio 2023, n. 6363).

Quanto all'assenza, lamentata dalla difesa in molti ricorsi[19], del protocollo informatico utilizzato per garantire la corrispondenza del dato originale con

---

marzo 2023, dep. 19 luglio 2023, n. 31200; Cass. IV, 28 marzo 2023, dep. 19 luglio 2023, n. 31201; Cass. IV, 28 marzo 2023, dep. 19 luglio 2023, n. 31202; Cass. I, 5 aprile 2023, dep. 18 aprile 2023, n. 16345; Cass. IV, 4 aprile 2023, dep. 4 maggio 2023, n. 18514; Cass. Sez. IV, 9 maggio 2023, dep. 5 giugno 2023, n. 23998; Cass. Sez. IV, 9 maggio 2023, dep. 5 giugno 2023, n. 23999; Cass. IV, 30 maggio 2023, dep. 13 giugno 2023, n. 25361; Cass. IV, 16 maggio 2023, dep. 15 giugno 2023, n. 25840; Cass. IV, 11 maggio 2023, dep. 27 giugno 2023, n. 27775; Cass. IV, 30 maggio 2023, dep. 27 giugno 2023, n. 27777; Cass. III, 5 luglio 2023, dep. 26 luglio 2023, n. 32495; Cass. III, 5 luglio 2023, dep. 26 luglio 2023, n. 32496; Cass. IV, 20 aprile2023, dep. 27 luglio 2023, n. 32686; Cass. IV, 30 maggio 2023, dep. 31 luglio 2023, n. 33386; Cass. IV, 13 giugno 2023, dep. 2 agosto 2023, n. 33937; Cass. IV, 16 maggio 2023, dep. 18 settembre 2023, n. 38001; Cass. IV, 16 maggio 2023, dep. 18 settembre 2023, n. 38002; Cass. III, 19 ottobre 23, dep. 24 novembre 2023, n. 47201; Cass. I, 2 febbraio 2023, dep. 18 gennaio 2024 n. 2312;

[18] *Inter alia* Cass. I, 1 luglio 2022, dep. 15 settembre 2022, n. 34059, Cass. I, 13 gennaio 2023, dep. 5 maggio 2023, n. 19082, Cass. I, 13 gennaio 2023, dep. 5 maggio 2023, n. 19083, Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363.

[19] In particolare, la difesa si doleva del fatto che l'Autorità francese, invece di veicolare il dato informatico attraverso una codifica hash, avesse utilizzato comuni file excel 3 privi della tutela di una password di protezione di scrittura, con ogni conseguenza in

quello trasmesso, la Corte ritiene che la difesa abbia confuso "*il tema della genuinità del dato decrittato con quello della garanzia di quella che viene definita come catena di custodia*" poiché "*ogni messaggio cifrato è inscindibilmente accoppiato alla sua chiave di cifratura, sicché la sola chiave esatta produrrà una decifratura corretta, dovendosi escludere che possa decifrarne una parte corretta e uno non corretta; né vi sono possibilità che una chiave errata possa decrittare il contenuto, anche parziale, del codice umano contenuto*"[20]. Ciò escluderebbe, salvo specifici e concreti elementi di segno contrario, la ricorrenza di alterazioni o manipolazioni dei testi trasmessi dopo la decriptazione.

Inoltre, ai fini della catena di custodia, la Corte ha ritenuto sufficiente che la stringa di *hash* fosse legata al contenitore, e non al contenuto, fungendo da sigillo digitale, attraverso l'uso di supporti di memoria a tecnologia ottica non riscrivibile (CD e DVD) trasmessi all'interno di buste sigilliate antieffrazione[21].

Ciò sarebbe corroborato da una "attestazione di conformità" sia del giudice francese che dell'autorità investigativa che ha eseguito l'estrazione[22], che sulla base del principio della reciproca fiducia in forza delle relazioni intercorrenti dagli stati, consente di realizzare la presunzione di legittimità degli atti compiuti dalle autorità straniere secondo la legislazione dello specifico stato straniero[23].

Quanto all'ipotesi che il controllo dell'attività di intercettazione/acquisizione della messaggistica non sia avvenuto in via esclusiva da parte dell'autorità giudiziaria, la censura secondo la Corte trascura il fatto che l'acquisizione sia avvenuta attraverso O.E.I. e che "*è stata condivisibilmente affermata l'utilizzabilità della documentazione di atti compiuti autonomamente da autorità straniere in un diverso procedimento penale all'estero, anche al di fuori dei limiti stabiliti per la loro utilizzabilità dagli artt. 238 cod. proc. pen. e 78 disp.*

---

termini di genuinità dei dati e tutela da rischio di manipolazione durante l'operazione di decrittazione.

[20] Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363.

[21] Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363.

[22] L'attestazione da parte dell'Autorità giudiziaria francese secondo la quale i dati trasmessi in esecuzione dell'O.I.E. corrispondono a quelli acquisiti nei procedimenti francesi risulterebbe attestata nel verbale di esecuzione (*Commission rogatoire*) in data 16 settembre 2021, in atti, nel quale il giudice istruttore francese, nel delegare la polizia giudiziaria al compimento dell'attività materiale di "copia", espressamente dichiara che «*Disons que les procès-verbaux dresses nous seront trasmis, avec une copie certifiée dans le meilleur délai*» («i verbali saranno trasmessi con copia certificata al più presto»).

[23] In tal senso, Cass. sez. III, 12 ottobre 2021, n. 1396, Torzi, in cui in motivazione si rinvia anche a Cass. sez. V, 16 novembre 2016, n. 1405, Ruso, Rv. 269015 - 01; a Cass. sez. II, 18 maggio 2010, n. 24776, Mutari, Rv. 247750 - 01; e a Cass. sez. I, 22 gennaio 2009, n. 21673, Pizzata, Rv. 243796; ma anche a Cass. sez. V, 13 luglio 2016, n. 45002, Crupi, Rv. 268457.

*att. cod. proc. pen., con il solo limite che tale attività non sia in contrasto con norme inderogabili e principi fondamentali, i quali, però, non si identificano necessariamente con il complesso delle regole dettate dal nostro codice di rito, spettando inoltre a chi eccepisca tale incompatibilità l'onere di dare la prova di tale incompatibilità (cfr. Sez. 5, n. 45002 del 13/07/2016, Crupi, Rv. 268457 - 01)"*[24].

Tale limite non sarebbe superato considerato che la Francia condivide i principi fondamentali dell'ordinamento europeo e si è resa garante del rispetto delle procedure dello Stato di esecuzione, fermo restando il "*pieno vigore della presunzione della regolarità dell'attività svolta, spettando al giudice straniero di verificare la correttezza della procedura e la competenza a risolvere qualsiasi questione in ordine ad eventuali irregolarità lamentate*"[25].

Su tale aspetto, una delle sentenze che ha sposato la tesi in commento ha valorizzato la presenza in atti di una informativa dalla quale sarebbero risultate "*la modalità di conservazione e di download dei dati informatici, essendo decisivi e riscontrabili i riferimenti al link e alla relativa password, implicanti la diretta interlocuzione con Eurojust, nonché il fatto che fosse stato generato un doppio codice hash*"[26].

Invero, non pare che i dati di cui all'informativa permettano di conoscere i dettagli dell'originaria operazione di acquisizione bensì solo dei successivi passaggi di trasferimento ed è interessante notare come la Corte ammetta che il "*dato conoscitivo suscettibile di contraddittorio*", non era "*realizzabile nell'immediata fase dell'originaria acquisizione e decifrazione*".

Quanto al *modus operandi* dell'autorità francese, in alcuni casi la Corte afferma che l'utilizzo della parola "*violata*"[27] o "*bucata*" [28] con riferimento alla rete Sky Ecc, da parte del Tribunale del Riesame, dovrebbe interpretarsi esclusivamente come superamento dell'ostacolo rappresentato dalle chiavi crittografate. Con ciò la Corte sembra voler allontanare l'idea che l'attività di indagine francese abbia seguito metodi non legali, evidentemente paventati dalla difesa.

Eppure in altra sentenza[29] la Cassazione sceglie un termine decisamente più esplicito ossia "*crack*" da interpretarsi come "*idonea manomissione*" del sistema operativo. Un'operazione che rimanda al concetto di hackeraggio dell'intero server più che al mero ostacolo della cifratura che rappresenterebbe semmai un *post-factum* dell'accesso abusivo.

Sul punto vi sono alcuni ricorsi che hanno dedotto maggiori informazioni in merito a quanto avvenuto in Francia. In particolare, è stato prodotto un parere

[24] Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363.
[25] Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363.
[26] Cass, VI, 25 ottobre 2022, dep. 20 dicembre 2022, n. 48330.
[27] Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6363.
[28] Cass, VI, 25 ottobre 2022, dep. 20 dicembre 2022, n. 48330.
[29] Cass. I, 2 febbraio 2023, dep. 18 gennaio 2024 n. 2312.

*pro veritate* redatto dagli avvocati francesi che permetterebbe di affermare come la tesi condivisa dalla Prima Sezione penale con la sentenza n. 34059, sull'applicabilità dell'art. 234 c.p.p. o comunque dell'art. 234 bis c.p.p., si fonderebbe su circostanze fattuali erronee[30].
Infatti, all'esito di indagini difensive, sarebbe emerso che la Francia era riuscita a entrare in possesso dei dati di comunicazione delle piattaforme EncroChat e Sky Ecc grazie a operazioni di intercettazione aventi ad oggetto i due interi sistemi di comunicazione e non singole utenze, avendo la gendarmeria francese «hackerato» i dati che transitavano sulle piattaforme[31].
In particolare, l'autorità giudiziaria di Lille nel 2019 avrebbe autorizzato l'accesso ad un intero sistema informatico e il successivo provvedimento dell'autorità giudiziaria di Parigi, volto a decriptare i messaggi individuali, si sarebbe innestato su quello adottato a Lille. Tali provvedimenti, secondo la difesa, sarebbero illegittimi sia per violazione della legislazione francese che per contrasto con i principi fondamentali della Costituzione italiana, non essendo consentito l'accesso ad un intero sistema criptato, violando il diritto alla segretezza e alla riservatezza delle comunicazioni e della corrispondenza senza l'individuazione ex ante di responsabilità penali di individui determinati. Secondo i ricorrenti, l'O.E.I. non avrebbe potuto sanare le illegittimità del provvedimento trasmesso[32].
Inoltre, la difesa – nel tentativo di rafforzare la solidità dei principi enunciati nella sentenza Lori - ha rilevato che con sentenza n. 1226 emessa in data 11/10/2022, la Corte di Cassazione francese, pronunciandosi nel procedimento per associazione finalizzata all'utilizzo di telefoni criptati, nel corso delle cui indagini erano stati acquisiti e decriptati i dati delle chat presenti sul server EncroChat, aveva annullato la decisione della Corte di appello di Nancy per violazione dell'art. 230-3 del codice di procedura penale francese, riscontrando la mancanza del certificato di originalità dei dati estratti dalle chat.
La Corte ha ritenuto non pertinente il richiamo alla suddetta sentenza poiché avente ad oggetto uno specifico provvedimento giurisdizionale dal quale non potrebbe desumersi che l'attestazione certificante la sincerità dei risultati trasmessi - non acquisita agli atti di un determinato procedimento - fosse mancante in tutti i casi in cui l'autorità francese ha acquisito dati sulle piattaforme EncroChat e Sky Ecc[33].
Nonostante gli elementi evidenziati dalla difesa, la Corte ha ritenuto che rimane *"una mera petizione di principio, del tutto indimostrata, la deduzione difensiva secondo cui l'acquisizione dei dati delle piattaforme EncroChat e Sky*

[30] Cass. I, 8 febbraio 2023, dep. 8 maggio 2023, n. 19155.
[31] Cass. I, 8 febbraio 2023, dep. 8 maggio 2023, n. 19155.
[32] Cass. IV, 28 marzo 2023, dep 19 luglio 2023, n. 31200.
[33] Cass. IV, 16 maggio 2023, dep. 15 giugno 2023, n. 25840.

*Ecc sarebbe avvenuta grazie a operazioni di intercettazione aventi ad oggetto i due interi sistemi di comunicazione e non singole utenze"*[34].
Analizzando altre sentenze della Cassazione, permane comunque incertezza rispetto a quanto effettivamente svolto dalla autorità francesi. Incertezza che – come vedremo – ha cominciato a destare perplessità nel giudice di legittimità solo con le sentenze gemelle della sezione sesta n. 44154 n. 44155 depositate il 2 novembre 2023.
In alcuni casi, la Corte ha affermato con assertività che "*l'autorità richiesta non ha ottenuto quei dati in forza di un'autorizzazione a procedere a intercettazioni di flussi in corso*"[35]. Dunque, non solo la Procura italiana avrebbe chiesto e acquisito dati statici, ma anche la Francia non avrebbe posto in essere attività d'intercettazione di comunicazioni in corso ma solo di quelle già presenti nel server.
In altri casi, la Corte ha affermato che "*dalla lettura dei provvedimenti emerge che tra i materiali trasmessi potrebbero esservi anche i risultati della acquisizione di flussi di dati avvenuta in tempo reale, potrebbero esservi, quindi, anche i risultati di attività di intercettazione autonomamente disposte dall'autorità giudiziaria francese secondo la normativa vigente in quello Stato*"[36].
Ad ogni modo, la Corte sminuisce queste incertezze, ritenendo che "*non assume rilevanza la questione (sulla quale la difesa si è lungamente soffermata) se quei dati siano stati acquisiti dalla magistratura francese ex post o in tempo reale (quindi come "dati freddi" o come "flussi di comunicazioni")*". Ciò che conta è che, quando la magistratura italiana chiese di ottenere quei dati e (a maggior ragione) quando quei dati le furono trasmessi, i flussi di comunicazione non erano certamente più in corso[37].
Inoltre, nell'analizzare la normativa (articolo 706-102-1 e art. 230-1 del codice di procedura penale francese, che consente al pubblico ministero nel corso dell'indagine, e al giudice istruttore in fase di istruzione, di avvalersi «di risorse dello Stato soggette al segreto di difesa nazionale» per accedere a dati informatici, registrarli, archiviarli e trasmetterli anche mentre vengono ricevuti e per procedere, se necessario, alla decrittazione dei dati stessi), la Corte ha concluso che – seppur non note le modalità di acquisizione – l'autorità francese aveva attestato con apposito processo verbale redatto e sottoscritto dall'ufficiale di polizia giudiziaria incaricato dell'adempimento la regolarità del

[34] Cass. I, 8 febbraio 2023, dep. 8 maggio 2023, n. 19155.
[35] Cass. IV, 28 marzo 2023, dep. 28 aprile 2023, n. 17647, Cass. IV, 30 maggio 2023, dep. 27 giugno 2023, n. 27777.
[36]Cass. I, 5 aprile 2023, dep. 18 aprile 2023, n. 16345.
[37] Cass. IV, 28 marzo 2023, dep. 28 aprile 2023, n. 17647.

trasferimento di quei dati su supporto informatico non modificabile. Ciò escluderebbe la violazione di legge[38].

Ed invero, afferma la Corte, "*anche nel sistema italiano, l'opposizione del segreto di Stato «inibisce all'autorità giudiziaria l'acquisizione e l'utilizzazione, anche indiretta, delle notizie coperte da segreto» (art. 202, comma 5, cod. proc. pen.), ma non le impedisce «di procedere in base ad elementi autonomi e indipendenti dagli atti, documenti e cose coperti dal segreto» (art. 202, comma 6). Nel caso di specie l'autorità giudiziaria francese ha ritenuto di non dover comunicare le modalità utilizzate per accedere ai dati informatici, registrarli, archiviarli e trasmetterli anche mentre vengono ricevuti e per procedere, se necessario, alla decrittazione dei dati stessi perché, nel compierla, ha utilizzato «risorse dello Stato soggette al segreto di difesa nazionale». Il segreto, dunque, non riguarda i dati acquisiti, ma solo le modalità dell'acquisizione*". A ciò deve aggiungersi che - diversamente da quanto avviene nei casi disciplinati dagli artt. 202 e 256 c.p.p. richiamati dalla difesa - il rifiuto non è stato opposto dallo Stato francese ai pubblici ministeri italiani, ma è l'autorità giudiziaria francese che, nel rispetto del proprio diritto interno, ha ritenuto di non poter rendere ostensibili quei dati, prima ancora che alla Procura italiana e (di conseguenza) ai difensori delle persone indagate, alla difesa delle persone indagate in Francia nel procedimento in relazione al quale i dati furono acquisiti[39].

Quanto alla tesi prospettata dalla difesa secondo cui la messaggistica sarebbe inutilizzabile a norma dell'art. 191 c.p.p., in quanto l'acquisizione delle risultanze digitali è frutto del lavoro di una squadra investigativa comune franco-belga-olandese, come tale inidonea a formare la prova secondo il combinato disposto dell'art. 3 e il considerando 8 della Direttiva europea n. 41/2014 come recepita dal d.lgs. n. 108/2017, la Corte ha affermato che l'art. 3 della Direttiva non prevede l'impossibilità di acquisire risultati di attività investigativa già compiuti (in ipotesi anche da squadre investigative comuni) bensì "*il divieto di istituire con l'O.I.E. le squadre comuni investigative e il conseguente divieto di acquisizione di prove acquisite nell'ambito di una squadra eventualmente così costituita*"[40].

---

[38] Cass. I, 5 aprile 2023, dep. 18 aprile 2023, n. 16345 "*i diritti della difesa devono necessariamente modularsi sulla legge dello Stato che ha dato esecuzione all'ordine di indagine. La verifica della correttezza della procedura e della legittimità dell'attività svolta, infatti, deve essere compiuta con riferimento alla legge processuale dello Stato richiesto e poiché, nel caso di specie, questo Stato può legittimamente opporre il segreto sul punto, la legittimità delle modalità di acquisizione e decrittazione dei dati deve ritenersi garantita dal controllo che su quella attività è stato compiuto dall'autorità giudiziaria francese*".

[39] Cass. Sez. IV, 9 maggio 2023, dep. 5 giugno 2023, n. 23998.

[40] Cass. I ud. 13 ottobre 2022, dep. 15 febbraio 2023, n. 6364.

Inoltre, la Corte ha escluso che la sopravvenuta disciplina in materia di acquisizione di tabulati, con l'attribuzione del potere al Giudice e non al PM, abbia reso l'acquisizione delle chat incompatibile con il diritto interno poiché nel caso di specie non si tratta di "dati esteriori" e le rassicurazioni dell'autorità francese porrebbero al riparo da qualsiasi censura in punto di legittimità delle modalità di acquisizione.
La Corte ha infine escluso l'applicabilità dell'art. 254-bis c.p.p., non essendo al cospetto di un sequestro, quanto della acquisizione di documenti informatici avvenuta con il consenso del legittimo titolare[41].

### 3.3. La tesi ritiene applicabile alternativamente l'art. 254-bis se riguardante comunicazioni avvenute nella fase "statica" o gli artt. 266 e ss. c.p.p. se avente ad oggetto comunicazioni registrate nella fase "dinamica".

Due sentenze hanno escluso l'applicazione dell'art. 234-bis c.p.p., [42] che sino a quel momento era stato invocato da tutte le sentenze della Cassazione, secondo un orientamento che sembrava ormai granitico.
Il dato di partenza è rappresentato dalle gravi carenze delle ordinanze impugnate rispetto ad alcune circostanze di fatto "*di non trascurabile importanza*":

- se l'autorità giudiziaria francese avesse avviato autonomamente, sulla base di preesistenti *notitiae criminis*, le indagini nel proprio Paese oppure se le investigazioni fossero state attivate (anche) sulla base delle sollecitazioni istruttorie che avevano sostanziato l'emissione di ordini europei di indagine da parte del pubblico ministero italiano.
- se, rispetto al momento della emissione e della trasmissione di tali ordini, le indagini compiute dall'autorità giudiziaria francese fossero state tutte definitivamente concluse, oppure se - come sembrerebbe da alcuni sintetici cenni contenuti nei provvedimenti impugnati - fossero proseguite anche sulla base delle richieste formulate dall'autorità giudiziaria italiana.

Secondo la Corte, l'assertività con la quale si era parlato di acquisizione di "dati freddi" vacillava in ragione ai riferimenti delle difese al compimento da parte dell'autorità straniera di operazioni di intercettazioni di comunicazioni in corso, pure caratterizzata dall'impiego di captatori informatici (c.d. "trojan" o "malware"), per l'acquisizione di dati di comunicazione telematica archiviati nel "server" della società e per consentire l'apprensione delle "chiavi di decifrazione" presenti negli apparecchi utilizzati dai fruitori della piattaforma di messagistica cifrata in questione.

[41] Cass. I, 8 febbraio 2023, dep. 8 maggio 2023, n. 19155.
[42] Cass. VI ud. 26 ottobre 2023, dep. 2 novembre 2023, n. 44154; Cass. VI ud. 26 ottobre 2023, dep. 2 novembre 2023, n. 44155.

Solo una volta superate tali incertezze è possibile *"dare una corretta definizione e un più preciso inquadramento normativo al mezzo di ricerca della prova di cui, volta per volta, occorreva autorizzare l'impiego. E ciò vale - come si avrà modo di rimarcare nel prosieguo - tanto più ai fini della verifica della utilizzabilità processuale di elementi di prova acquisiti all'estero con uno o più ordini europei di indagine (di seguito o.e.i.), in ragione del "principio di equivalenza" previsto dall'art. 6, par. 1, lett. b), della Direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale (di seguito Direttiva OEI), per cui tale ordine può essere emesso a condizione che l'autorità dello Stato di emissione verifichi che «l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo»"*.

Ad ogni modo, secondo la Corte, va esclusa l'applicabilità dell'art. 234-bis c.p.p. che, introdotto dal decreto-legge 18 febbraio 2015, n. 7, convertito dalla legge 17 aprile 2015, n. 43, stabilisce che "*E' sempre consentita l'acquisizione di documenti e di dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare*".

*"L'operatività della richiamata disposizione può ritenersi giustificata esclusivamente nell'ipotesi di acquisizione di documenti e dati informatici, intesi come elementi informativi "dematerializzati", che preesistevano rispetto al momento dell'avvio delle indagini da parte dell'autorità giudiziaria francese ovvero che erano stati formati al di fuori di quelle investigazioni: nel caso portato all'odierna attenzione di questa Corte, di contro, risulta in maniera sufficientemente chiara che quella acquisita è stata in parte documentazione di attività di indagine e in parte documentazione preesistente che ha, però, costituito oggetto delle ulteriori iniziative istruttorie di quella autorità straniera.*

La fattispecie ex art. 234-bis c.p.p., dunque, va delimitata alla sola acquisizione di dati informatici in ogni caso estranei, nella loro formazione, a qualsivoglia coinvolgimento di autorità investigative.

Diversamente, l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma Sky Ecc, se riguardante comunicazioni avvenute nella fase "statica", deve essere inquadrata nelle disposizioni in materia di perquisizione e sequestro e, in particolare, in quella di cui all'art. 254-bis c.p.p. (in tema di sequestri di dati informatici allocati presso fornitori di servizi informatici, telematici e di comunicazioni), mentre, se avente ad oggetto comunicazioni registrate nella fase "dinamica", deve essere ricondotta alla disciplina degli artt. 266 e ss. c.p.p. (in materia di intercettazioni).

Questo orientamento, rispetto alla individuazione dell'autorità legittimata ad emettere l'ordine di acquisizione della prova, ha dato atto della mutazione esegetica avviata da alcune decisioni della Corte di giustizia dell'Unione Europea (in particolare CGUE, Grande Camera, 2 marzo 2021 H.K., C-746/18, cit.), che ha spinto in via d'urgenza il legislatore italiano (d.l. n. 132 del 2021,

convertito nella legge n. 178 del 2021) a riformare l'art. 132 Cod. privacy, prevedendo che la procedura di acquisizione dei dati esterni di traffico telefonico e telematico esiga un provvedimento autorizzatorio motivato del giudice.

Ne deriva che "*l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione debba essere sempre autorizzata da un giudice: sarebbe davvero singolare ritenere che per l'acquisizione dei dati esterni del traffico telefonico e telematico sia necessario un preventivo provvedimento autorizzativo del giudice, mentre per compiere il sequestro di dati informatici riguardanti il contenuto delle comunicazioni oggetto di quel traffico sia sufficiente un provvedimento del pubblico ministero*".

Ciò sarebbe coerente con la sentenza della Corte Costituzionale in ordine alla estensione applicativa delle garanzie previste dall'art. 15 Cost. in materia di libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (Corte Cost., sent. n. 170 del 2023) e con le posizioni assunte in materia dalla Corte Europea dei Diritti dell'Uomo, che ha ricondotto "*sotto il cono di protezione dell'art. 8 CEDU, ove pure si fa riferimento alla "corrispondenza" tout court, i messaggi di posta elettronica (Corte EDU, sent. 5/09/2017, Barbulescu c. Romania, § 72; Corte EDU, sent. 3/04/2007, Copland c. Regno Unito, § 41), gli SMS (Corte EDU, sent. 17/12/2020, Saber c. Norvegia, § 48) e la messaggistica istantanea inviata e ricevuta tramite internet (Corte EDU, sent. Barbulescu, cit., § 74)*"[43].

Il collegio si è interrogato sulle conseguenze derivanti dalla illegittima emissione dell'ordine perché non preceduto dal necessario provvedimento del Giudice, concludendo che la difesa può far valere i mezzi di impugnazione disponibili nello stato di esecuzione (per impedire il riconoscimento dell'O.E.I. o la trasmissione della prova o comunque la sua utilizzazione) ma diverse sono le conseguenze dell'illegittimità se l'O.E.I. è stato emesso per acquisire una prova già disponibile nello stato di esecuzione. In tal caso, se la prova è stata definitivamente trasmessa da detto Stato, la difesa non ha mezzi a disposizione se non far valere la mancanza delle condizioni di ammissibilità della prova secondo l'ordinamento processuale italiano. La Direttiva 2014/411, infatti, fa salvi i diritti della difesa e le garanzie del giusto processo (art. 14 par. 7). L'art. 270 c.p.p. che regola l'utilizzazione della prova acquisita in altro procedimento non può essere l'unica norma di riferimento. Per evitare "*la circolazione di una prova privata della memoria della sua genesi*" non è sufficiente che tale prova sia stata autorizzata da un giudice di uno stato membro nel rispetto della legislazione di tale stato ma occorre il controllo – che non può essere affidato

[43] Per una analisi dottrinale delle pronunce della Corte costituzionale e della Corte di giustizia, si veda F. Dinacci, *I modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, in Archivio Penale 2024, n. 1.

che al giudice nazionale dello stato di emissione – sull'ammissibilità e utilizzazione della prova stessa secondo la legislazione italiana.
Quanto al regime di utilizzabilità della prova raccolta con il sistema dell'O.E.I., la Corte ricorda come la Direttiva 2014/41 non contenga disposizioni sul punto, posto che è affermazione costante della Corte di Giustizia che "*in assenza di una normativa dell'Unione in tema di ammissibilità e valutazione delle prove acquisite attraverso gli strumenti di cooperazione giudiziaria, dovrebbe spettare agli ordinamenti nazionali, ai sensi del principio dell'autonomia procedurale*", stabilire "*le modalità processuali dei ricorsi intesi a garantire la tutela dei diritti spettanti ai singoli in forza del diritto dell'Unione*" (Grande Sezione, 6 ottobre 2020, C-511/18, C-512/18 e C-520/18).
Vengono in considerazione pertanto, in quanto compatibili, i consolidati principi affermati dalla giurisprudenza di legittimità in tema di utilizzabilità dei risultati delle rogatorie, ovvero la regola della prevalenza della *lex loci* sulla *lex fori*, secondo cui l'atto è eseguito secondo le norme processuali dello Stato richiesto, con l'unico limite che la prova non può essere utilizzata se la stessa sia in contrasto con i principi fondamentali dell'ordinamento giuridico italiano (tra le tante, Cass. Sez. 3, n. 1396 del 12/10/2021, dep. 2022, Rv. 282886; Cass. Sez. 5, n. 1405 del 16/11/2016, dep. 2017, Rv. 269015; Cass. Sez. 2, n. 2173 del 22/12/2016, dep. 2017, Rv. 269000; Cass. Sez. 5, n. 45002 del 13/7/2016, Rv. 268457).
Tra i principi cardine dell'ordinamento italiano, ai quali l'atto probatorio assunto all'estero deve conformarsi, secondo la cennata interpretazione costituzionalmente vincolata, la giurisprudenza di legittimità ha fatto costantemente riferimento alla tutela dell'inviolabile diritto di difesa ex art. 24 comma 2 Cost. e del contraddittorio per la prova di cui all'art. 111 Cost. (Cass. Sez. 1, n. 19678 del 03/03/2003, Rv. 225744)[44].
Per quel che attiene al diritto dell'imputato di conoscere e contestare il materiale probatorio, la citata sentenza ha richiamato un precedente della Cassazione, relativo all'attività di messa in chiaro dei messaggi criptati Blackberry svolta all'estero dal fornitore al di fuori del contraddittorio, nel quale la Corte ha affermato il diritto della difesa di ottenere la versione originale criptata dei messaggi e le chiavi di sicurezza per la decriptazione a

[44] Per quel che attiene, in particolare, al diritto della persona imputata di poter conoscere e contestare il materiale probatorio utilizzato a proprio carico, la Suprema Corte ha ritenuto, in tema di intercettazioni, che vada garantito il diritto della difesa di accesso alla prova anche se raccolta all'estero: nel caso in cui l'attività di messa in chiaro di messaggi criptati (nella specie scambiati mediante sistema "Blackberry") sia stata svolta all'estero dal fornitore del servizio fuori dal contraddittorio, la difesa ha diritto di ottenere la versione originale e criptata dei messaggi e le chiavi di sicurezza necessarie alla decriptazione, a pena di nullità ex art. 178, lett. c), c.p.p. (Cass. Sez. 4, 15 ottobre 2019, n. 49896, Rv. 277949).

pena di nullità ex art. 178 lett. c) c.p.p. (sez. IV, n. 49896 del 15 ottobre 2019). Inoltre, ha richiamato la sentenza CEDU Yuksel Yalcinkaya v. Turchia del 26 settembre 2023, in cui era stato compresso il diritto della difesa in relazione ai dati raccolti in un server di messaggistica crittografata non consentendo la verifica dei dati grezzi, ove è stato affermato che l'eventuale restrizione del diritto al contraddittorio per esigenze concorrenti, quali la sicurezza nazionale e le segretezza di metodi di indagine, deve avvenire nei limiti strettamente necessari e sia controbilanciato da adeguate garanzie procedurali ai sensi dell'art. 6 CEDU.
Ciò premesso, secondo la Corte non è chiaro quale parte delle iniziative istruttorie svolte all'estero risulti coperta da un non meglio delineato "segreto di Stato" apposto dall'autorità francese, e in quale momento del procedimento di esecuzione dell'O.E.I. sia stato eventualmente opposto alle parti il segreto in questione.
"*Va pertanto verificato, sulla base delle produzioni delle parti, se e in quale misura l'esercizio delle facoltà difensive di accesso alla prova sia stato in concreto limitato dal segreto di Stato francese*" poiché non emerge dai provvedimenti di merito "*se sia stata data alla difesa l'opportunità di ottenere la versione originale dei messaggi nonché i dati necessari per rendere intellegibili i messaggi criptati*".
La Corte ha dunque annullato con rinvio imponendo, in fase rescissoria, di colmare le indicate lacune motivazionali:

- chiarire quali siano state la natura e le caratteristiche delle attività di indagine svolte all'estero, attribuire alle stesse la corretta qualificazione giuridica e individuarne il relativo regime processuale applicabile;
- verificare, ai fini della utilizzabilità dei dati informativi acquisiti, concernenti comunicazioni nella fase "statica", se sussistevano le condizioni originarie per l'autorizzabilità in sede giurisdizionale delle relative attività investigative oggetto degli ordini europei;
- dichiarare, se del caso, la inutilizzabilità degli elementi di conoscenza acquisiti, concernenti comunicazioni nella fase "dinamica", in assenza di un preventivo provvedimento autorizzativo del giudice italiano;
- valutare la utilizzabilità in Italia della prova raccolta all'estero sulla base delle questioni poste dalla difesa in tema di accesso al materiale indiziario.

### 3.4. La tesi che ritiene applicabile l'art. 234 c.p.p.

Dopo la decisione della Corte di rimettere la questione alle Sezioni Unite e nelle more della redazione dell'ordinanza di rimessione, sono stati elaborati ulteriori orientamenti. In particolare, due sentenze hanno concluso per l'utilizzabilità nel procedimento penale della corrispondenza, anche informatica, già decriptata all'estero, acquisita con O.E.I., individuando nell'art.

234 c.p.p., e non nell'art. 234 bis c.p.p., il parametro normativo di riferimento[45]. Quest'ultima norma, come già affermato, consente l'acquisizione all'estero di documentazione digitale accessibile al pubblico (o con il consenso del titolare del documento, se non in libera disponibilità) senza ricorso alle procedure di collaborazione con lo Stato in cui i documenti sono collocati. Nella specie, invece, i dati sono stati acquisiti all'esito di una attività di collaborazione internazionale.

Nell'ambito della valutazione se "*l'atto o gli atti di indagine richiesti nell'O.E.I. avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo*", la conclusione della Corte è che "*gli atti in questione potevano essere emessi in Italia, nella forma del sequestro probatorio di documentazione/corrispondenza con provvedimento del Pubblico ministero"*.

Quanto all'individuazione dell'Autorità che può provvedere alla emissione dell'ordine di acquisizione delle chat, è stato sostenuto che, nel caso in cui la prova sia già stata acquisita con atto del giudice nel Paese di esecuzione, il suo semplice trasferimento nel procedimento in Italia, può essere disposto sulla base della sola richiesta del pubblico ministero. Del resto, nell'ordinamento interno, rispetto alle intercettazioni già raccolte, "*l'ulteriore circolazione in diversi procedimenti trova limiti nell'art. 270 cod. proc. pen. con riferimento all'ambito dei procedimenti per cui ciò è possibile, ma non richiede alcun ulteriore provvedimento autorizzatorio del giudice potendo essere trasferiti gli atti con provvedimento del pubblico ministero*".

La Corte affronta anche i dubbi prospettati dalle difese (risolti dalle precedenti sentenze pressoché sempre nel senso della loro inconsistenza e non della loro serietà) sulla violazione di diritti fondamentali della difesa legata alla dedotta mancata ostensibilità di informazioni necessarie per la difesa in ragione del segreto di stato.

Secondo la Corte trattasi di mera "suggestione" difensiva per le seguenti ragioni:

- gli artt. 706/95/1 e 706/102/1 prevedono che, in caso di necessità a fine di indagine, con provvedimento motivato del giudice possa disporsi l'accesso occulto a sistemi informatici, con captazione e registrazione dei relativi dati. Ne deriva che la normativa francese applica, per l'acquisizione della messaggistica già trasmessa e conservata nei dispositivi personali, regole sostanzialmente corrispondenti a quelle italiane sulle intercettazioni (ovvero provvedimento motivato del giudice, per reati ben individuati e gravi, secondo criteri di necessità proporzionalità e per tempo limitato).
- La normativa interna, non prevedendo una regola di inutilizzabilità per il caso di acquisizione irregolare della documentazione (l'unica

[45] Cass. VI, 27 settembre 2023 dep. 17 novembre 2023, n. 46482; Cass. VI, 26 ottobre 2023, dep. 21 novembre 2023, n. 46833.

previsione è nell'art. 254 c.p.p. ma riguarda la inutilizzabilità della sola corrispondenza acquisita irregolarmente presso il gestore del servizio postale), rende tendenzialmente irrilevante il tema del "segreto" rispetto all'acquisizione di tale stessa documentazione.

- Si fa confusione tra modalità di accesso ai sistemi informatici protetti e decriptazione e sequestro di dati/documenti: Il supporto tecnico, coperto da segreto, ha riguardato la capacità di mettere in chiaro messaggi, immagini, metadati relativi ai singoli utenti dei sistemi quindi ciò che è "segreto" è la tecnica di hackeraggio, al contrario, è stato reso disponibile il materiale prelevato.
- In definitiva, il tema della segretezza delle modalità tecniche di intercettazione e della decodifica di password, chiavi di decriptazione non è rilevante, corrispondendo all'analoga previsione interna che non obbliga ad alcuna ostensione degli "attrezzi virtuali"[46].

Di analogo tenore la sentenza Cass. VI, 26 ottobre 2023, dep. 21 novembre 2023, n. 46833 che si dilunga in una apologia del principio mutuo riconoscimento (art. 82, paragrafo 1, del Trattato sul funzionamento dell'Unione europea) e della fiducia reciproca (art. 4, paragrafo 3, primo comma, del Trattato sull'Unione europea).

La struttura di cooperazione giudiziaria "*si fonda sulla presunzione che lo Stato membro dell'Unione europea si attenga ad una condotta convenzionalmente conforme non solo rispetto alle garanzie sostanziali, ma anche ai meccanismi procedurali di controllo della loro osservanza, che offrono una tutela equivalente a quella prevista dalla CEDU (Corte EDU, Grande Camera, Bosphorus Hava Yollar Turizm ve Ticaret Anonim Sirketi c. Irlanda, 30 giugno 2005, § 155, n. 45036/98)*".

In questo senso, assumerebbe rilievo centrale la sentenza n. 987 QPC dell'8 aprile 2022 della Corte costituzionale francese che, su ricorso della Corte di Cassazione, ha ritenuto costituzionalmente legittime e non lesive né del diritto ad un giusto processo, né del rispetto della vita privata e di ogni altro diritto e libertà garantite dalla Costituzione, le norme del codice di procedura penale

[46] La Corte richiama alcune precedenti decisioni con le quali è stato affermato che la decriptazione delle conversazioni e delle comunicazioni (e, per converso, dei documenti digitali con codifica di sicurezza) è attività distinta dalla captazione, in quanto tali dati costituiscono rappresentazioni comunicative incorporate in una base materiale con un metodo digitale, ovvero dati informatici che hanno consentito l'intelligibilità del contenuto di stringhe secondo il sistema binario (Cass. Sez. VI, 20 aprile 2021, n. 18907, Civale, Rv. 281819) escludendosi, quindi, che l'interessato, al quale sia reso disponibile il contenuto in forma intellegibile dei documenti, abbia un diritto al controllo diretto mediante l'utilizzo esclusivo, e non mediato, del programma e/o algoritmo di decriptazione (Cass. Sez. VI, 27 novembre 2018, n. 14395, Testa, rv. 275534) essendo comunque garantita una sua efficace difesa.

(secondo comma dell'art. 706-102-1) poiché "*l'unico elemento sottratto al contraddittorio è la tecnica di decriptazione*".
A tale sentenza si aggiungono tre pronunce dalla Corte di cassazione francese (n. 592 del 12 aprile 2022, n. 1226 dell'11 ottobre 2022 e n. 116 del 15 febbraio 2023) che, nel confermare la legittimità del procedimento svolto dai giudici di merito nell'acquisizione dei dati digitali, ha escluso la violazione del diritto al contraddittorio degli imputati di riciclaggio nell'ambito di procedimenti fondati sulle chat criptate scambiate sulla piattaforma Sky ECC (e EncroChat).
La Corte conclude affermando che "*le questioni concernenti le modalità attraverso le quali l'Autorità giudiziaria francese è riuscita a superare i meccanismi di protezione dei server, previo dirottamento delle comunicazioni su altro server su cui è stato conservato il flusso intercettato a seguito delle autorizzazioni del giudice; così come di quali fossero le chiavi di decriptazione, peraltro adottate da un soggetto istituzionale (diversamente da quello che avviene in Italia) e con un procedimento svoltosi sempre sotto il controllo del giudice, costituiscono questioni di natura tecnica non incidenti, in alcun modo, sul diritto di difesa*".
Quanto alla eccezione difensiva circa l'assenza di garanzie sulla "catena di custodia" in ragione della mancata conoscenza dell'algoritmo, la Corte ritiene innanzitutto che le questioni che riguardano il procedimento francese avrebbero dovuto essere sollevate con impugnazione dell'OEI ex art. 14, par. 2 della Direttiva 2014/41/UE. Inoltre, richiamando alcuni precedenti[47], ribadisce la confusione tra la genuinità del dato decriptato con la garanzia di integrità della catena di custodia. Ogni messaggio cifrato è inscindibilmente accoppiato alla sua chiave di cifratura, per cui "*o si decifra tutto e in modo integrale o non si decifra nulla in quanto l'esito errato del tentativo di decifratura crea una stringa di bit priva di significato*".

### 3.5. La tesi che ritiene applicabile l'art. 270 c.p.p.

Una sentenza, successiva alla remissione a SSUU, partendo dalla premessa per cui l'attività svolta nello Stato di esecuzione consiste in intercettazioni, ha ritenuto che la richiesta del pubblico ministero con O.E.I. di trasferimento della corrispondenza e delle conversazioni intercettate tra due procedimenti penali è riconducibile in un caso analogo nell'ordinamento italiano alla previsione dell'art. 270 c.p.p. per la cui applicazione, nel caso di specie, sussistevano tutti i presupposti (la rilevanza e l'indispensabilità per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza).
Anche in questo caso è stata esclusa l'applicabilità dell'art. 266-bis c.p.p., stante l'assenza di contestualità tra la trasmissione della comunicazione e l'atto acquisitivo, ed è stato ritenuto inconferente il richiamo all'art. 234-bis c.p.p. "*Tale previsione, introdotta nella trama sistematica del codice di rito dall'art. 2,*

[47] Cass. IV, 05/04/2023, n. 16347, Rv. 284563; Cass. I, 13/10/2022, n. 6364, Rv. 283998.

*comma 1-bis, d.l. 18 febbraio 2015, n. 7, convertito, con modificazioni dalla l. 17 aprile 2015, n. 43, si ispira all'art. 32 della Convenzione di Budapest sul cybercrime del 23 novembre 2001, che disciplina il trans-border access to stored computer data with consent or where public available".*

Tale disposizione consente l'acquisizione diretta da parte dell'autorità giudiziaria all'estero di documenti e dati informatici senza ricorrere alla disciplina rogatoriale, tuttavia, l'acquisizione nel caso di specie non ha riguardato direttamente dati digitali disponibili in rete o presenti presso un server, ma dati già previamente acquisiti dall'autorità giudiziaria francese per fini di giustizia interni.

La Corte ha inoltre escluso che l'O.E.I. dovesse essere preceduto da un provvedimento autorizzativo del giudice italiano sulla base dell'art. 43, comma 4, del d.lgs. n. 108 del 2017, che, nel regolare le modalità di intercettazione di telecomunicazioni da eseguirsi con l'assistenza tecnica dell'autorità giudiziaria di altro Stato membro dell'Unione europea, stabilisce che la richiesta contenuta in un O.E.I. «*possa avere ad oggetto la trascrizione, la decodificazione o la decrittazione delle comunicazioni intercettate*». Ciò vale solo per i casi in cui l'autorità giudiziaria italiana chieda congiuntamente alla «*intercettazione delle conversazioni o comunicazioni o del flusso di comunicazioni relativo a sistemi informatici o telematici*» anche ulteriori attività accessorie.

La Corte ha poi affrontato una serie di censure relative alla violazione dei diritti fondamentali (ritenuta già di per sé di difficile verificazione in relazione all'attività giudiziaria di uno Stato membro dell'Unione Europea, tenuto a condividere i principi fondamentali dell'ordinamento europeo):

- Quanto alla dedotta impossibilità di partecipare alla selezione delle prove trasmesse dall'autorità giudiziaria francese all'autorità italiana, la censura è stata disattesa poiché il ricorrente non avrebbe dimostrato alcun effettivo pregiudizio per il proprio diritto di difesa alla stregua della disciplina operante nel caso di specie.
- Quanto alla mancata conoscenza dell'algoritmo utilizzato per la decriptazione della messaggistica acquisita, qualificato come «segreto di sicurezza nazionale» dall'autorità francese, la Corte ha svolto un parallelo con l'ordinamento italiano ricordando come il difensore possa avere conoscenza solo del verbale delle operazioni di cui all'art. 268 c.p.p. e delle registrazioni, ma non anche dei mezzi tecnici, hardware e software, utilizzati per l'intrusione nelle conversazioni intercettate, o per decodificare il contenuto. *"L'interessato può avvalersi della procedura prevista dall'art. 268, commi 6 e 7, cod. proc. pen. per verificare il contenuto delle captazioni, ma non può anche pretendere un controllo diretto mediante l'utilizzo esclusivo e non mediato del programma di decriptazione (Sez. 6, n. 14395 del 27/11/2018 dep. 2019, Testa, Rv. 275534)".* Anche l'art. 89 disp.att. c.p.p., come modificato con riferimento all'introduzione dei captatori informatici, prevede che

venga indicato il tipo di programma di intrusione utilizzato e vengano utilizzati solo quelli conformi ai requisiti tecnici stabiliti al Ministero della giustizia; non è, invece, in alcun modo previsto che sia reso disponibile il contenuto del programma utilizzato, di norma di proprietà di soggetti privati coperte da "segreto industriale". "*Resta ferma la possibilità per la difesa di dedurre, sulla base di ragioni specifiche, anomalie tecniche in grado di fare dubitare della correttezza delle acquisizioni e dell'inquinamento del risultato probatorio*".

Sul punto, si deve tuttavia osservare che non ha senso gravare la difesa dell'onere di allegare la mancata corrispondenza tra testo introdotto in giudizio, da un lato, e il risultato effettivamente ricavabile dalla stringa informatica una volta decriptata, se si nega alla difesa di conoscere sia la stringa informatica sia l'algoritmo[48]. Inoltre, le conclusioni del giudice di legittimità trascurano il fatto che le difese (che in caso di dispositivi ordinari avrebbero potuto visionare i messaggi direttamente sul dispositivo) non sono in possesso dei messaggi scambiati stante il meccanismo di cancellazione automatica dei contenuti dei criptofonini. Ciò, ad esempio, non permetterebbe alla difesa di verificare se vi stata una selezione di messaggi da parte dell'autorità giudiziaria straniera, ed in quel caso di ricercare autonomamente messaggi a discarico nella certezza di avere a disposizione l'intero compendio di comunicazioni e relativi metadati.

## 4. Le remissioni a Sezioni Unite

### 4.1. Ordinanza 47798/2023

Il caso oggetto dell'ordinanza riguarda conversazioni con il sistema cifrato SkyEcc ed il ricorrente ha dedotto:

- *il vizio ex art. 606, lett. c) cod. proc. pen. in relazione agli artt. 234-bis e 191 cod. proc. pen.* ritenendo che 1) nonostante si versi nell'ipotesi di documenti informatici, poiché si è in presenza di conversazioni già intercorse tuttavia la relativa acquisizione, non sarebbe riconducibile all'art. 234 bis c.p.p. in quanto acquisite non presso un privato avente sede all'estero bensì dall'autorità francese tramite O.E.I. per la cui emissione l'art. 6 della Direttiva 2014/41/UE impone che l'atto d'indagine richiesto debba essere alle stesso condizioni di un caso interno analogo; 2) ove ritenuto applicabile l'art. 234 bis c.p.p., questo sarebbe stato violato perché il Giudice non avrebbe verificato "*la modalità di acquisizione dei predetti dati conservati all'estero e, in particolare, non avrebbe accertato la manifestazione del "consenso del legittimo titolare" degli stessi, come previsto dal predetto articolo";*

[48] In questo senso, Nunzio Gallo, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, Archivio penale, 2023, n. 3.

- *violazione di norme processuali ex art. 606, comma 1, lett. c), cod. proc. pen., in relazione all'art. 191 cod. proc. pen. e in relazione agli artt. 27 Cost. e 6 della CEDU*, poiché qualificando le chat come prova documentale la parti avrebbero valutato solo la fase terminale del processo di acquisizione della prova e non l'intero compendio investigativo, ed erronea sarebbe la valutazione di superfluità della conoscenza dei file originari e della chiave di decifratura in base al rilievo per cui l'utilizzo di un algoritmo non conforme avrebbe condotto alla elaborazione di espressioni prive di senso.

Il ricorrente ha altresì proposto, ai sensi dell'art. 267 del Trattato sul funzionamento dell'Unione Europea (TFUE), una questione pregiudiziale da sollevare innanzi alla Corte di Giustizia Europea con i seguenti quesiti:

- "*se l'art. 6 paragrafo 1 della Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale, letto alla luce degli artt. 7, 8, e 11 nonché 52 par. 1, della carta dei diritti fondamentali dell'Unione europea, deve esser interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'acquisizione di dati elettronici relativi al traffico e relativi all'ubicazione già in possesso della autorità di esecuzione e la acquisizione di dati elettronici relativi al traffico e relativi alla ubicazione contenuti in basi di dati della polizia o delle autorità giudiziarie, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sulla ubicazione di apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto nonché dalla quantità o dalla natura dei dati disponibili per tale periodo*".
- *"se il divieto di utilizzo degli elementi investigativi o di prova possa derivare direttamente dal principio di effettività sancito dal diritto dell'Unione nel caso di elementi investigativi o prove ottenute tramite un OEI contrario a detto diritto. Se dal diritto dell'Unione Europea, in particolare dal principio di effettività, discenda che le violazioni di tale diritto verificatesi nell'ambito dell'acquisizione di elementi investigativi o di prove in un procedimento penale nazionale non possono rimanere del tutto prive di conseguenze anche nel caso di reati gravi e devono quindi essere prese in considerazione a favore dell'imputato quantomeno sul piano della valutazione delle prove e della determinazione della pena*".

La Cassazione affronta *in primis* la questione se l'acquisizione, mediante O.E.I., di messaggi su chat di gruppo presso Autorità Giudiziaria straniera, che ne abbia già eseguito la decrittazione, costituisca acquisizione o meno di "documenti e di dati informatici" ai sensi dell'art. 234-bis c.p.p. muovendo dalla distinzione tra intercettazioni da una parte e acquisizione/decrifrazione di dati comunicativi dall'altra.
Solo alla captazione e registrazione di messaggi cifrati in transito dal mittente al destinatario è applicabile l'art. 266 bis cpp, mentre "*quando il messaggio telematico sia acquisito allorquando non sia più all'interno di un flusso in corso di comunicazioni, e sia stato criptato - come è appunto accaduto nel caso di specie -, va esclusa la disciplina delle intercettazioni, destinata ad operare solo con riferimento a flussi di comunicazioni in atto*". Ciò renderebbe irrilevante se gli stessi siano stati acquisiti dalla magistratura straniera *ex post* o in tempo reale perché ciò che conta è che i flussi non fossero in corso nel momento in cui sono stati chiesi i dati.
Ne discende, secondo la Corte, che è consentita l'acquisizione delle comunicazioni, ove già acquisite e conservate da Autorità Giudiziaria estera, mediante O.E.I. attivato dal Pubblico ministero, individuando l'art. 234 bis c.p.p. come norme interna di riferimento che legittima il potere di procedere, senza necessità di ulteriori verifiche giurisdizionali interne anteriori e tantomeno posteriori, rispetto alla citata acquisizione, poiché vige "*la presunzione di legittimità dell'attività svolta* (salvo concreta verifica di segno contrario) *e spetta al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate nella fase delle indagini preliminari (in tal senso, Sez. 5, n. 1405 del 16/11/2016, dep. 2017, Rv. 269015 - 01; Sez. 2, n. 24776 del 18/05/2010, Rv. 247750 - 01; Sez. 1, n. 21673 del 22/01/2009, Rv. 243796 - 01)*".
Ciò varrebbe a maggior ragione ove l'originaria attività investigativa non sia stata compiuta su richiesta dell'autorità giudiziaria italiana, ma sia stata eseguita, nell'ambito di altro procedimento instaurato nel detto Stato, su iniziativa di quell'Autorità, che ne trasferisca poi gli esiti come "dati freddi".
Sarebbe altresì da escludersi un'asserita incompatibilità delle chat così acquisite con il diritto interno in ragione della sopravvenuta disciplina dello Stato italiano in materia di acquisizione di tabulati introdotta con il d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178, perché il caso in esame ha ad oggetto documenti informatici e non dati esteriori.
Tuttavia, rileva la Corte, sono intervenute due sentenze della Sezione VI che risultano aprire orientamenti dissenzienti rispetto all'orientamento a lungo prevalente: sentenze 26 ottobre 2023 n. 44154 e 44155 di cui l'ordinanza ripercorre i tratti salienti (già ripercorsi al paragrafo sub 3.3).

Pertanto, in data 3 novembre 2023, la Cassazione sez. III con ordinanza n. 47798[49], ha rimesso alle Sezioni Unite i seguenti quesiti: a) Se il trasferimento all'Autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate attraverso criptofonini e già acquisite e decrittate dall'Autorità giudiziaria estera in un proprio procedimento penale, costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234-bis c.p.p. o di documenti ex art. 234 c.p.p. ovvero sia riconducibile ad altra disciplina relativa all'acquisizione di prove, b) Se il trasferimento di cui sopra debba essere oggetto di verifica giurisdizionale preventiva della sua legittimità, nello Stato di emissione dell'ordine europeo di indagine, c) Se l'utilizzabilità degli esiti investigativi di cui al precedente punto a) sia soggetta a vaglio giurisdizionale nello Stato di emissione dell'ordine europeo di indagine.
Secondo l'informazione provvisoria diffusa dalla Suprema Corte, ai quesiti sono state date le seguenti soluzioni:
«*primo quesito: il trasferimento di cui sopra rientra nell'acquisizione di atti di un procedimento penale che, a seconda della loro natura, trova alternativamente il suo fondamento negli artt. 78 disp. att. cod. proc. pen., 238, 270 cod, proc. pen. e, in quanto tale, rispetta l'art. 6 della Direttiva 2014/41/UE;*
*secondo quesito: negativa, rientrando nei poteri del pubblico ministero quello di acquisizione di atti di altro procedimento penale;*
*terzo quesito: affermativa; l'Autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo*».

### 4.2. Ordinanza 2329/24

Il caso oggetto dell'ordinanza riguarda conversazioni con il sistema cifrato SkyEcc ed i ricorrenti hanno dedotto, per quanto qui d'interesse:

1. Violazione di legge e vizio di motivazione in ordine all'art. 294 c.p.p. per la mancata produzione da parte del PM di una serie di provvedimenti emessi all'interno del procedimento base francese: provvedimento del 14 giugno 2019 del giudice istruttore presso il Tribunale di Lille con cui era stata disposta l'intercettazione del flusso telematico che fosse transitato sui server di Roubaix, noleggiati dalla società Sky Global; decreti di proroga delle intercettazioni; ordinanza D 207/1 del 17 dicembre 2020 con cui il giudice istruttore presso il Tribunale di Parigi aveva autorizzato l'installazione di un primo trojan sul server di Roubaix contrassegnato con il nome di host "server 2 o

[49] Ordinanza Cass. III ud. 3 novembre 2023, dep. 30 novembre 2023, n. 47798, pronunciandosi sul ricorso per cassazione avverso l'ordinanza del Tribunale di Potenza sezione riesame in relazione all'ordinanza custodiale cautelare in relazione ad ipotesi di reato di cui agli artt. 73 e 74 DPR 309/90.

server di back up"; provvedimento D 212/1 adottato in data 24 febbraio 2021 dal giudice istruttore presso il Tribunale di Parigi per acconsentire l'installazione di un secondo Trojan sul server denominato "server 1". Ciò avrebbe precluso alla difesa di conoscere le modalità di acquisizione e decriptazione dei messaggi.

2. Violazione di legge e vizio di motivazione con riferimento alla procedura seguita dall'autorità francese per l'acquisizione dei dati e inutilizzabilità degli stessi per le seguenti ragioni:
   - i) Non sarebbe applicabile l'art. 234 bis c.p.p. poiché si sarebbe trattato di una vera e propria attività di intercettazione eseguita attraverso un doppio passaggio: prima l'intercettazione di tutte le comunicazioni veicolate dal server Roubaix poi l'acquisizione tramite trojan delle chiavi di cifratura (due delle quali presenti nel server e due nel singolo cellulare) necessarie alla decriptazione.
   - ii) L'attività di intercettazione svolta all'estero va qualificata come intercettazione massiva, generalizzata e indiscriminata, come tale non permessa nel nostro ordinamento, la cui acquisizione non può essere consentita tramite O.I.E. a mente dell'art. 6 par. 1 lett. b della Direttiva 2014/41/UE e preclusa da disposizioni euro-unitarie (art. 47 par. 2 Carta dei diritti fondamentali, art. 6 par. 1 e 8, par. 2 CEDU), come riconosciuto dalla sentenza CGUE (Prokuratuur, C-746/18 2 marzo 2021)
   - iii) Non sussistono i presupposti di utilizzabilità dell'art. 270 c.p.p. né rispettate le previsioni di cui all'art. 268 commi 6,7, c.p.p.
   - iv) Anche a voler considerare le risultanze francesi come prove atipiche, l'acquisizione sarebbe in contrasto con i principi costituzionali e convenzionali sulla tutela del domicilio informatico difettando i presupposti degli artt. 14 cost e 8 par. 2 Cedu.

In data 15 gennaio 2024, anche la Cassazione sezione VI, con ordinanza n. 2329[50], ha rimesso alle SSUU ulteriori quesiti: a) se l'acquisizione, mediante ordine europeo di indagine, dei risultati di intercettazioni disposte dall'autorità giudiziaria estera su piattaforma informatica criptata integri, o meno, l'ipotesi disciplinata nell'ordinamento interno dall'art. 270 c.p.p., b) Se, ai fini dell'emissione dell'ordine europeo di indagine finalizzato al suddetto trasferimento, occorra la preventiva autorizzazione del giudice, c) Se l'utilizzabilità degli esiti investigativi di cui al precedente punto a) sia soggetta a vaglio giurisdizionale nello Stato di emissione dell'ordine europeo di indagine.

[50] Ordinanza Cass. VI ud. 15 gennaio 2024, dep. 18 gennaio 2024, n. 2329.

Secondo l'informazione provvisoria, ai quesiti sono state date le seguenti soluzioni:
«*Primo quesito: affermativa.*
*Secondo quesito: negativa.*
*Terzo quesito: affermativa; l'Autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo*».
Applicando i principi espressi dalle SSUU nella comunicazione provvisoria, la Cassazione, sezione I, con sentenza n. 13535 del 13 marzo 2024, depositata il 4 aprile 2024, ha confermato l'esclusione dell'applicazione dell'art. 234 bis c.p.p. e affermato che il Tribunale del Riesame, aderendo ad un orientamento ormai superato, ha erroneamente ritenuto ininfluente accertare le modalità con le quali l'autorità francese aveva acquisito le conversazioni. Tale accertamento, opportunamente sollecitato della difesa, era infatti funzionale a stabilire le regole di acquisizione della messaggistica e conseguentemente i limiti alla sua utilizzabilità ai fini della decisione cautelare. La Corte ha dunque annullato con rinvio imponendo al Tribunale di Bari di colmare le lacune motivazionali attinenti al procedimento probatorio seguito dall'autorità straniera.

### 4.3. Le motivazioni delle SSUU 29 febbraio 2024 n. 23755 e 23756.

In data 14 giugno 2024 sono state depositate le motivazioni di entrambe le pronunce.
La sentenza n. 23755 esordisce con una dettagliata panoramica di tutte le pronunce, raggruppate per orientamento, con riferimento all'utilizzo delle chat acquisite dai criptofonini per riassumere i termini del contrasto.
Prima conclusione raggiunta dalle Sezioni Unite riguarda la non applicabilità della disciplina di cui all'art. 234 bis c.p.p. in quanto "*alternativa e incompatibile rispetto a quella dettata in tema di o.e.i*", avendo peraltro quest'ultima una "funzione di preminenza" in materia di acquisizione di prove in ambito UE.
La disposizione di cui all'art. 234 bis c.p.p. non disciplina un mezzo di prova bensì una modalità di acquisizione di particolari tipologie di elementi di prova presenti all'estero che viene attuata in via diretta dall'autorità italiana e prescinde da forme di collaborazione con l'autorità dello stato in cui il dato è custodito.
Individuate nella direttiva 2014/41/UE e nel d.lgs. 108/2017 le coordinate, la Corte esamina le regole generali di tale sistema normativo a partire dalle condizioni di ammissibilità dell'o.e.i.: "*solo se l'o.e.i. è stato legittimamente emesso, gli elementi acquisiti per il suo tramite potranno essere validamente utilizzati nel procedimento o nel processo pendente in Italia*".
Tuttavia, "*le disposizioni dell'ordinamento nazionale di carattere generale sono estremamente laconiche*". In particolare, l'art. 27, comma 1, d.lgs. n. 108 del 2017 si limita a prevedere che "*il pubblico ministero e il giudice che procede*

*possono emettere, nell'ambito delle relative attribuzioni, un ordine di indagine e trasmetterlo direttamente all'autorità di esecuzione*". Disposizioni più dettagliate sono previste in relazione a specifici atti di indagine, quali la richiesta di intercettazioni di telecomunicazioni (art. 43), e la richiesta di documentazione inerente ai dati esterni relativi al traffico telefonico o telematico (art. 45). Tuttavia, la precisazione di carattere generale contenuta nell'art. 1 d.lgs. cit. induce a ritenere applicabili anche agli O.E.I. emessi dall'autorità giudiziaria italiana le condizioni di ammissibilità previste dall'art. 6, paragrafo 1, Direttiva 2014/41/UE: a) l'emissione dell'O.E.I. è necessaria e proporzionata ai fini del procedimento di cui all'art. 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata; b) l'atto o gli atti di indagine richiesti nell'O.E.I, avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo.

La seconda condizione, come osservato in dottrina, "*postula una valutazione in astratto, ed è quindi logicamente preliminare*", mentre la prima condizione implica una "*valutazione in concreto, rapportata allo specifico procedimento nel cui ambito è stato emesso l'o.e.i.*".

Le ragioni di merito dell'emissione di un O.E.I., secondo quanto precisa l'art.14, paragrafo 2, Direttiva cit., possono essere oggetto di controllo successivo, e precisamente "*impugnate*", solo "*mediante un'azione introdotta nello Stato di emissione*", salvo la necessita di assicurare tutela ai diritti fondamentali nello Stato di esecuzione; e, però,"[*u]n'impugnazione non sospende l'esecuzione dell'atto di indagine, a meno che ciò non abbia tale effetto in casi interni analoghi*" (art. 14, paragrafo 6, Direttiva cit.).

Sulla scia della lamentata incompletezza, la Corte aggiunge che "*la fase di esecuzione di un o.e.i. emesso dall'autorità giudiziaria italiana non riceve puntuale regolamentazione nel d.lgs. n. 108 del 2017*", se non attraverso un generico richiamo al "*rispetto dei principi dell'ordinamento costituzionale e della Carta dei diritti fondamentali dell'Unione europea in tema di diritti fondamentali, nonché in tema di diritti di libertà e di giusto processo*".

D'altronde, afferma la sentenza, "*la disciplina posta dalla Direttiva 2014/41/UE, dal canto suo, non contiene regole relative alla fase di esecuzione degli o.e.i. che incidano specificamente sulla utilizzabilità degli atti acquisiti nel procedimento davanti all'autorità di emissione*".

"*In forza del coordinamento normativo tra il d.lgs. n. 108 del 2017 e la Direttiva 2014/41/UE, sembra ragionevole affermare che, ai fini dell'utilizzabilità di atti acquisiti mediante o.e.i. dall'autorità giudiziaria italiana, è necessario garantire il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo, ma non anche l'osservanza, da parte dello Stato di esecuzione, di tutte le disposizioni previste dall'ordinamento giuridico italiano in tema di formazione ed acquisizione di tali atti*". Soluzione che sarebbe

coerente con la costante tradizione del nostro ordinamento in materia di rogatoria internazionale.
Diviene allora fondamentale, ai fini dell'accertamento del rispetto dei diritti fondamentali, considerare i principi della presunzione relativa di conformità ai diritti fondamentali dell'attività svolta dall'autorità giudiziaria estera, nell'ambito di rapporti di collaborazione ai fini dell'acquisizione di prove, e dell'onere per la difesa di allegare e provare il fatto dal quale dipende la violazione denunciata, entrambi oggetto di costante e generale enunciazione da parte della Suprema Corte[51].
Chiarite le regole generali, è necessario individuare il "tipo" di atto oggetto di richiesta e trasmissione nella singola vicenda poiché è in ragione del "tipo" di atto specificamente richiesto e trasmesso che è possibile valutare la sussistenza delle condizioni di ammissibilità dell'O.E.I., e, in particolare, quella della possibilità di disporne l'assunzione alle stesse condizioni in un caso interno analogo, nonché verificare se vi sia una violazione dei diritti di difesa e giusto processo.
Poste queste premesse, e passando all'applicazione in concreto, la Corte parte dal presupposto "*incontroverso*" che i messaggi fossero a disposizione dell'autorità giudiziaria francese già prima della presentazione dell'O.E.I. da parte dell'autorità giudiziaria italiana. Nel sistema dell'O.E.I., "*l'acquisizione di prove già in possesso delle autorità competente dello Stato di esecuzione è oggetto di alcune specifiche disposizioni, di deroga alla disciplina generale, e funzionali a renderne più agevole la circolazione*". In particolare, l'art. 10 Direttiva cit. esclude la possibilità, per l'autorità di esecuzione, di disporre un atto di indagine alternativo a quello richiesto. Inoltre, dal combinato disposto degli artt. 12, paragrafo 4, e 13, paragrafo 1, Direttiva cit., poi, si evince che, quando le prove siano già nel possesso dello Stato di esecuzione, la loro trasmissione allo Stato di emissione dovrebbe avvenire con immediatezza.
Analizzando la normativa interna italiana (con particolare riferimento agli artt. 238 e 270 c.p.p. e 78 disp. att. c.p.p.), la Corte ritiene che la circolazione di prove già formate abbia una disciplina diversa da quella riservata alla "*formazione delle prove*", impregiudicato il potere del giudice competente per

[51] Cfr. sul primo principio, *ex plurimis*: Cass. Sez. VI, 4 ottobre 2023, n. 44882, Barbaro, Rv. 285386 - 01; Cass. Sez. III, 12 ottobre 2021, n. 1396, Torzi, Rv. 282886 - 01; Cass. Sez. IV, 6 novembre 2019, n. 19216, Ascone, Rv. 279246 - 01. Corte giustizia, 11 novembre 2021, Gavanozov, C-852/19, § 54; cfr., nello stesso senso, Corte giustizia, 8 dicembre 2020, Staatsanwaltschaft Wien, C-584/19, § 40. Cfr. sul secondo principio Cass. Sez. U, 16 luglio 2009, n. 39061, De Iorio, Rv, 244329 - 01, e, in termini analoghi, Cass. Sez. U, 17 novembre 2004, n. 45189, Esposito, Rv. 229245 - 01; tra le tante successive conformi, cfr. Cass. Sez. V, 19 aprile 2023, n. 23015, Bernardi, Rv. 284519 - 01, e Cass. Sez. VI, 14 dicembre 2017, n. 18187, Nunziato, Rv. 273007 – 01; Cass. Sez. V, 18 novembre 2010, n. 1915, Durantini, Rv. 249048 - 01, e Cass. Sez. V, 17 dicembre 2008, n. 600, Cavallaro, Rv. 242551 - 01.

il procedimento penale nel quale le parti intendono avvalersi delle prove già separatamente formate o acquisite in altra sede di valutare se vi siano i presupposti per ammetterle ed utilizzarle ai fini della decisione.
L'art. 238 c.p.p., che si riferisce espressamente anche agli atti non ripetibili, non prevede, ai fini dell'acquisizione delle prove formate altrove, alcun intervento preventivo da parte del giudice del procedimento nel quale si vorrebbero utilizzarle.
L'art, 270 c.p.p., speciale rispetto all'art. 238 c.p.p., perché riferito ad uno specifico mezzo di ricerca della prova, non prevede alcun intervento autorizzativo preventivo del giudice del procedimento di "*destinazione*".
L'art, 78 disp. att. c.p.p. dispone al comma 1 che "[*l*]*a documentazione di atti di un procedimento penale compiuti da autorità giudiziaria straniera può essere acquisita a norma dell'art. 238 del codice*", al comma 2, che, per gli atti non ripetibili compiuti dalla polizia straniera, l'acquisizione nel fascicolo per il dibattimento è subordinata al previo esame in contraddittorio dell'autore degli stessi, o al consenso delle parti.
In conclusione, le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richiesti e acquisiti dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice del procedimento nel quale si vogliono usare, lasciando però integro il potere di quest'ultimo di valutare se vi siano i presupposti per ammetterle ed utilizzarle ai fini delle decisioni di sua spettanza.
Resta necessario però chiarire il "tipo" di atto trasmesso nel caso de quo, posto che l'ordinanza impugnata lo qualifica come "*documento informatico*" mentre il ricorrente come "*dato concernente il traffico, l'ubicazione e il contenuto di comunicazioni elettroniche*".
La Corte analizzando la prima ipotesi afferma che l'applicabilità dell'art. 234 c.p.p. "*non è ostacolata dalla sola circostanza che le entità rappresentative siano comunicazioni elettroniche, data la latitudine della nozione di prova documentale*". Tuttavia, la suddetta disposizione "*non è sempre esaustiva*". In particolare, quando la prova documentale ha ad oggetto comunicazioni scambiate in modo riservato tra un numero determinato di persone, indipendentemente dal mezzo tecnico impiegato a tal fine, occorre assicurare la tutela prevista dall'art. 15 Cost. in materia di corrispondenza (cosi Corte cost., sent. n. 170 del 2023; nello stesso senso, Corte cost., sent. n. 227 del 2023 e Corte cost., sent. n. 2 del 2023). Vero è, tuttavia, che l'art. 15 Cost. impiega il sintagma "autorità giudiziaria", il quale indica una categoria nella quale sono inclusi sia il giudice, sia il pubblico ministero.
Ove gli atti consegnati dall'autorità francese fossero qualificati come documenti, la Corte afferma che "*l'acquisizione di documenti, pur se relativi a "corrispondenza", quando attiene a prove già in possesso delle autorità competenti dello Stato di esecuzione, può essere chiesta mediante o.e.i. presentato dal pubblico ministero, senza necessita di autorizzazione del giudice*".

Con riferimento alla prospettazione difensiva, i giudici di legittimità ritendono che la disciplina che richiede la preventiva autorizzazione del giudice si riferisce alla acquisizione dei dati presso il gestore dei servizi telefonici e telematici, ma non anche all'utilizzazione dei dati in un procedimento penale diverso da quello in cui sono stati già acquisiti. L'art. 132 d.lgs. 196/2003 fa infatti riferimento ai dati "*conservati dal fornitore*". In sostanza, quando i dati in questione sono già stati acquisiti in un procedimento penale, non si pone più la questione dell'autorizzazione all'accesso di un'autorità pubblica, siccome gli stessi sono già a disposizione di un'autorità pubblica.
Ne discende che l'O.E.I. emesso dal pubblico ministero italiano avente ad oggetto l'acquisizione di dati relativi al traffico o all'ubicazione, concernenti comunicazioni elettroniche, pur se manchi una preventiva autorizzazione del giudice competente per il procedimento nel quale si intende utilizzarli, soddisfa la condizione di ammissibilità di cui all'art, 6, paragrafo 1, lett. b), Direttiva 2014/41/UE.
Chiarito anche questo passaggio, la sentenza passa ad analizzare la garanzia del rispetto dei diritti fondamentali. Non risulterebbe costituire violazione di diritti fondamentali l'acquisizione dei dati in questione da parte del pubblico ministero senza previa autorizzazione del giudice competente per il procedimento nel quale si intende utilizzarli, quando gli stessi siano già stati acquisiti in altro procedimento previa autorizzazione di un giudice.
Neppure l'accesso ad un'ampia mole di dati relativi al traffico e all'ubicazione, concernenti comunicazioni elettroniche, integrerebbe, di per sé, violazione di diritti fondamentali. In proposito, la giurisprudenza della Corte di giustizia "*non pone limiti quantitativi*" bensì "*criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione*", ed indica, come accessibili, "*i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere*" (cosi Corte giustizia, Grande Sezione, 02/03/2021, H.K./Prokuratuur, C-706/18, § 50, e Corte giustizia, Grande Sezione, 05/04/2022, Commissioner of An Garda Siochana, C-140/20, § 105).
Neanche l'impossibilità, per 1a difesa, di accedere all'algoritmo utilizzato per "*criptare*" il contenuto delle comunicazioni determinerebbe, almeno in linea di principio, una violazione di 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 ha alcuna possibilità di decriptarlo anche solo parzialmente*".
Applicando i suddetti principi di diritto all'oggetto del ricorso, la Corte pur condividendo la tesi della inapplicabilità dell'art. 234-bis c.p.p., non ritiene che l'errore di qualificazione abbia avuto influenza decisiva sul dispositivo, "*in quanto, nella specie, sussistono le condizioni di ammissibilità necessarie per*

*emettere legittimamente l'o.e.i. e non risultano violazioni dei diritti fondamentali*". Su tale ultimo aspetto, la Corte evidenzia che i) non è stato allegato che i dati trasmessi siano stati acquisiti in difetto di un provvedimento autorizzative di un giudice, ii) l'acquisizione è stata effettuata dall'autorità giudiziaria estera in relazione ad indagini concernenti, in particolare, il narcotraffico ed i fatti per i quali l'ordinanza è stata adottata si riferiscono proprio al narcotraffico e ad un'associazione a tal fine costituita, iii) l'affermazione difensiva secondo cui l'autorità estera avrebbe effettuato attività di captazione e di apprensione dei dati in modo generalizzato ed indifferenziato è meramente assertiva ed aspecifica, iv) le modalità di consegna dei file relativi alle comunicazioni, siccome trasfusi in una consulenza tecnica avente ad oggetto la loro decrittazione, e l'indisponibilità delle chiavi di cifratura necessarie per renderle intelligibili non sono circostanze relative all'acquisibilità o all'utilizzabilità di tale tipologia di elementi, ma attengono alla verifica di affidabilità di questi ultimi e del loro contenuto e l'asserita alterazione dei dati è stata unicamente ipotizzata dal ricorrente.
Per tali motivi, deve escludersi anche la necessita di formulare alla Corte di giustizia dell'Unione Europea i quesiti prospettati dalla difesa, ovvero di sollevare questione di legittimità costituzionale.
La sentenza n. 23756 replica pressoché integralmente le motivazioni della sentenza gemella, con l'aggiunta di una replica all'argomento difensivo che lamentava la violazione dei principi fissati dall'art. 31 della Direttiva cit. in ordine alle intercettazioni effettuate nei confronti di persone il cui "indirizzo di comunicazione" è utilizzato nel territorio di uno stato diverso da quello nel quale le operazioni di captazione sono state disposte.
Tale disposizione prevede che lo stato che effettua l'intercettazione dia notifica di tale attività all'autorità dello stato nel quale è utilizzato l'indirizzo di comunicazione sottoposto a controllo quando viene a conoscenza di tale circostanza e che tale autorità possa vietare il compimento o prosecuzione delle operazioni nonché l'utilizzazione dei risultati ottenuti.
La Corte rileva che l'obbligo sorge quando l'autorità viene a conoscenza della circostanza e che l'eventuale intempestività della notifica non è sanzionata di per sé. Inoltre, il divieto di compimento o prosecuzione scatta solo quando l'intercettazione non sia ammessa in caso interno analogo e la disciplina italiana di recepimento prevede una unica ipotesi vietata ossia se le intercettazioni siano disposte per un reato per il quale non è consentito procedere (art. 24 d.lgs. 108/2017). Circostanza non sussistente poiché il reato per quale si procedeva in Italia, associazione a delinquere finalizzata al traffico di sostanze stupefacenti, prevede la possibilità di disporre intercettazioni.
Negata dalla Corte la richiesta formulata per la prima volta in udienza di annullamento con rinvio per far disporre una perizia al fine di assicurare in contradditorio gli esiti della decriptazione, analisi e selezione delle conversazioni.

Entrambi i ricorsi sono stati dunque rigettati.
Un dato emerge evidente dall'analisi delle sentenze in commento, ossia quanto sia imponente l'onere probatorio posto in capo alla difesa che - diversamente dalle Procure, soprattutto in caso di indagini transfrontaliere - non ha certamente gli stessi mezzi a disposizione, finendo per non riuscire a provare documentalmente alcune circostanze, quali ad esempio la natura massiva dell'intercettazione disposta dall'autorità francese, che finanche le fonti pubbliche internazionali diffondono come dato certo.

## 5. Le questioni pendenti dinanzi alle Corti sovranazionali

L'Italia non è certamente l'unico paese nel quale i difensori hanno sollevato eccezioni. In tutta Europa vi è stata una moltitudine di casi e ricorsi le cui doglianze possono così sintetizzarsi: rispetto al rifiuto di rivelare eventuali dettagli tecnici dell'operazione di intercettazione coperta da segreto di stato, è stata lamentata la violazione del diritto ad un giusto processo e diritto della difesa ad un contraddittorio pieno; rispetto al tema della intercettazione massiva e indiscriminata, è stata lamentata la violazione del diritto al rispetto della vita privata e familiare e diritto alla protezione dei dati personali.

### 5.1. La sentenza della CGUE 30 aprile 2024

I pubblici ministeri tedeschi hanno subito una prima battuta d'arresto quando il Tribunale Regionale di Berlino ha ritenuto inammissibili le prove EncroChat nel luglio 2021. Tuttavia, su appello della Procura, il Tribunale Regionale Superiore di Berlino ha annullato tale decisione nell'agosto 2021, in linea con una serie di sentenze di altri Tribunali.
Il 19 ottobre 2022, il Tribunale Regionale di Berlino è tornato sul punto ed ha sospeso il processo contro un imputato (M.N.), indagato per traffico di droga sulla base dei dati di EncroChat, chiedendo una pronuncia pregiudiziale alla Corte di giustizia dell'Unione Europea su 14 questioni critiche relative all'interpretazione della Direttiva 2014/41.
Tra queste vi è la questione se l'OIE tedesco fosse proporzionato e necessario, considerato che riguardava la ricezione di tutti i dati EncroChat degli utenti sul territorio tedesco senza che i singoli sospettati fossero stati individuati in anticipo. Inoltre, è messa in discussione la compatibilità dell'OIE tedesco con l'art. 6(1)(b) della Direttiva, perché l'atto d'indagine non avrebbe potuto essere autorizzato in un caso simile in Germania[52].
Per quanto riguarda le conseguenze generate da un'eventuale violazione del diritto comunitario, il Tribunale ritiene che i principi di effettività ed equivalenza dell'Unione, come interpretati dalla precedente giurisprudenza della CGUE, dovrebbero condurre ad una declaratoria di inammissibilità delle

[52] T. Wahl, *EncroChat turns into a Case for the CJEU*, in Eucrim issue 3/2002

prove. In questo contesto, il Tribunale ha evidenziato la mancanza di trasparenza da parte delle autorità:

- in primo luogo, a causa della mancata divulgazione delle modalità tecniche utilizzate dalla Francia per accedere ai dati, non sarebbe stato possibile valutarne l'integrità;
- in secondo luogo, il rifiuto delle agenzie dell'UE e delle forze dell'ordine tedesche di consegnare parti del fascicolo alla difesa avrebbe reso l'accertamento dei fatti ancora più difficile nel corso del processo.

Infine, secondo il Tribunale rimettente, gli altri tribunali tedeschi, nel dichiarare le prove utilizzabili, avrebbero commesso un errore attribuendo maggiore importanza agli obiettivi di repressione penale piuttosto che alle violazioni dei diritti fondamentali delle persone.

L'Avvocato Generale della Corte di giustizia europea ha emesso un parere preliminare sulle questioni il 26 ottobre 2023[53], affermando che la Germania avrebbe utilizzato legittimamente l'ordine d'indagine per ottenere dati intercettati dagli investigatori francesi relativi ad utenti tedeschi dei telefoni EncroChat. Gli Stati membri, infatti, vincolati dal principio di mutuo riconoscimento, sarebbero tenuti ad accettare la liceità dell'operazione di intercettazione francese già vagliata dai tribunali francesi. L'Avvocato Generale ha sostanzialmente concluso che le questioni giuridiche rimesse debbano essere risolte dai tribunali nazionali.

La CGUE (Grande Sezione) si è pronunciata in data 30 aprile 2024 precisando quanto segue:

1) L'articolo 1, paragrafo 1, e l'articolo 2, lettera c), della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale, devono essere interpretati nel senso che: un ordine europeo di indagine 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.
2) L'articolo 6, paragrafo 1, della direttiva 2014/41 deve essere interpretato nel senso che: esso non osta a che un pubblico ministero adotti un ordine europeo di indagine inteso a ottenere la trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione, qualora tali prove siano state acquisite a seguito dell'intercettazione, da parte di tali autorità, nel territorio dello Stato di emissione, di telecomunicazioni

[53] Si veda, anche per l'elenco dettagliato delle questioni rimesse alla CJEU, l'Opinion of Advocate General Ćapeta, Case C-670/22, Staatsanwaltschaft Berlin V M.N. Request for a preliminary ruling from the Landgericht Berlin (Regional Court, Berlin, Germany).

dell'insieme degli utenti di telefoni cellulari che permettono, grazie a un software speciale e a un hardware modificato, una comunicazione cifrata da punto a punto, purché un tale ordine di indagine rispetti tutte le condizioni eventualmente previste dal diritto dello Stato di emissione per la trasmissione di tali prove in un caso puramente interno a detto Stato[54].

3) L'articolo 31 della direttiva 2014/41 deve essere interpretato nel senso che: una misura connessa all'infiltrazione in apparecchi terminali, diretta a estrarre dati relativi al traffico, all'ubicazione e alle comunicazioni di un servizio di comunicazione basato su Internet, costituisce un'«intercettazione di telecomunicazioni», ai sensi di tale articolo, che deve essere notificata all'autorità a tal fine designata dallo Stato membro sul cui territorio si trova la persona sottoposta all'intercettazione[55]. Nel

[54] In relazione a questo punto, uno dei difensori nel procedimento tedesco ha rilevato che, seguendo tale principio, si deve dedurre che i requisiti di cui agli artt. 100e e 100b del codice di procedura penale tedesco avrebbero dovuto essere soddisfatti al momento di emissione dell'OIE, mentre alla data del 2 giugno 2020 non erano ancora emersi concreti e specifici sospetti nei confronti dei singoli utenti oggetto di intercettazione. CGUE Sentenza (Grande Sezione) del 30 aprile 2024, nella causa C-670/22, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Landgericht Berlin (Tribunale del Land, Berlino, Germania), paragrafi 13-15: *L'intercettazione delle telecomunicazioni ai fini dell'esercizio di un'azione penale è disciplinata dalla Strafprozessordnung (StPO) (codice di procedura penale) (in prosieguo: la «StPO»). L'articolo 100a, paragrafo 1, frasi dalla prima alla terza, della StPO autorizza, rispettivamente, il controllo delle comunicazioni in corso sotto forma di un controllo «classico» delle telecomunicazioni, la sorveglianza delle comunicazioni in corso mediante l'installazione di un software spia nelle apparecchiature terminali («intercettazione di telecomunicazioni alla fonte») e il sequestro delle comunicazioni ultimate e già registrate su un apparecchio alla data di emissione dell'ordinanza del Landgericht (Tribunale del Land, Germania) che ordina la misura di cui trattasi («perquisizione online ristretta»). Ai sensi dell'articolo 100b della StPO, è possibile accedere a tutti i dati registrati su un'apparecchiatura terminale («perquisizione online»). Tutte queste misure presuppongono l'esistenza di un sospetto concreto della commissione di un reato, e la categoria dei reati considerati è limitata a talune fattispecie elencate all'articolo 100a, paragrafo 2, e all'articolo 100b, paragrafo 2, della StPO.*

[55] In relazione a questo punto, uno dei difensori nel procedimento tedesco ha rilevato che la notifica doveva intervenire prima che la misura investigativa fosse posta in essere e che, in ogni caso, le autorità tedesche avrebbero dovuto impedire l'intercettazione ai sensi dell'art. 91g par. 6 IRG non si può ragionevolmente sostenere che l'intercettazione massima di oltre 4.600 dispositivi in Germania attraverso un trojan fosse legittima ai sensi del diritto nazionale in assenza di concreti e specifici sospetti a carico degli utenti intercettati. CGUE Sentenza (Grande Sezione) del 30 aprile 2024, nella causa C-670/22, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Landgericht Berlin (Tribunale del Land, Berlino, Germania), paragrafo 18: *L'articolo 91g, paragrafo 6, dell'IRG, che*

caso in cui lo Stato membro di intercettazione non sia in grado di identificare l'autorità competente dello Stato membro notificato, tale notifica può essere inviata a qualsiasi autorità dello Stato membro notificato che lo Stato membro di intercettazione ritenga idonea a tal fine.

4) L'articolo 31 della direttiva 2014/41 deve essere interpretato nel senso che: esso mira anche a tutelare i diritti degli utenti interessati da una misura di «intercettazione di telecomunicazioni», ai sensi di tale articolo.
5) L'articolo 14, paragrafo 7, della direttiva 2014/41 deve essere interpretato nel senso che: esso 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 se tale persona non è 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.

In particolare, i principi di cui ai punti 2, 3 e 5 dovrebbero aprire margini di manovra in relazione alle eccezioni difensive circa l'integrità, l'autenticità, il trattamento e i metodi di raccolta dei dati.
Si attende dunque una nuova decisione del Tribunale Regionale di Berlino, circa l'ammissibilità delle prove, in applicazione dei principi di diritto elaborati dalla CGUE.

### 5.2. I ricorsi pendenti dinanzi alla CEDU

Due detenuti britannici hanno presentato ricorso contro la Francia alla Corte Europea dei Diritti dell'Uomo (A.L. contre la France et E.J. contre la France).
Il primo ricorrente (n. 44715/20), arrestato il 18 giugno 2020, è stato accusato presso la Snarebrook Crown Court di associazione a delinquere finalizzata a commettere importazione e possesso illegali a scopo di rivendita di eroina e cocaina.
Il secondo ricorrente (n. 47930/21), arrestato il 16 giugno 2020, è stato accusato presso la Crown Court di Liverpool di associazione a delinquere finalizzata allo spaccio di cocaina ed eroina e di aver commesso tre omicidi.
Le accuse si fondano sulle chat ottenute con un OIE dell'11 marzo 2020 emesso dalla National Crime Agency (NCA) del Regno Unito con il quale è stato richiesto alle autorità francesi di trasferire i dati di tutti i titolari britannici di utenze EncroChat.

---

*traspone nel diritto tedesco l'articolo 31 della direttiva 2014/41, prevede che l'autorità competente, alla quale uno Stato membro notifica la sua intenzione di procedere ad una misura di intercettazione nel territorio tedesco, deve vietare l'attuazione di tale misura o l'utilizzo dei dati intercettati entro 96 ore oppure subordinare l'utilizzo di tali dati a determinate condizioni qualora, in casi interni analoghi, detta misura non sia autorizzata.*

I ricorrenti lamentano l'intrusione delle autorità francesi nella rete criptata EncroChat, l'accesso, il sequestro e la copia dei dati dei suoi utenti condivisi con le autorità britanniche. Contestano la legalità, la necessità e la proporzionalità di queste ingerenze.
Supponendo che i ricorsi siano ricevibili, la Corte dovrà stabilire se la raccolta dei dati, il loro trattamento e/o la loro condivisione con le autorità britanniche abbiano violato il diritto dei ricorrenti al rispetto della loro vita privata e della loro corrispondenza, ai sensi dell'art. 8 § 1 della Convenzione e/o il diritto ad un ricorso effettivo dinanzi alle autorità francesi ai sensi degli artt. 6 e 13 della Convenzione.
In data 16 dicembre 2021, la Corte ha richiesto al Governo francese convenuto di fornire una serie di precisazioni:

- Quanti dispositivi sono stati interessati dalla captazione dei dati contestata?
- Qual è la natura dei dati raccolti?
- Quali garanzie contro l'arbitrarietà e il rischio di abusi sono state implementate nella fase di esame, selezione, utilizzo e conservazione dei dati raccolti, quali nella fase di trasmissione a terzi, quali nella fase di distruzione dei dati acquisiti?
- I soggetti destinatarie della sorveglianza dei loro dati avevano il diritto di accedere ai dati che li riguardavano o di essere informati dell'esistenza di tale misura? È stato previsto un successivo meccanismo di notifica? In caso di abuso era possibile ricorrere a un organismo o a un tribunale indipendente?

In data 7 aprile 2022 il Governo francese ha depositato le sue osservazioni sull'ammissibilità e sul merito dei ricorsi[56].
Innanzitutto, il Governo ha evidenziato "le peculiarità" della controversia, vale a dire che:
1) *il servizio EncroChat era di per sé illegale (perché non era dichiarato Agenzia nazionale francese per la sicurezza informatica - ANSSI*): in particolare il Governo – con l'evidente intento di contrastare l'eccezione sulla intercettazione massiva e indiscriminata a carico di utenti rispetto ai quali non vi erano necessariamente specifici indizi di reità – pone l'accento sulla illiceità *ex sé* dell'uso dei criptofonini. Ciò deriverebbe dal fatto che i dispositivi EncroChat non erano venduti ufficialmente sul "mercato bianco", in quanto non disponibili direttamente sul sito EncroChat, ma esclusivamente tramite annunci inseriti dai venditori –anonimi – su varie piattaforme non identificative come eBay e Facebook. Gli utenti di questi dispositivi sarebbero stati quindi consapevoli che l'acquisto avveniva sul "mercato grigio". A ciò si aggiunge la

[56] *Observations of the Government of the French Republic on the admissibility and merits of applications nos 44715/20, a.l. v. France and 47930/21, e.j. v. France before the European Court of Human Rights.*

"natura intrinsecamente clandestina" della configurazione dei dispositivi. Infatti, qualsiasi soluzione di crittografia di questo tipo deve essere dichiarata al ANSSI prima di essere immessa sul mercato, cosa che nel caso di specie non è avvenuta. Il Tribunale di Lille avrebbe dunque autorizzato l'operazione perché gli utenti avrebbero agito illecitamente fin dall'acquisto e, dunque, avrebbero potuto "potenzialmente essere accusati di reati". Confermerebbero la suddetta illiceità presunta l'elevato prezzo di mercato dei dispositivi, l'anonimato, la funzione di cancellazione automatica e il *panic code*, nonché l'aver riscontrato *ex post* che i contenuti decifrati dei dispositivi sequestrati facevano riferimento al traffico di droga.

2) *i dati raccolti e attribuiti ai ricorrenti dai tribunali del Regno Unito non erano stati attribuiti a singoli individui prima che le autorità francesi trasferissero i dati nel Regno Unito*: in particolare, tale circostanza è valorizzata dal governo francese per escludere che sussista la giurisdizione della Francia rispetto ai ricorrenti[57].

Il governo francese ha poi valorizzato la legalità della procedura di "*captation judiciare*" ai sensi dell'art. 706-102-1 del codice di procedura penale francese, evidenziando la presenza di un controllo giurisdizionale su presupposti e durata, nonché l'esistenza di rimedi legali[58].

Vi era inoltre un rimedio legale contro la memorizzazione dei dati in Francia nell'ambito dei rimedi previsti per la cancellazione o la rettifica dei dati informatici (legge n. 78-17 del 6 gennaio 1978 sull'informatica, gli archivi di dati e le libertà individuali).

Il Governo segnala al riguardo che, nel corso di una conferenza stampa tenutasi presso Eurojust il 2 luglio 2020 dal pubblico ministero di Lille, era stato reso pubblico un apposito indirizzo email creato e gestito dal dipartimento

---

[57] *Non esiste alcun legame tra i ricorrenti, che sono cittadini britannici su territorio britannico, e la Francia. Sul territorio francese sono transitati solo i dati ma erano crittografati e anonimi stante l'uso di pseudonimi. Le autorità francesi non avevano specifiche informazioni che consentissero loro di identificare i ricorrenti come utenti. L'attribuzione dei dati acquisiti ai due ricorrenti è stata quindi effettuata dalle autorità britanniche sulla base di prove distinte dal procedimento condotto in Francia. I dati grezzi catturati in Francia sono stati trasferiti alle autorità britanniche sulla base di un OIE emesso dal Regno Unito. Anche se questo OIE è intervenuto dopo il provvedimento del giudice francese di sequestro dei dati, è stato l'OIE a consentire il perseguimento dei ricorrenti nel Regno Unito.*

[58] *Sebbene la misura adottata ai sensi dell'articolo 706-102-1 non sia appellabile, può essere rivista sia nei termini che nel merito dal giudice della libertà e della custodia (articolo 706-95-14, sopra citato). Inoltre, gli articoli 170 e ss del codice di procedura penale prevedono che le parti del procedimento possano intervenire nel corso dell'indagine rinviando la questione alla Camera istruttoria per "l'annullamento di un atto o di un documento del procedimento da parte del giudice istruttore", compresi i documenti introdotti nel procedimento prima che diventassero parte*.

investigativo del Centro per la lotta contro i crimini digitali (C3N), consentendo agli utenti di EncroChat (che erano essenzialmente anonimi e non potevano essere informati individualmente) di richiedere la cancellazione dei propri dati. Tuttavia, evidenzia il Governo, nessuna delle persone coinvolte si è avvalsa di questa opzione, probabilmente per evitare che i dati - dai quali emergeva la commissione di attività criminali - gli fossero attribuiti.
Inoltre, il diritto dell'Unione prevedeva mezzi di ricorso interni in relazione al trasferimento di dati alle autorità del Regno Unito in base all'OIE emesso.
Il governo francese nega che i ricorrenti possano dirsi vittime di una violazione dell'art. 8 CEDU nei confronti della Francia poiché, secondo gli stessi ricorrenti, l'attribuzione dei dati nei loro confronti è avvenuta ad opera delle autorità del Regno Unito, dunque non possono essere vittime del sequestro in Francia di dati che non erano a loro attribuiti.
Allo stato, i ricorsi sono pendenti e si attende una decisione della Corte.